



Guida per l'utente

Amazon Simple Storage Service



Versione API 2006-03-01

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Simple Storage Service: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in qualsiasi modo che possa causare confusione tra i clienti o in qualsiasi modo che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è Amazon S3?	1
Caratteristiche di Amazon S3	1
Classi di archiviazione	1
Gestione dello storage	2
Gestione degli accessi e sicurezza	3
Elaborazione dei dati	4
Registrazione e monitoraggio dell'archiviazione	4
Analisi dei dati e informazioni dettagliate	5
Forte coerenza	5
Come funziona Amazon S3	6
Bucket	6
Oggetti	9
Chiavi	10
Funzione Controllo delle versioni S3	10
ID versione	10
Policy del bucket	11
Punti di accesso S3	11
Liste di controllo degli accessi (ACL)	12
Regioni	12
Modello di consistenza dati Amazon S3	13
Applicazioni simultanee	14
Servizi correlati	16
Accesso ad Amazon S3	16
Console di gestione AWS	16
AWS Command Line Interface	17
AWS SDK	17
API REST di Amazon S3	17
Prezzi di Amazon S3	18
Conformità PCI DSS	18
Modifica della disponibilità di Lambda per oggetti Amazon S3	20
Nozioni di base	22
Configurazione	22
Registrati per un Account AWS	23
Fase 1: creazione di un bucket	23

Fase 2: Caricamento di un oggetto	30
Fase 3: donwload di un oggetto	31
Utilizzo della console S3	31
Fase 4: copiare un oggetto	32
Fase 5: eliminare gli oggetti e il bucket	33
Eliminazione di un oggetto	34
Svuotamento del bucket	34
Eliminazione del bucket	35
Fasi successive	35
Conoscere i casi d'uso comuni	36
Controllo dell'accesso a bucket e oggetti	36
Proteggere e monitorare lo storage	38
Sviluppo con Amazon S3	38
Informazioni sui tutorial	40
Esplora la formazione e il supporto	41
Utilizzo di Amazon S3 con AWS CLI	41
Configurazione	42
Fase 1: creare il primo bucket Amazon S3	43
Fase 2: Carica un oggetto nel tuo bucket	49
Fase 3: donwload di un oggetto	50
Fase 4: copiare l'oggetto in una cartella	51
Fase 5: eliminare gli oggetti e il bucket	52
Fasi successive	55
Utilizzo di bucket per uso generico	57
Panoramica dei bucket per uso generico	58
Panoramica dei bucket per uso generico	59
Modelli comuni di bucket per uso generico	60
Permissions	60
Gestione dell'accesso pubblico ai bucket per uso generico	61
Gestione dell'accesso pubblico ai bucket per uso generico	62
Configurazione dei bucket per uso generico	63
Operazioni su bucket per uso generico	66
Monitoraggio delle prestazioni dei bucket per uso generico	66
Namespace per bucket per uso generico	67
Bucket globali per uso generico	68
Bucks generici con namespace regionali dell'account	69

Restrizioni e considerazioni	71
AWS Formato del codice regionale	72
Richiesta della creazione di bucket nel namespace regionale del tuo account	72
Creazione di un bucket nel namespace regionale del tuo account	74
Modelli comuni di bucket	74
Multi-tenant modello di bucket per uso generico	75
Bucket-per-use modello	76
Regole di denominazione	77
Regole di denominazione dei bucket per uso generico	78
Regole di denominazione dei namespace regionali degli account	80
Esempi di nomi di bucket per uso generico	81
Best practice	81
Creazione di un bucket che utilizza un GUID nel nome del bucket	83
Creazione di un bucket nel namespace regionale del tuo account	84
Quote, restrizioni e limitazioni	85
Quote dei bucket	85
Limiti su oggetti e bucket	86
Regole di denominazione dei bucket	86
Accesso a un bucket	86
Casi d'uso	86
Console Amazon S3	88
AWS CLI	88
AWS SDK	89
API REST di Amazon S3	89
Hosting virtuale di bucket per uso generico	90
Creazione di un bucket per uso generico	99
Impostazioni del bucket per uso generico	99
Visualizzazione delle proprietà di un bucket	112
Elenco di bucket	116
Eliminazione del contenuto di un bucket per uso generico	120
Svuotare un secchio generico con AWS CloudTrail disposto	123
Eliminazione di un bucket per uso generico	123
Mountpoint per Amazon S3	128
Installazione di Mountpoint	128
Configurazione e utilizzo di Mountpoint	134
Risoluzione dei problemi di Mountpoint	140

Storage Browser per Amazon S3	141
Utilizzo di Storage Browser per S3	142
Installazione di Storage Browser per S3	143
Impostazione di Storage Browser per S3	143
Configurazione di Storage Browser per S3	158
Risoluzione dei problemi di Storage Browser per S3	159
Configurazione di Transfer Acceleration	159
Perché utilizzare Transfer Acceleration?	159
Requisiti per l'utilizzo di Transfer Acceleration	160
Nozioni di base	161
Abilitazione di Transfer Acceleration	164
Strumento Speed Comparison	171
Utilizzo dei pagamenti a carico del richiedente	172
Come funzionano i pagamenti a carico del richiedente	173
Configurazione di pagamenti a carico del richiedente	174
Recupero della configurazione di requestPayment	176
Download di oggetti dai bucket con pagamento a carico del richiedente	177
Utilizzo degli oggetti	179
Panoramica sugli oggetti	180
Risorse secondarie	182
Denominazione di oggetti	182
Scelta dei nomi delle chiavi di oggetti	183
Linee guida per la denominazione delle chiavi degli oggetti	184
Ordinamento delle chiavi degli oggetti	188
Utilizzo dei metadati	189
Metadati degli oggetti personalizzati	190
System-defined metadati degli oggetti	193
Annotazione di oggetti	196
Etichettare gli oggetti	207
Modifica dei metadati dell'oggetto	220
Individuazione dei dati con le tabelle di S3 Metadata	224
Caricamento degli oggetti	339
Caricamento di un oggetto	341
Impedisci il caricamento di oggetti con nomi di chiavi identici	346
Utilizzo del caricamento in più parti	346
Esecuzione di richieste condizionali	423

Come recuperare o copiare gli oggetti in base ai metadati	424
Come prevenire la sovrascrittura degli oggetti	426
Come eseguire le eliminazioni condizionali	439
Copia, spostamento e denominazione di oggetti	445
Copiare le annotazioni	448
Per copiare un oggetto	448
Spostare un oggetto.	458
Per rinominare un oggetto	459
Download di oggetti	461
Download di un oggetto	462
Download di più oggetti	464
Download di parte di un oggetto	466
Scaricamento di un oggetto da un altro Account AWS	467
Download di oggetti archiviati	468
Download di oggetti in base ai metadati	468
Risoluzione dei problemi di download degli oggetti	468
Verifica dell'integrità degli oggetti in Amazon S3	469
Verifica dell'integrità degli oggetti per caricamenti dei dati in Amazon S3	470
Verifica dell'integrità degli oggetti per i dati a riposo in Amazon S3	492
Eliminazione di oggetti	501
Best practice da considerare prima di eliminare un oggetto	501
Eliminazione di oggetti da un bucket con controllo delle versioni abilitato	502
Eliminazione di oggetti da un bucket con controllo delle versioni sospeso	503
Eliminazione di oggetti da un bucket senza controllo delle versioni	503
MFA-enabled Eliminazione di oggetti da un bucket	503
Eliminazione di un singolo oggetto	504
Eliminazione di più oggetti	514
Organizzare ed elencare gli oggetti	517
Utilizzo dei prefissi	517
Elenco degli oggetti	519
Utilizzo di cartelle	523
Visualizzazione delle proprietà di un oggetto	528
Utilizzo di URL prefirmati per scaricare e caricare oggetti	530
Chi può creare un URL prefirmato	531
Tempo di scadenza per gli URL prefirmati	532
Limitazione delle funzionalità degli URL prefirmati	532

Domande frequenti sugli URL prefirmiti	534
Condivisione di oggetti mediante URL prefirmiti	535
Caricamento di oggetti con URL prefirmiti	540
Trasformazione di oggetti	545
Creazione di punti di accesso Object Lambda	547
Utilizzo dei punti di accesso Amazon S3 Object Lambda	562
Considerazioni relative alla sicurezza	567
Scrittura delle funzioni Lambda	574
Utilizzo di funzioni AWS integrate	607
Best practice e linee guida per S3 Object Lambda	610
Tutorial di S3 Object Lambda	612
Risoluzione dei problemi di Lambda per oggetti S3	651
Esecuzione di operazioni sugli oggetti in blocco	652
Nozioni di base sulle operazioni in batch	652
Tutorial su Operazioni in batch S3	654
Concessione di autorizzazioni	655
Creazione di un processo	669
Operazioni supportate	690
Gestione dei processi	743
Monitoraggio dei rapporti sullo stato e sul completamento dei processi	747
Utilizzo dei tag	763
Gestione di Object Lock con Operazioni in batch	777
Tutorial: Batch-transcoding video	792
Risoluzione dei problemi relativi a Operazioni in batch S3	833
Interrogazione dei dati in loco	846
Requisiti e limiti	846
Costruzione di una richiesta	847
Errori	849
Esempi S3 Select	849
Documentazione di riferimento a SQL	851
Utilizzo di bucket di directory	892
Nomi dei bucket di directory	893
Directory	893
Nomi delle chiavi	893
Gestione degli accessi	894
Quote dei bucket di directory	894

Creazione e utilizzo di bucket di directory	895
Casi d'uso dei bucket di directory	896
Carichi di lavoro ad alte prestazioni	896
Carichi di lavoro di residenza dei dati	954
Differenze per i bucket di directory	972
Differenze per i bucket di directory	973
Operazioni API supportate per i bucket della directory	975
Funzioni di Amazon S3 non supportate dai bucket della directory	975
Collegamento in rete per i bucket di directory	976
Endpoints	976
Configurazione degli endpoint VPC del gateway	977
Regole di denominazione dei bucket di directory	977
Visualizzazione delle proprietà	978
Gestione delle policy dei bucket	979
Aggiunta di una policy di bucket	979
Visualizzazione di una policy del bucket	983
Eliminazione di una policy del bucket	983
Svuotamento di un bucket di directory	984
Eliminazione di un bucket di directory	986
Elencare i bucket di directory	988
Determinazione dell'accesso a un bucket	991
Utilizzo di oggetti in un bucket di directory	992
Importazione di oggetti in un bucket di directory	993
Operazioni con S3 Lifecycle	995
Utilizzo di Operazioni in batch con S3 Express One Zone	1008
Aggiunta di dati agli oggetti	1011
Ridenominazione di un oggetto	1013
Caricamento di un oggetto	1020
Copia di un oggetto	1053
Eliminazione di un oggetto	1059
Download di un oggetto	1064
Generazione di URL prefirmati per la condivisione di oggetti	1066
Recupero dei metadati degli oggetti	1066
Elenco degli oggetti	1067
Sicurezza per i bucket di directory	1068
Protezione e crittografia dei dati	1068

Autenticazione e autorizzazione delle richieste	1093
Best practice di sicurezza	1107
Utilizzo dei punti di accesso per bucket di directory	1111
Regole di denominazione, restrizioni e limitazioni	1112
Riferimento ai punti di accesso per bucket di directory	1113
Operazioni sugli oggetti per i punti di accesso	1114
Configurazione delle policy IAM	1115
Monitoraggio e registrazione dei log	1121
Creazione di punti di accesso per bucket di directory	1122
Gestione dei punti di accesso	1126
Tagging dei punti di accesso	1141
Registrazione con AWS CloudTrail per bucket di directory	1157
CloudTrail eventi di gestione per bucket di directory	1157
CloudTrail eventi di dati per bucket di directory	1158
.....	1159
Metriche di monitoraggio con CloudWatch quattro bucket di directory	1166
Metriche e dimensioni per i bucket di directory	1168
Configurazione delle metriche delle richieste per i bucket di directory	1174
Ottimizzazione delle prestazioni del bucket della directory	1176
Utilizzo dell'autenticazione basata sulla sessione	1176
Best practice per il checksum S3 aggiuntivo	1177
Usa l'ultima versione di AWS SDK e librerie di runtime comuni	1177
Sviluppo con i bucket di directory	1177
Endpoint regionali e di zona per i bucket di directory	1178
Lavorare con i bucket di directory utilizzando la console S3, AWS CLI e AWS SDK	1178
Operazioni API del bucket della directory	1180
Tagging dei bucket di directory	1182
Metodi comuni per utilizzare i tag con i bucket di directory	1182
Gestione dei tag per bucket di directory	1187
Creazione di bucket di directory con tag	1187
Aggiunta di un tag a un bucket di directory	1191
Visualizzazione dei tag di bucket di directory	1194
Eliminazione di un tag da un bucket di directory	1197
Test di resilienza	1200
Come funziona	1200
Considerazioni e limitazioni	1200

Utilizzo di Tabelle Amazon S3 e dei bucket di tabelle	1202
Funzionalità di Tabelle S3	1203
Servizi correlati	1204
Tutorial: Nozioni di base su Tabelle S3	1205
Fase 1: Crea un table bucket e integralo con AWS servizi di analisi	1206
Fase 2: creare un namespace di tabelle e una tabella	1207
Fase 3: Interroga i dati con SQL in Athena	1210
Bucket di tabelle	1211
tipo dei bucket di tabelle	1212
Regole di denominazione dei bucket di tabelle	1213
Creare un bucket di tabelle	1215
Eliminare un bucket di tabelle	1217
Visualizzazione dei dettagli del bucket di tabelle	1218
Gestione delle policy	1219
AWS bucket di tabelle gestiti	1222
Etichettare i bucket da tavolo	1226
Manutenzione di Tabelle S3	1240
Stato dei processi di manutenzione di Tabelle S3	1240
Manutenzione dei bucket di tabelle	1242
Manutenzione delle tabelle	1244
Registra la scadenza per le tabelle	1250
Considerazioni e limitazioni	1256
Tabelle S3 Intelligent-Tiering	1259
Livelli di accesso alle tabelle S3 Intelligent-Tiering	1259
Auto-tiering comportamento con S3 Intelligent-Tiering	1260
Specificare S3 Intelligent-Tiering come classe di archiviazione	1261
Monitoraggio dell'utilizzo dello storage	1262
Spazi dei nomi	1264
Creare un namespace	1265
Eliminare uno spazio dei nomi	1267
Tabelle	1267
Creare una tabella	1269
Eliminazione di una tabella	1275
Visualizzazione dei dettagli di una tabella	1276
Gestione delle policy	1278
Etichettare le tabelle	1281

Accesso alle tabelle	1294
L'accesso alle tabelle tramite AWS Glue Data Catalog integrazione	1294
Accesso diretto alle tabelle	1295
Panoramica dell'integrazione di Tabelle S3	1296
Accesso alle tabelle utilizzando l'endpoint AWS Glue Iceberg REST	1304
Accesso alle tabelle utilizzando l'endpoint Iceberg REST di Tabelle Amazon S3	1309
Accesso alle tabelle con il catalogo client	1315
Amazon Athena	1318
Amazon Redshift	1320
Amazon EMR	1321
di base	1325
Amazon Data Firehose	1327
AWS Glue ETL	1333
Interrogazione di tabelle S3 con Unified Studio SageMaker	1345
Tavoli in streaming con Amazon MSK	1347
Lavorare con Apache Iceberg V3	1350
Caratteristiche principali di V3	1350
Compatibilità delle versioni	1351
Guida introduttiva alla V3	1351
Le migliori pratiche per la versione V3	1355
Strategia di migrazione	1356
Considerazioni sulla compatibilità	1357
Risoluzione dei problemi	1357
Prezzi	1359
Disponibilità	1359
Risorse aggiuntive	1360
Replica delle tabelle S3	1360
Quando utilizzare la replica di S3 Tables	1360
Funzionalità	1361
Come funziona la replica di S3 Tables	1362
Configurazione della replica delle tabelle S3	1366
Gestione della replica delle tabelle S3	1381
Regioni AWS, endpoint e quote	1384
Tabelle S3 Regioni AWS ed endpoint	1385
Quote di Tabelle S3	1385
Esecuzione di richieste su IPv6	1386

Nozioni di base sull'esecuzione di richieste di Tabelle S3 su IPv6	1386
Sicurezza per Tabelle S3	1387
Encryption (Crittografia)	1389
Gestione degli accessi	1404
Connettività VPC	1437
Restrizioni e limitazioni	1444
Registrazione di log e monitoraggio	1444
Registrazione con AWS CloudTrail per tabelle S3	1445
Metriche di monitoraggio con Amazon CloudWatch	1452
Utilizzo di S3 Vectors e bucket vettoriali	1461
Che cos'è Amazon S3 Vectors?	1461
Casi d'uso: ricerche per similarità su set di dati di grandi dimensioni	1462
Funzionalità di S3 Vectors	1462
Archiviazione appositamente progettata per vettori	1462
Esecuzione di query di somiglianza	1463
Filtro dei metadati	1463
Gestione degli accessi e sicurezza	1463
Integrazione con i servizi AWS	1463
Tutorial: Nozioni di base su S3 Vectors	1464
Fase 1. Creazione di un bucket vettoriale con la console	1464
Fase 2. Creazione di un indice vettoriale in un bucket vettoriale con la console	1466
Fase 3. Inserimento di vettori in un indice vettoriale con SDK per Python (Boto3)	1468
Passaggio 4. Query sui vettori in un indice vettoriale con SDK per Python (Boto3)	1470
(Facoltativo) Automazione della creazione di embedding vettoriali con S3 Vectors Embed CLI	1471
(Facoltativo) Integrazione di S3 Vectors con Knowledge Base per Amazon Bedrock	1472
(Facoltativo) Integra i vettori S3 con Amazon OpenSearch	1474
Bucket vettoriali	1474
Regole di denominazione dei bucket vettoriali	1475
Creazione di un bucket vettoriale	1476
Elenco di bucket vettoriali	1479
Visualizzazione degli attributi del bucket vettoriale	1481
Eliminazione di un bucket vettoriale	1481
Gestione delle policy di bucket vettoriali	1483
Etichettare i bucket vettoriali	1485
Indici vettoriali	1497

Requisiti per la denominazione degli indici vettoriali	1497
Requisiti per la dimensione	1497
Opzioni di metrica della distanza	1498
Non-filterable chiavi di metadati	1498
Creazione di un indice vettoriale in un bucket vettoriale	1499
Elenco degli indici vettoriali	1504
Eliminazione di un indice vettoriale	1507
Etichettare gli indici vettoriali	1508
Vettori	1519
Concetti sui vettori	1519
Inserimento di vettori in un indice vettoriale	1520
Elenco dei vettori	1523
Query sui vettori	1526
Eliminazione dei vettori da un indice vettoriale	1529
Filtro dei metadati	1530
Limitazioni e restrizioni	1535
Best practice per S3 Vectors	1536
Creazione e ricerca di embedding vettoriali con <code>s3vectors-embed-cli</code>	1537
Utilizzo di S3 Vectors con altri servizi AWS	1538
Integrazioni disponibili	1538
Vantaggi dell'integrazione	1538
Utilizzo di vettori S3 con servizio OpenSearch	1539
Utilizzo di S3 Vectors con Knowledge Base per Amazon Bedrock	1542
Regioni AWS, endpoint e quote per S3 Vectors	1547
S3 Vectors AWS Regioni ed endpoint	1547
Quote di servizio di S3 Vectors	1552
Sicurezza in S3 Vectors	1552
Identity and Access Management in S3 Vectors	1553
Protezione e crittografia dei dati in S3 Vectors	1570
Endpoint VPC per S3 Vectors	1582
Registrazione con AWS CloudTrail per i vettori S3	1588
Informazioni sui vettori S3 in CloudTrail	1589
CloudTrail eventi di gestione per S3 Vectors	1589
CloudTrail eventi di dati per S3 Vectors	1590
Abilitazione della registrazione di log degli eventi di dati per S3 Vectors	1591
CloudTrail esempio di file di registro per S3 Vectors	1592

Lavorare con i file Amazon S3	1595
Che cos'è S3 Files?	1595
Come funziona S3 Files?	1596
Sei il primo utente di S3 Files?	1597
Concetti chiave	1597
Funzionalità	1598
Come viene fatturato il costo di S3 Files?	1599
Prerequisiti	1600
AWS configurazione dell'account e del computer	1600
Client S3 Files	1600
Ruoli IAM e policy	1602
Gruppi di sicurezza	1607
Tutorial: Guida introduttiva a S3 Files	1607
Iniziare con S3 Files utilizzando il AWS Console	1607
Guida introduttiva a S3 Files utilizzando il AWS CLI	1609
Montaggio di bucket S3 su risorse di elaborazione	1612
Montaggio su Amazon EC2	1612
Montaggio su AWS Lambda	1621
Montaggio su Amazon EKS	1622
Montaggio su Amazon ECS	1624
Cross-account montaggio	1626
Creazione e gestione delle risorse	1633
CloudFormation modello	1635
Creazione di file system	1635
Eliminare i file system	1638
Crea obiettivi di montaggio	1639
Gestione degli obiettivi di montaggio	1641
Eliminare gli obiettivi di montaggio	1642
Creazione di policy del file system	1642
Eliminazione delle politiche del file system	1644
Creazione di punti di accesso	1644
Eliminare i punti di accesso	1647
Tag	1648
Sincronizzazione dei dati	1649
Il bucket S3 è accessibile tramite il file system	1650
Le modifiche al file system si riflettono automaticamente nel bucket S3	1651

Le modifiche nel bucket S3 vengono visualizzate automaticamente nel file system	1651
Comprendere l'impatto delle operazioni di ridenominazione e spostamento	1651
I dati non utilizzati vengono eliminati dal file system per ottimizzare l'archiviazione	1652
Il bucket S3 è la fonte della verità in caso di conflitti	1653
Personalizza la sincronizzazione	1654
Monitoraggio e controllo	1657
CloudWatch monitoraggio	1658
CloudTrail registrazione	1662
Specifiche prestazionali	1668
Riepilogo delle prestazioni	1668
In che modo S3 Files offre prestazioni	1668
Prestazioni di lettura	1669
Prestazioni di scrittura	1669
Latenza del primo accesso	1670
Prestazioni di sincronizzazione	1670
Monitoraggio delle prestazioni	1671
Sicurezza	1671
Protezione dei dati	1672
Encryption (Crittografia)	1673
Come funziona S3 Files con IAM	1677
Esempi di controllo degli accessi dei client	1683
Autorizzazioni POSIX	1687
Misurazione	1691
Come viene misurato lo storage del file system	1692
Come viene misurato l'accesso ai dati	1692
Come viene misurato l'accesso ai dati dal file system	1692
Come viene misurato lo streaming diretto dal tuo bucket S3	1693
Come viene misurata la sincronizzazione dei bucket	1693
Esempi di misurazione	1694
Best practice	1695
Ottimizzazione delle prestazioni e dei costi	1695
Sincronizzazione	1697
Controllo accessi	1697
Monitoraggio	1698
Migrazione	1698
Funzionalità, limiti e quote non supportati	1698

Funzionalità S3 non supportate	1698
Limitazioni del file system	1699
Quote	1699
Funzionalità NFS non supportate	1701
Risoluzione dei problemi	1701
Il comando Mount non riesce	1702
Autorizzazione negata per le operazioni sui file	1702
Il routing di lettura intelligente non funziona	1703
Il file system restituisce costantemente un errore del server NFS	1704
Oggetto mancante nel bucket S3 dopo la scrittura del file system	1704
Oggetto S3 non visibile nel file system	1706
File che appaiono nella directory oggetti smarriti	1706
La sincronizzazione è in ritardo	1708
Attivazione dei log di debug dei client	1708
Controllo accessi	1711
Risorse S3	1712
Identità	1717
Proprietari di bucket o risorse	1719
Strumenti di gestione degli accessi	1719
Azioni	1726
Casi d'uso della gestione degli accessi	1727
Risoluzione dei problemi di gestione degli accessi	1734
Identity and Access Management (IAM)	1735
Destinatari	1736
Autenticazione con identità	1737
Gestione dell'accesso tramite policy	1738
Come funziona Amazon S3 con IAM	1740
Autorizzazione di una richiesta	1767
Autorizzazioni necessarie per le operazioni API S3	1777
Policy e autorizzazioni	1823
Policy di bucket	1827
Identity-based politiche	1883
Procedure con l'uso di policy	1921
Utilizzo dei ruoli collegati ai servizi per Amazon S3 Storage Lens	1963
Risoluzione dei problemi di identità e accesso ad Amazon S3	1967
AWS politiche gestite	1995

Utilizzo dei punti di accesso	1997
Regole di denominazione, restrizioni e limitazioni	1999
Riferimento ai punti di accesso	2003
Compatibilità dei punti di accesso	2007
Configurazione delle policy IAM	2010
Monitoraggio e registrazione dei log	2019
Creazione di un access point	2021
Gestione dei punti di accesso	2030
Utilizzo dei punti di accesso	2035
Tagging dei punti di accesso	2048
Gestione dell'accesso con S3 Access Grants	2064
Concetti di S3 Access Grants	2066
S3 Access Grants e identità delle directory aziendali	2071
Nozioni di base su S3 Access Grants	2080
Operazioni con le istanze S3 Access Grants	2082
Operazioni con le posizioni S3 Access Grants	2095
Operazioni con le concessioni in S3 Access Grants	2117
Ottenere i dati S3 utilizzando i grant di accesso	2131
Accesso multi-account S3 Access Grants	2150
Gestione dei tag per S3 Access Grants	2163
Limitazioni di S3 Access Grants	2165
Integrazioni con S3 Access Grants	2168
Gestione degli accessi con le ACL	2170
Panoramica dell'ACL	2171
Configurazione delle ACL	2191
Esempi di policy	2209
Blocco dell'accesso pubblico	2214
Impostazioni di blocco dell'accesso pubblico	2217
Gestione dei blocchi di accesso pubblico a livello di organizzazione	2221
Esecuzione di operazioni di accesso pubblico di blocco su un punto di accesso	2222
Significato di "pubblico"	2222
Utilizzo di IAM Access Analyzer per S3 per esaminare i bucket pubblici	2226
Permissions	2226
Configurazione del blocco dell'accesso pubblico	2227
Configurazione delle impostazioni dell'account	2228
Configurazione delle impostazioni del bucket e dei punti di accesso	2231

Revisione dell'accesso al bucket	2235
Revisione dell'accesso esterno con il riepilogo degli accessi esterni	2237
Informazioni fornite dallo strumento di analisi degli accessi IAM per S3	2240
Blocco di tutti gli accessi pubblici	2241
Revisione e modifica dell'accesso al bucket	2242
Archiviazione dei risultati del bucket	2243
Attivazione di un risultato di bucket archiviato	2244
Visualizzazione dei dettagli del risultato	2244
Download di un report IAM Access Analyzer per S3	2245
Verifica della proprietà del bucket	2245
Quando utilizzare la condizione proprietario del bucket	2246
Verifica del proprietario del bucket	2247
Esempi	2248
Restrizioni e limitazioni	2250
Controllo della proprietà degli oggetti	2250
Impostazioni di Object Ownership	2252
Modifiche introdotte disabilitando le ACL	2254
Prerequisiti per la disabilitazione delle ACL	2257
Autorizzazioni di Object Ownership	2257
Disabilitare le ACL per tutti i nuovi bucket	2257
Replication e Object Ownership	2258
Impostazione di Object Ownership	2258
Prerequisiti per la disabilitazione delle ACL	2259
Creazione di un bucket	2275
Impostazione di Object Ownership	2284
Visualizzare le impostazioni di Object Ownership	2287
Disabilitare le ACL per tutti i nuovi bucket	2289
Risoluzione dei problemi	2292
Sicurezza	2296
Best practice di sicurezza	2298
Best practice di sicurezza per Amazon S3	2298
Best practice di monitoraggio e audit di Amazon S3	2306
Monitoraggio della sicurezza dei dati	2310
Protezione dei dati	2313
Crittografia dei dati	2315
Server-side crittografia	2317

Utilizzo della crittografia lato client	2439
Crittografia per i dati in transito	2439
Riservatezza del traffico Internet	2447
Traffico tra servizio e applicazioni e client locali	2447
Traffico tra AWS risorse nella stessa regione	2447
AWS PrivateLink per Amazon S3	2448
Convalida della conformità	2469
Resilienza	2471
Crittografia di backup	2473
Sicurezza dell'infrastruttura	2474
Analisi della configurazione e delle vulnerabilità	2475
Gestione degli accessi	2475
Inventario dei dati Amazon S3	2478
Simple Storage Service (Amazon S3)	2478
Posizione geografica	2479
Bucket	2479
Oggetti	2480
Classi di storage	2480
Gestione dello storage	2481
Gestione degli accessi e sicurezza	2481
Trasferimento dati	2482
Risorse correlate	2482
Protezione dei dati	2483
Replica di oggetti all'interno e tra le Regioni	2485
Perché utilizzare la replica?	2486
Quando usare la replica Cross-Region	2487
Quando utilizzare la replica Same-Region	2488
Quando utilizzare la replica bidirezionale	2488
Quando utilizzare S3 Batch Replication	2489
Requisiti del carico di lavoro e replica in tempo reale	2489
Cosa viene replicato?	2490
Requisiti e considerazioni sulla replica	2494
Configurazione della replica in tempo reale	2498
Gestione o sospensione della replica in tempo reale	2592
Replica di oggetti esistenti	2594
Risoluzione dei problemi nella replica	2610

Monitoraggio dell'avanzamento e acquisizione dello stato	2619
Gestione del traffico multi-regione	2644
Creazione di punti di Multi-Region accesso	2646
Configurazione dei punti di accesso multi-regione	2657
Utilizzo dei punti di Multi-Region accesso	2664
Conservazione più versioni degli oggetti	2718
Bucket senza versione, con funzione Controllo delle versioni e con funzione Controllo delle versioni sospesa	2719
Utilizzo della funzione Controllo delle versioni S3 con il ciclo di vita di S3	2720
Funzione Controllo versioni S3	2721
Abilitazione della funzione Controllo delle versioni sui bucket	2725
Configurazione dell'eliminazione di MFA	2733
Utilizzo di oggetti con funzione Controllo delle versioni abilitata	2736
Utilizzo di oggetti con funzione Controllo delle versioni sospesa	2770
Risoluzione dei problemi relativi al controllo delle versioni	2775
Blocco degli oggetti	2781
Come funziona il blocco oggetti S3	2782
Considerazioni su Object Lock	2787
Configurazione del blocco oggetti	2793
Backup dei dati	2804
Ottimizzazione dei costi	2806
Creazione di report di utilizzo e fatturazione	2807
Utilizzo dei tag per l'allocazione dei costi	2808
Report di fatturazione	2810
Report di utilizzo	2814
Comprensione dei report di utilizzo e fatturazione	2816
Fatturazione per le risposte di errore di Amazon S3	2843
Comprensione e gestione delle classi di storage	2866
Oggetti con accesso frequente	2867
Ottimizzazione automatica dei dati con modelli di accesso variabili o sconosciuti	2868
Oggetti a cui si accede raramente	2870
Oggetti con accesso non frequente	2872
Amazon S3 su Outposts	2873
Confronto delle classi di storage	2873
Impostazione della classe di storage di un oggetto	2874
Analisi della classe di storage	2879

Gestione dei costi di storage con il Piano intelligente Amazon S3	2887
Classi di storage Amazon S3 Glacier	2900
Utilizzo di oggetti archiviati	2906
Gestione del ciclo di vita	2920
Gestione del ciclo di vita completo degli oggetti	2922
Trasferimento degli oggetti	2923
Oggetti in scadenza	2932
Impostazione della configurazione del ciclo di vita	2936
Utilizzo di altre configurazioni del bucket	2953
Configurazione delle notifiche di eventi del ciclo di vita S3	2956
Elementi della configurazione del ciclo di vita	2958
Conflitti di configurazione del ciclo di vita	2977
Esempi di configurazioni del ciclo di vita S3	2982
Risoluzione dei problemi del ciclo di vita	2999
Logging e monitoraggio	3006
Strumenti di monitoraggio	3010
Strumenti automatici	3010
Strumenti manuali	3010
Opzioni di registrazione	3011
Registrazione con CloudTrail	3015
Utilizzo CloudTrail dei log con i log e CloudWatch i log di accesso al server Amazon S3 ...	3016
CloudTrail tracciamento con chiamate API SOAP di Amazon S3	3017
CloudTrail eventi	3018
File di log di esempio	3030
Abilitazione CloudTrail	3034
Identificazione delle richieste S3	3037
Registrazione dell'accesso al server	3045
Opzioni di distribuzione	3045
Best-effort consegna dei log del server	3047
Tempo richiesto per l'applicazione delle modifiche dello stato di registrazione del bucket ...	3047
Prezzi	3048
Consegna ai CloudWatch log	3048
Consegna a un bucket GP	3076
Monitoraggio delle metriche con CloudWatch	3124
Metriche e dimensioni	3126
Accesso alle CloudWatch metriche	3146

CloudWatch configurazioni delle metriche	3147
Notifiche di eventi Amazon S3	3157
Panoramica	3158
Tipi di notifiche e destinazioni	3159
Utilizzo di SQS, SNS e Lambda	3168
Usando EventBridge	3198
Monitoraggio dell'attività e dell'utilizzo dello storage con S3 Storage Lens	3211
Caratteristiche e parametri di S3 Storage Lens	3212
Informazioni su S3 Storage Lens	3215
Glossario dei parametri	3230
Impostazione delle autorizzazioni	3311
Lavorare con S3 Storage Lens	3316
Visualizzazione dei parametri di storage	3359
Lavorare con le tabelle S3	3440
Utilizzo di Organizations	3483
Operazioni con i gruppi Storage Lens	3493
Catalogazione e analisi dei dati	3538
Bucket di Amazon S3 Inventory	3540
Elenchi dell'inventario	3540
Configurazione di Amazon S3 Inventory	3546
Individuazione dell'inventario	3559
Impostazione delle notifiche per il completamento dell'inventario	3564
Esecuzione di query sull'inventario con Athena	3565
Convertire stringhe di ID versione vuote in stringhe nulle	3570
Utilizzo del campo ACL oggetto	3573
Ottimizzazione delle prestazioni	3576
Linee guida per le prestazioni di Amazon S3	3577
Misurare le prestazioni	3578
Scala orizzontale	3579
Utilizza i recuperi con intervallo di byte	3579
Richieste di ripetizione	3579
Combinare Amazon S3 e Amazon EC2 nella stessa Regione	3580
Utilizza l'accelerazione del trasferimento per ridurre al minimo la latenza	3580
Utilizza gli ultimi SDK di AWS	3580
Modelli di progettazione delle prestazioni per Amazon S3	3581
Caching dei contenuti a cui si accede di frequente	3581

Timeout e retry per le applicazioni sensibili alla latenza	3582
Scalabilità orizzontale e parallelizzazione delle richieste	3583
Accelerazione dei trasferimenti di dati geograficamente eterogenei	3584
Ottimizzazione per carichi di lavoro a elevata frequenza di richieste	3585
Hosting di un sito Web statico	3587
Endpoint del sito Web	3588
Esempi di endpoint del sito Web	3590
Aggiunta di un CNAME DNS	3590
Utilizzo di un dominio personalizzato con Route 53	3591
Differenze chiave tra un endpoint del sito Web e un endpoint REST API	3591
Abilitazione dell'hosting di siti Web	3592
Configurazione di un documento indice	3597
Documento di indice e cartelle	3598
Configurazione di un documento indice	3599
Configurazione di un documento di errore personalizzato	3600
Codici di risposta HTTP di Amazon S3	3601
Configurazione di un documento di errore personalizzato	3604
Impostazione delle autorizzazioni per l'accesso al sito Web	3605
Fase 1: modifica delle impostazioni dell'accesso pubblico ai blocchi Amazon S3	3606
Fase 2: aggiunta di una policy del bucket	3608
Liste di controllo accessi dell'oggetto	3609
Registrazione del traffico Web	3610
Configurazione di un reindirizzamento	3612
Reindirizzamento delle richieste a un altro host	3612
Configurazione delle regole di reindirizzamento	3613
Reindirizzamento delle richieste per un oggetto	3622
Utilizzo di CORS	3624
Cross-origin condivisione delle risorse: scenari Use-case	3625
In che modo Amazon S3 valuta la configurazione CORS in un bucket?	3625
In che modo Punto di accesso per le espressioni Lambda dell'oggetto supporta CORS	3626
Elementi di una configurazione CORS	3626
Configurazione di CORS	3632
Test di CORS	3641
Risoluzione dei problemi di CORS	3643
Tutorial per siti web statici	3649
Hosting di streaming video	3650

Configurazione di un sito Web statico	3670
Configurazione di un sito web statico utilizzando un dominio personalizzato	3679
Implementazione di un sito web statico su Amplify da Amazon S3	3705
Tagging delle risorse S3	3708
Come funzionano i tag	3708
User-defined tag	3708
Modi comuni per utilizzare i tag	3710
Utilizzo dei tag per l'allocazione dei costi	3711
Utilizzo dei tag per il controllo degli accessi basato su attributi (ABAC)	3712
Pianificazione della strategia di tagging	3714
Gestione dei tag per risorse Amazon S3	3715
Etichettare i bucket	3716
Modi comuni per utilizzare i tag con i bucket	3716
ABAC per bucket S3 per uso generico	3716
Esempi di politiche ABAC per i bucket	3718
Gestione dei tag per i bucket per uso generico	3721
Abilita il bucket ABAC	3721
Esecuzione di audit sulle policy prima dell'abilitazione dell'ABAC	3721
Creazione di bucket generici con tag	3726
Permissions	3726
Risoluzione degli errori	3726
Fasi	3727
Aggiungere un tag a un bucket	3729
Permissions	3729
Risoluzione degli errori	3729
Fasi	3723
Visualizzazione dei bucket tag	3731
Permissions	3732
Risoluzione degli errori	3732
Fasi	3732
Eliminare un tag da un bucket	3734
Permissions	3735
Risoluzione degli errori	3735
Fasi	3735
Quote	3738
Aumenti delle quote	3738

Riferimento 3739

Cronologia dei documenti 3741

Aggiornamenti precedenti 3806

..... mmmmdcccxxv

Che cos'è Amazon S3?

Amazon Simple Storage Service (Amazon S3) è un servizio di archiviazione di oggetti che offre scalabilità, disponibilità dei dati, sicurezza e prestazioni tra le migliori del settore. I clienti di tutte le dimensioni e settori possono utilizzare Amazon S3 per archiviare e proteggere qualsiasi quantità di dati in un'ampia gamma di casi d'uso, come data lake, siti Web, applicazioni mobili, backup e ripristino, archivi, applicazioni per aziende, dispositivi IoT e analisi dei Big Data. Amazon S3 offre caratteristiche di gestione che consentono di ottimizzare, organizzare e configurare l'accesso ai dati per soddisfare specifici requisiti aziendali, organizzativi e di conformità.

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Argomenti

- [Caratteristiche di Amazon S3](#)
- [Come funziona Amazon S3](#)
- [Modello di consistenza dati Amazon S3](#)
- [Servizi correlati](#)
- [Accesso ad Amazon S3](#)
- [Prezzi di Amazon S3](#)
- [Conformità PCI DSS](#)

Caratteristiche di Amazon S3

Classi di archiviazione

Amazon S3 offre una gamma di classi di storage concepite per i diversi casi d'uso. Ad esempio, puoi archiviare i dati di produzione cruciali in S3 Standard o S3 Express One Zone per un accesso frequente, risparmiare sui costi archiviando i dati a cui si accede raramente in S3 Standard-IA o S3 One e archiviare i dati ai costi più bassi in S3 Glacier Instant Retrieval Zone-IA, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

Amazon S3 Express One Zone è una classe di archiviazione Amazon S3 a zona singola ad alte prestazioni, creata appositamente per fornire un accesso ai dati coerente di pochi millisecondi per le applicazioni sensibili alla latenza. S3 Express One Zone è la classe di storage di oggetti cloud con la latenza minima attualmente disponibile, con velocità di accesso ai dati fino a 10 volte maggiori e con costi di richiesta inferiori del 50% rispetto a S3 Standard. S3 Express One Zone è la prima classe di archiviazione S3 in cui è possibile selezionare una singola zona di disponibilità con la possibilità di co-ubicare l'archiviazione di oggetti con le risorse di calcolo, che offre la massima velocità di accesso possibile. Inoltre, per aumentare ulteriormente la velocità di accesso e supportare centinaia di migliaia di richieste al secondo, i dati vengono archiviati in un nuovo tipo di bucket: un bucket di directory Amazon S3. Per ulteriori informazioni, consultare [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Puoi archiviare dati con modelli di accesso mutevoli o sconosciuti in S3 Intelligent-Tiering, il che ottimizza i costi di archiviazione spostando automaticamente i dati tra quattro livelli di accesso quando i modelli di accesso cambiano. Questi quattro livelli di accesso includono due livelli di accesso a bassa latenza ottimizzati per l'accesso frequente e sporadico e due livelli di accesso all'archivio progettati per l'accesso asincrono e per dati a cui accedi raramente.

Per ulteriori informazioni, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

Gestione dello storage

Amazon S3 dispone di caratteristiche di gestione dell'archiviazione utilizzabili per gestire i costi, rispettare i requisiti normativi, ridurre la latenza e salvare più copie distinte dei dati per soddisfare i requisiti di conformità.

- [Ciclo di vita S3](#): consente di impostare la configurazione del ciclo di vita per gestire gli oggetti e archivarli all'insegna dell'efficienza in termini di costi durante l'intero ciclo di vita. Puoi spostare gli oggetti in altre classi di archiviazione S3 o far scadere oggetti che raggiungono la fine del loro ciclo.
- [Blocco degli oggetti S3](#): impedisce che un oggetto di Amazon S3 venga eliminato o sovrascritto per un determinato periodo di tempo o in modo indefinito. Il blocco degli oggetti consente di soddisfare i requisiti normativi che richiedono l'archiviazione write-once-read-many (WORM) o semplicemente di aggiungere un ulteriore livello di protezione contro la modifica e l'eliminazione degli oggetti.
- Replica [S3: replica](#) gli oggetti e i rispettivi metadati e tag degli oggetti in uno o più bucket di destinazione uguali o diversi Regioni AWS per ridurre latenza, conformità, sicurezza e altri casi d'uso.
- [Operazioni in batch S3](#): consente di gestire qualsiasi numero di oggetti su larga scala con una singola richiesta API S3 o pochi clic nella console di Amazon S3. È possibile utilizzare Batch

Operations per eseguire operazioni come Copy, Invoke AWS Lambda e Restore su milioni o miliardi di oggetti.

Gestione degli accessi e sicurezza

Amazon S3 offre caratteristiche per la verifica e la gestione degli accessi ai tuoi bucket e oggetti. Per impostazione predefinita, i bucket S3 e gli oggetti al loro interno sono privati. Puoi accedere solo alle risorse S3 che hai creato. Per concedere autorizzazioni granulari delle risorse che supportano il tuo caso d'uso specifico o per verificare le autorizzazioni delle tue risorse Amazon S3, puoi utilizzare le seguenti caratteristiche.

- [Blocco dell'accesso pubblico di S3](#): blocca l'accesso pubblico a bucket S3 e oggetti. Per impostazione predefinita, le impostazioni Blocco dell'accesso pubblico sono attivate a livello di bucket. È consigliabile mantenere tutte le impostazioni Blocco dell'accesso pubblico disattivate, a meno che non sia necessario disattivarne una o più di una per il caso d'uso specifico. Per ulteriori informazioni, consulta [Configurazione delle impostazioni di blocco dell'accesso pubblico per i bucket S3](#).
- [AWS Identity and Access Management \(IAM\)](#): IAM è un servizio Web che consente di controllare in modo sicuro l'accesso alle AWS risorse, incluse le risorse Amazon S3. Con IAM, puoi gestire centralmente le autorizzazioni che controllano le AWS risorse a cui gli utenti possono accedere. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse.
- Policy [relative ai bucket](#): utilizza il linguaggio IAM-based delle policy per configurare le autorizzazioni basate sulle risorse per i bucket S3 e gli oggetti in essi contenuti.
- [Punto di accesso Amazon S3](#): configura gli endpoint di rete denominati con policy di accesso dedicate per gestire l'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3.
- [Liste di controllo degli accessi \(ACL\)](#): concedi autorizzazioni di lettura e scrittura per singoli bucket e oggetti agli utenti autorizzati. Come regola generale, è consigliabile utilizzare policy basate sulle risorse S3 (policy di bucket e policy dei punti di accesso) o policy utente IAM per il controllo degli accessi anziché ACL. Le policy sono un'opzione di controllo degli accessi semplificata e più flessibile. Con le policy dei bucket e le policy dei punti di accesso, puoi definire le regole applicabili globalmente a tutte le richieste alle risorse Amazon S3. Per ulteriori informazioni su casi specifici quando desideri utilizzare le ACL anziché le policy basate sulle risorse o le policy utente IAM, consultare [Gestione degli accessi con le ACL](#).
- [S3 Proprietà dell'oggetto](#): consente di assumere la proprietà di ogni oggetto nel bucket, semplificando la gestione degli accessi per i dati archiviati in Amazon S3. S3 Proprietà dell'oggetto

è un'impostazione a livello di bucket di Amazon S3 che puoi utilizzare per disabilitare o abilitare le ACL. Per impostazione predefinita, le ACL sono disabilite. Con le ACL disabilite, il proprietario del bucket possiede tutti gli oggetti nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy di gestione dell'accesso.

- [IAM Access Analyzer per S3](#): valuta e monitora le policy di accesso al bucket S3, assicurando che forniscano solo l'accesso previsto alle risorse S3.

Elaborazione dei dati

Per trasformare i dati e attivare i flussi di lavoro in modo che automatizzino una serie di altre attività di elaborazione su larga scala, puoi utilizzare le seguenti caratteristiche.

- [Lambda dell'oggetto S3](#): aggiungi il tuo codice alle richieste GET, HEAD e LIST di S3 per modificare ed elaborare i dati quando vengono restituiti a un'applicazione. Questa caratteristica consente di filtrare righe, ridimensionare dinamicamente immagini, oscurare dati riservati e molto altro ancora.
- [Notifiche di eventi](#): attiva flussi di lavoro che utilizzano Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) e quando viene apportata una modifica alle tue risorse S3. AWS Lambda

Registrazione e monitoraggio dell'archiviazione

Amazon S3 fornisce strumenti di registrazione e monitoraggio che puoi utilizzare per monitorare e controllare come vengono utilizzate le tue risorse Amazon S3. Per ulteriori informazioni, [Strumenti di monitoraggio](#).

Strumenti di monitoraggio automatici

- [CloudWatchParametri Amazon per Amazon S3](#): monitora lo stato operativo delle tue risorse S3 e configura avvisi di fatturazione quando gli addebiti stimati raggiungono una soglia definita dall'utente.
- [AWS CloudTrail](#)— Registra le azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS in Amazon S3. CloudTrail i log forniscono un tracciamento dettagliato delle API per le operazioni S3 a livello di bucket e a livello di oggetto.

Strumenti di monitoraggio manuali

- [Registrazione degli accessi al server](#): fornisce registri dettagliati per le richieste effettuate a un bucket. Puoi utilizzare i registri di accesso al server per molti casi d'uso, come eseguire verifiche di sicurezza e accesso, conoscere la tua base clienti o capire meglio la fattura Amazon S3.
- [AWS Trusted Advisor](#): valuta il tuo account utilizzando i controlli delle AWS migliori pratiche per identificare modi per ottimizzare l'AWS infrastruttura, migliorare la sicurezza e le prestazioni, ridurre i costi e monitorare le quote di servizio. Puoi quindi seguire i suggerimenti per ottimizzare i servizi e le risorse.

Analisi dei dati e informazioni dettagliate

Amazon S3 offre caratteristiche per aiutarti a ottenere visibilità sull'utilizzo dello spazio di archiviazione, che ti consente di comprendere, analizzare e ottimizzare meglio lo spazio di archiviazione su larga scala.

- [Amazon S3 Storage Lens](#): consente di comprendere, analizzare e ottimizzare l'archiviazione. S3 Storage Lens offre oltre 60 metriche di utilizzo e attività e dashboard interattivi per aggregare i dati per l'intera organizzazione, account specifici, bucket o prefissi. Regioni AWS
- [Analisi della classe di storage](#): consente di analizzare i modelli di accesso all'archiviazione per decidere quando è il momento di spostare i dati in una classe più conveniente.
- [S3 Inventory con report di Inventory](#): consente di verificare e creare report sugli oggetti e sui relativi metadati e configurare altre caratteristiche di Amazon S3 per intervenire sui report di Inventory. Ad esempio, puoi creare report sullo stato di replica e crittografia degli oggetti. Per un elenco di tutti i metadati disponibili per ogni oggetto nei report di Amazon S3 Inventory, consulta [questa sezione](#).

Forte coerenza

Amazon S3 offre una forte coerenza di lettura dopo scrittura per le richieste PUT e DELETE di oggetti nel bucket Amazon S3 in generale. Regioni AWS Questo comportamento vale sia per le scritture dei nuovi oggetti che per le richieste PUT che sovrascrivono gli oggetti esistenti e le richieste DELETE. Inoltre, le operazioni di lettura su Amazon S3 Select, le liste di controllo accessi (ACL) Amazon S3, i tag oggetto Amazon S3 e i metadati degli oggetti (ad esempio, l'oggetto HEAD) sono fortemente coerenti. Per ulteriori informazioni, consulta [Modello di consistenza dati Amazon S3](#).

Come funziona Amazon S3

Amazon S3 è un servizio di archiviazione di oggetti che archivia i dati come oggetti, dati gerarchici o dati tabulari all'interno di bucket. Un oggetto è un file e tutti i metadati che lo descrivono. Un bucket è un container per oggetti o file.

Per archiviare dati in Amazon S3, per prima cosa devi creare un bucket e specificarne nome e Regione AWS, quindi devi caricare i dati nel bucket come oggetti in Amazon S3. Ogni oggetto contiene una chiave (o nome chiave), che è l'identificatore univoco dell'oggetto nel bucket.

S3 fornisce funzionalità che puoi configurare per supportare il tuo caso d'uso specifico. Puoi utilizzare Controllo delle versioni S3 per mantenere più versioni di un oggetto in un unico bucket e consentire di ripristinare oggetti che vengono accidentalmente eliminati o sovrascritti.

I bucket e gli oggetti che contengono sono privati e accessibili solo se concedi esplicitamente le autorizzazioni di accesso. Puoi utilizzare policy bucket, policy AWS Identity and Access Management (IAM), liste di controllo degli accessi (ACL) e punti di accesso S3 per gestire l'accesso.

Argomenti

- [Bucket](#)
- [Oggetti](#)
- [Chiavi](#)
- [Funzione Controllo delle versioni S3](#)
- [ID versione](#)
- [Policy del bucket](#)
- [Punti di accesso S3](#)
- [Liste di controllo degli accessi \(ACL\)](#)
- [Regioni](#)

Bucket

Amazon S3 supporta quattro tipi di bucket: bucket per uso generico, bucket di directory, bucket di tabelle e bucket vettoriali. Ogni tipo di bucket offre un set unico di funzionalità per diversi casi d'uso.

Bucket per uso generico: i bucket per uso generico sono il tipo di bucket S3 originale e sono consigliati per la maggior parte dei casi d'uso e dei modelli di accesso. Un bucket per uso generico

è un container per gli oggetti archiviati in Amazon S3 che può archiviare qualsiasi numero di oggetti e utilizzare tutte le classi di archiviazione (ad eccezione di S3 Express One Zone), in modo da poter archiviare oggetti in modo ridondante su più zone di disponibilità. Per ulteriori informazioni, consulta [Creazione, configurazione e utilizzo di bucket per uso generico Amazon S3](#).

Per impostazione predefinita, i bucket generici esistono in un namespace globale, il che significa che ogni nome di bucket deve essere univoco all'interno di una partizione. Account AWS Regioni AWS Una partizione è un raggruppamento di regioni. AWS attualmente ha quattro partizioni: `aws` (Regioni standard), `aws-cn` (Regioni della Cina), `aws-us-gov` (AWS GovCloud (US)) e `aws-eu-c` (European Sovereign Cloud). Quando crei un bucket generico, puoi scegliere di creare un bucket nello spazio dei nomi globale condiviso oppure puoi scegliere di creare un bucket nello spazio dei nomi regionale del tuo account. Lo spazio dei nomi regionale del tuo account è una suddivisione dello spazio dei nomi globale in cui solo il tuo account può creare bucket. I nuovi bucket generici creati nel namespace regionale del tuo account sono unici per il tuo account e non possono mai essere ricreati da un altro account. [Per ulteriori informazioni sui namespace dei bucket, consulta Namespace per bucket generici](#).

Note

Per impostazione predefinita, tutti i bucket per uso generico sono privati. È comunque possibile fornire l'accesso pubblico ai bucket per uso generico. È possibile controllare l'accesso ai bucket per uso generico a livello di bucket, prefisso (cartella) o tag dell'oggetto. Per ulteriori informazioni, consulta [Controllo degli accessi in Amazon S3](#).

Bucket di directory: sono consigliati per i casi d'uso della bassa latenza e della residenza dei dati. Per impostazione predefinita, è possibile creare fino a 100 bucket di directory nell'Account AWS, senza limiti al numero di oggetti che si possono archiviare in un bucket di directory. I bucket di directory organizzano gli oggetti in directory gerarchiche (prefissi) anziché nella struttura di archiviazione piatta dei bucket per uso generico. Questo tipo di bucket non ha limiti di prefissi e le singole directory possono essere scalate orizzontalmente. Per ulteriori informazioni, consulta [Utilizzo dei bucket di directory](#).

- Per i casi d'uso a bassa latenza, puoi creare un bucket di directory in una singola zona di disponibilità per archiviare i dati. AWS I bucket di directory nelle zone di disponibilità supportano la classe di storage S3 Express One Zone. Con S3 Express One Zone, i dati vengono archiviati in modo ridondante su più dispositivi all'interno di una singola zona di disponibilità. La classe di storage S3 Express One Zone è consigliata se la tua applicazione è sensibile alle prestazioni e

beneficia di latenze a una cifra al millisecondo PUT e GET. Per ulteriori informazioni sulla creazione di bucket di directory nelle zone di disponibilità, consulta [Carichi di lavoro ad alte prestazioni](#).

- Per i casi d'uso relativi alla residenza dei dati, è possibile creare un bucket di directory in un'unica zona locale AWS dedicata (DLZ) per archiviare i dati. In Zone locali dedicate è possibile creare bucket di directory S3 per archiviare i dati in un perimetro dei dati specifico, che aiuta a supportare i casi d'uso della residenza dei dati e dell'isolamento dei dati. I bucket di directory in Local Zones supportano la classe di storage S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA). Per ulteriori informazioni sulla creazione di bucket di directory in Zone locali, consulta [Carichi di lavoro di residenza dei dati](#).

Note

Per impostazione predefinita, i bucket di directory hanno l'accesso pubblico disabilitato. Questo comportamento non può essere modificato. Non è possibile concedere l'accesso agli oggetti archiviati nei bucket di directory, ma solo ai bucket di directory. Per ulteriori informazioni, consulta [Autenticazione e autorizzazione delle richieste](#).

Bucket di tabelle: consigliati per l'archiviazione di dati tabulari, come le transazioni di acquisto giornaliero, i dati dei sensori di streaming o le ad impression. I dati tabulari rappresentano i dati in colonne e righe, come in una tabella di database. I bucket di tabelle forniscono un'archiviazione S3 ottimizzata per i carichi di lavoro di analisi e machine learning, con funzionalità progettate per migliorare costantemente le prestazioni delle query e ridurre i costi di archiviazione per le tabelle. Tabelle S3 è progettato appositamente per l'archiviazione di dati tabulari nel formato Apache Iceberg. Puoi interrogare i dati tabulari nelle tabelle S3 con i motori di query più diffusi, tra cui Amazon Athena, Amazon Redshift e Apache Spark. Per impostazione predefinita, puoi creare fino a 10 bucket di tabella per ogni tabella Regione AWS e fino a 10.000 tabelle Account AWS per bucket. Per ulteriori informazioni, consulta [Utilizzo di Tabelle S3 e bucket di tabelle](#).

Note

Tutti i bucket di tabelle e le tabelle sono privati e non possono essere resi pubblici. L'accesso a queste risorse è possibile solo per gli utenti a cui è concesso esplicitamente l'accesso. Per concedere l'accesso, è possibile utilizzare le policy basate sulle risorse IAM per i bucket di tabelle e le tabelle e per le policy basate sull'identità IAM per utenti e ruoli. Per ulteriori informazioni, consulta [Sicurezza per Tabelle S3](#).

Bucket di vettori: i bucket vettoriali S3 sono un tipo di bucket Amazon S3 creato appositamente per poter archiviare e sottoporre a query i vettori. I bucket vettoriali utilizzano operazioni API dedicate per scrivere e sottoporre a query i dati vettoriali in modo efficiente. Con i bucket vettoriali S3, puoi archiviare incorporamenti vettoriali per modelli di machine learning, eseguire ricerche di similarità e integrarti con servizi come Amazon Bedrock e Amazon. OpenSearch

I bucket vettoriali S3 organizzano i dati utilizzando indici vettoriali, ovvero risorse all'interno di un bucket che archiviano e organizzano i dati vettoriali per eseguire operazioni di ricerca per similarità in modo efficiente. Ogni indice vettoriale può essere configurato con dimensioni, metriche della distanza (come la somiglianza del coseno) e configurazioni di metadati specifiche da ottimizzare per il caso d'uso specifico. Per ulteriori informazioni, consulta [Utilizzo di S3 Vectors e bucket vettoriali](#).

Ulteriori informazioni su tutti i tipi di bucket

Quando crei un bucket, inserisci un nome e scegli la Regione AWS dove si troverà. Dopo avere creato un bucket, non puoi modificarne il nome né la regione. I nomi dei bucket devono seguire le seguenti regole di denominazione:

- [Regole di denominazione dei bucket per uso generico](#)
- [Regole di denominazione dei bucket di directory](#)
- [Regole di denominazione dei bucket di tabelle](#)

I bucket inoltre:

- Organizzano lo spazio dei nomi Amazon S3 al livello più alto. Per i bucket per uso generico, questo namespace è S3. Per i bucket di directory, questo namespace è s3express. Per i bucket di tabelle, questo namespace è s3tables.
- Identificano l'account responsabile del costo di archiviazione e trasferimento dati.
- Servono come unità di aggregazione per i report di utilizzo.

Oggetti

Entità fondamentali archiviate in Amazon S3, gli oggetti sono composti da dati e metadati. I metadati sono invece un set di coppie nome-valore che descrivono l'oggetto. Queste coppie includono alcuni metadati di default, ad esempio la data dell'ultima modifica, e metadati HTTP standard, come Content-Type. È anche possibile specificare metadati personalizzati al momento dell'archiviazione dell'oggetto.

Ogni oggetto è contenuto in un bucket. Ad esempio, se l'oggetto denominato `photos/puppy.jpg` è archiviato nel bucket per uso generico `amzn-s3-demo-bucket` nella Regione Stati Uniti occidentali (Oregon), è indirizzabile tramite l'URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg`. Per ulteriori informazioni, consulta [Accesso a un bucket](#).

Un oggetto viene identificato in modo univoco in un bucket tramite un [\(nome\) chiave](#) e un [ID versione](#) (se Controllo delle versioni S3 è abilitato nel bucket). Per ulteriori informazioni sugli oggetti, consulta [Panoramica degli oggetti di Amazon S3](#).

Chiavi

Una chiave oggetto (o nome chiave) è l'identificatore univoco di un oggetto in un bucket. Per ogni oggetto in un bucket è presente esattamente una chiave. La combinazione di bucket, chiave oggetto e, facoltativamente, ID versione (se il Controllo delle versioni S3 è abilitato per il bucket) identificherà in modo univoco ogni oggetto. Quindi puoi pensare ad Amazon S3 come a una mappa di dati di base tra "bucket + chiave + versione" e l'oggetto stesso.

Si può fare riferimento in modo univoco a ogni oggetto in Amazon S3 tramite la combinazione di endpoint del servizio Web, nome del bucket, chiave e, facoltativamente, una versione. Ad esempio, nell'URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg`, **`amzn-s3-demo-bucket`** è il nome del bucket e `photos/puppy.jpg` è la chiave.

Per ulteriori informazioni sulle chiavi degli oggetti, consulta [Denominazione di oggetti Amazon S3](#).

Funzione Controllo delle versioni S3

Puoi utilizzare Controllo delle versioni S3 per conservare più versioni di un oggetto nello stesso bucket. Puoi utilizzare Controllo delle versioni S3 per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nei bucket. Puoi facilmente eseguire il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente.

Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

ID versione

Se abiliti Controllo delle versioni S3 per un bucket, Amazon S3 genera un ID versione univoco per tutti gli oggetti aggiunti a tale bucket. Gli oggetti già esistenti nel bucket al momento dell'attivazione

del controllo delle versioni hanno un ID versione null. Se modifichi questi (o altri) oggetti con altre operazioni, come [CopyObject](#), i nuovi oggetti ottengono un ID di versione [PutObject](#) univoco.

Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Policy del bucket

Una bucket policy è una policy basata sulle risorse AWS Identity and Access Management (IAM) che puoi utilizzare per concedere le autorizzazioni di accesso al tuo bucket e agli oggetti in esso contenuti. Solo il proprietario del bucket può associare una policy a un bucket. Le autorizzazioni allegate a un bucket si applicano a tutti gli oggetti del bucket di proprietà del proprietario del bucket. Le policy di bucket sono limitate a dimensioni di 20 KB.

Le policy Bucket utilizzano un linguaggio di policy di JSON-based accesso che è standard in tutti. AWS Puoi utilizzare policy di bucket per aggiungere o negare autorizzazioni per gli oggetti in un bucket. Le policy di bucket approvano o negano le richieste in base agli elementi che contengono, inclusi richiedente, operazioni S3, risorse e aspetti o condizioni della richiesta (ad esempio, l'indirizzo IP utilizzato per inviarla). Ad esempio, puoi creare una policy che conceda autorizzazioni tra account per caricare oggetti in un bucket S3 garantendo al contempo che il proprietario del bucket abbia il pieno controllo degli oggetti caricati. Per ulteriori informazioni, consulta [Esempi di policy del bucket Amazon S3](#).

Nella policy di bucket puoi utilizzare caratteri jolly negli Amazon Resource Name (ARN) e altri valori per concedere autorizzazioni a un sottoinsieme di oggetti. Ad esempio, puoi controllare l'accesso a gruppi di oggetti che iniziano con un [prefisso](#) comune o terminano con una determinata estensione, come .html.

Punti di accesso S3

I punti di accesso Amazon S3 sono endpoint di rete denominati con policy di accesso dedicate che descrivono come è possibile accedere ai dati utilizzando tali endpoint. I punti di accesso sono collegati a un'origine dati sottostante, ad esempio un bucket per uso generico, un bucket di directory o un volume FSx per OpenZFS, che è possibile utilizzare per eseguire operazioni sugli oggetti S3, ad esempio GetObject e PutObject. Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3.

Ogni punto di accesso ha una propria policy. È inoltre possibile configurare le impostazioni di [Blocco dell'accesso pubblico](#) per ciascun punto di accesso collegato a un bucket. Per limitare l'accesso ai

dati di Amazon S3 a una rete privata puoi configurare qualsiasi punto di accesso per accettare le richieste solo da un virtual private cloud (VPC).

Per ulteriori informazioni sui punti di accesso per bucket per uso generico, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#). Per ulteriori informazioni sui punti di accesso per bucket di directory, consulta [Gestione dell'accesso ai set di dati condivisi in bucket di directory con punti di accesso](#).

Liste di controllo degli accessi (ACL)

È possibile utilizzare le ACL per fornire autorizzazioni di lettura e scrittura per singoli oggetti e bucket per uso generico agli utenti autorizzati. A ogni oggetto e bucket per uso generico è collegata una ACL come risorsa secondaria. L'ACL definisce a quali Account AWS gruppi è concesso l'accesso e il tipo di accesso. Le ACL sono un meccanismo di controllo degli accessi che precede IAM. Per ulteriori informazioni sulle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le liste di controllo degli accessi (ACL) sono disabilitate. Quando le ACL sono disabilitate, il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ad essi in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne nelle circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Con le ACL disabilitate, puoi utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Regioni

Puoi scegliere l'area geografica Regione AWS in cui Amazon S3 archivia i bucket che crei. La scelta di una regione permette di ottimizzare la latenza, ridurre al minimo i costi o rispondere ai requisiti normativi. Gli oggetti archiviati in un'altra regione Regione AWS non escono mai dalla regione a meno che non vengano trasferiti o replicati esplicitamente in un'altra regione. Ad esempio, gli oggetti archiviati nella regione Europa (Irlanda) non lasceranno mai tale regione.

 Note

Puoi accedere ad Amazon S3 e alle sue funzionalità solo nelle versioni abilitate per il Regione AWS tuo account. Per ulteriori informazioni sull'abilitazione di una regione per la creazione e la gestione di AWS risorse, consulta [Managing Regioni AWS](#) in the Riferimenti generali di AWS.

Per un elenco degli endpoint e delle regioni Amazon S3 disponibili, consultare la sezione relativa a [regioni ed endpoint](#) nella Riferimenti generali di AWS.

Modello di consistenza dati Amazon S3

Amazon S3 offre una forte coerenza di lettura dopo scrittura per le richieste PUT e DELETE di oggetti nel bucket Amazon S3 in generale. Regioni AWS Questo comportamento vale sia per le scritture di nuovi oggetti che per le richieste PUT che sovrascrivono gli oggetti esistenti e le richieste DELETE. Inoltre, le operazioni di lettura su Amazon S3 Select, le liste di controllo accessi Amazon S3, i tag oggetto Amazon S3 e i metadati degli oggetti (ad esempio, l'oggetto HEAD) sono fortemente coerenti.

Gli aggiornamenti a una singola chiave sono atomici. Ad esempio, se esegui una richiesta PUT su una chiave esistente da un thread ed esegui poi una richiesta GET sulla stessa chiave da un secondo thread contemporaneamente, otterrai i vecchi dati o i nuovi dati, ma mai dati parziali o danneggiati.

Amazon S3 ottiene un'alta disponibilità replicando i dati su più server in data center AWS . Se una richiesta PUT ha esito positivo, i dati verranno archiviati in totale sicurezza. Qualsiasi lettura (richiesta GET o LIST) avviata dopo la ricezione di una risposta PUT riuscirà restituire i dati scritti dall'operazione PUT. Di seguito sono riportati alcuni esempi di questo comportamento.

- Un processo scrive un nuovo oggetto in Amazon S3 ed elenca immediatamente le chiavi nel relativo bucket. Il nuovo oggetto viene visualizzato nell'elenco.
- Un processo sostituisce un oggetto esistente e tenta immediatamente di effettuarne la lettura. Amazon S3 restituisce i nuovi dati.
- Un processo elimina un oggetto esistente e tenta immediatamente di effettuarne la lettura. Amazon S3 non restituisce alcun dato poiché l'oggetto è stato eliminato.
- Un processo elimina un oggetto esistente ed elenca immediatamente le chiavi nel relativo bucket. L'oggetto non viene visualizzato nell'elenco.

Note

- Amazon S3 non supporta il blocco degli oggetti per istanze di scrittura simultanee. Se vengono effettuate simultaneamente due richieste PUT per la stessa chiave, la richiesta con l'ultimo timestamp ha la precedenza. Se questo rappresenta un problema, devi creare un meccanismo di blocco degli oggetti nell'applicazione.
- Gli aggiornamenti sono basati su chiave. Non è possibile eseguire aggiornamenti atomici tra le chiavi. Non si può ad esempio eseguire l'aggiornamento di una chiave dipendente dall'aggiornamento di un'altra chiave, a meno che non si progetti questa funzionalità nell'applicazione.

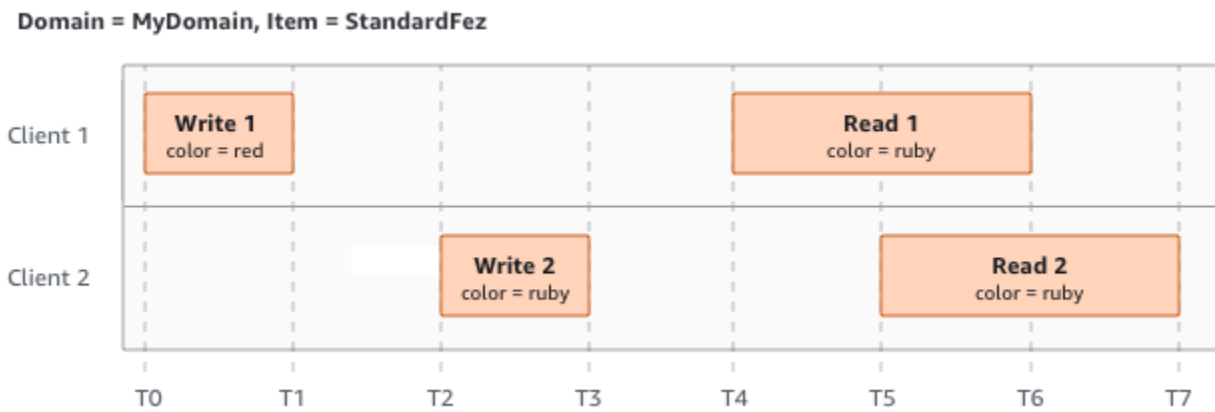
Le configurazioni dei bucket hanno un modello di consistenza. In particolare, questo significa che:

- Se elimini un bucket e visualizzi immediatamente tutti i bucket, il bucket eliminato potrebbe comunque essere visualizzato nell'elenco.
- Se abiliti il controllo delle versioni su un bucket per la prima volta, potrebbe essere necessario un breve periodo di tempo per la propagazione completa della modifica. Sugeriamo di attendere 15 minuti dopo aver abilitato il controllo delle versioni prima di eseguire operazioni di scrittura (richieste PUT o DELETE) sugli oggetti nel bucket.

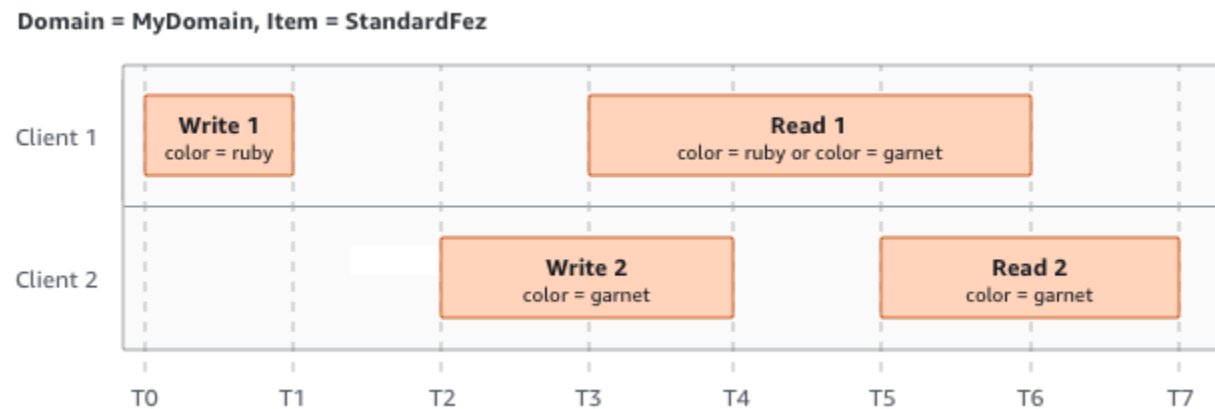
Applicazioni simultanee

In questa sezione sono riportati esempi di comportamento previsto da Amazon S3 quando più client scrivono sugli stessi articoli.

In questo esempio, entrambe le richieste di scrittura W1 e W2 terminano prima dell'avvio delle letture R1 e R2. Poiché S3 è fortemente consistente, R1 e R2 restituiscono entrambi `color = ruby`.

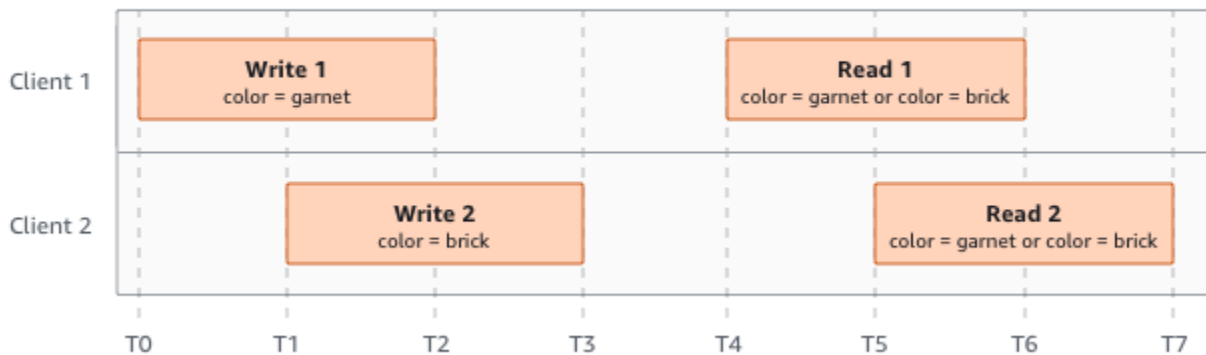


Nell'esempio successivo, la scrittura W2 non termina prima dell'avvio della lettura R1. Pertanto, R1 potrebbe restituire `color = ruby` o `color = garnet`. Tuttavia, dal momento che W1 e W2 terminano prima dell'inizio di R2, R2 restituisce `color = garnet`.



Nell'ultimo esempio, W2 inizia prima che W1 abbia ricevuto una notifica. Pertanto, queste scritture sono considerate simultanee. Amazon S3 utilizza internamente la semantica *last-writer-wins* per determinare quale scrittura ha la precedenza. Tuttavia, l'ordine in cui Amazon S3 riceve le richieste e l'ordine in cui le applicazioni ricevono le notifiche non possono essere previsti a causa di vari fattori quali la latenza della rete. Ad esempio, W2 potrebbe essere avviata da un'istanza Amazon EC2 nella stessa regione, mentre W1 potrebbe essere avviata da un host più lontano. Il modo migliore per determinare il valore finale è eseguire una lettura dopo che entrambe le scritture sono state riconosciute.

Domain = MyDomain, Item = StandardFaz



Servizi correlati

Dopo aver caricato i dati in Amazon S3, puoi utilizzarli con altri AWS servizi. Di seguito vengono riportati i servizi che potresti utilizzare più di frequente:

- [Amazon Elastic Compute Cloud \(Amazon EC2\)](#): fornisce capacità di calcolo scalabile e sicura in Cloud AWS. L'utilizzo di Amazon EC2 elimina la necessità di investimenti anticipati in hardware e ti permette di sviluppare e implementare più rapidamente le applicazioni. Puoi utilizzare Amazon EC2 per avviare il numero di server virtuali necessari, configurare la sicurezza e i servizi di rete, nonché gestire l'archiviazione.
- [Amazon EMR](#): consente ad aziende, ricercatori, analisti e sviluppatori di elaborare un'enorme quantità di dati in modo semplice ed economico. Amazon EMR usa un framework Hadoop gestito eseguito sull'infrastruttura a livello Web di Amazon EC2 e Amazon S3.
- [AWS Transfer Family](#): fornisce supporto completamente gestito per i trasferimenti di file diretti in entrata e uscita da Amazon S3 o Amazon Elastic File System (Amazon EFS) utilizzando i protocolli SFTP, FTPS e FTP.

Accesso ad Amazon S3

Puoi lavorare con Amazon S3 nei modi descritti di seguito:

Console di gestione AWS

La console è un'interfaccia utente basata sul Web per la gestione di Amazon S3 AWS e delle risorse. Se ti sei registrato a Account AWS, puoi accedere alla console Amazon S3 accedendo Console di gestione AWS e scegliendo S3 dalla Console di gestione AWS home page.

AWS Command Line Interface

Puoi usare gli strumenti della AWS riga di comando per impartire comandi o creare script dalla riga di comando del tuo sistema per eseguire attività AWS (incluso S3).

Il [AWS Command Line Interface \(AWS CLI\)](#) fornisce comandi per un ampio set di Servizi AWS. AWS CLI È supportato su Windows, macOS e Linux. Per iniziare, consulta la [Guida per l'utente di AWS Command Line Interface](#) . Per ulteriori informazioni sui comandi per Amazon S3, consulta [s3api](#) e [s3control](#) nella pagina di riferimento dei comandi della AWS CLI .

AWS SDK

AWS fornisce SDK (kit di sviluppo software) costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (Java, Python, Ruby, .NET, iOS, Android e così via). Gli AWS SDK offrono un modo conveniente per creare l'accesso programmatico a S3 e. AWS Amazon S3 è un servizio REST. Puoi inviare richieste ad Amazon S3 utilizzando le librerie AWS SDK, che racchiudono l'API REST di Amazon S3 sottostante e semplificano le attività di programmazione. Ad esempio, gli SDK si occupano di attività quali il calcolo delle firme, la firma crittografica delle richieste, la gestione degli errori e la ripetizione automatica delle richieste. [Per informazioni sugli AWS SDK, incluso come scaricarli e installarli, consulta Tools for. AWS](#)

Ogni interazione con Amazon S3 è autenticata o anonima. Se utilizzi gli AWS SDK, le librerie calcolano la firma per l'autenticazione dalle chiavi che fornisci. Per ulteriori informazioni su come effettuare richieste ad Amazon S3, consulta [Esecuzione di richieste](#).

API REST di Amazon S3

L'architettura di Amazon S3 è ideata per essere indipendente dal linguaggio di programmazione e per utilizzare le interfacce supportate da AWS per archiviare e recuperare oggetti. Puoi accedere a S3 e AWS a livello di programmazione utilizzando l'API REST di Amazon S3. L'API REST è un'interfaccia HTTP per Amazon S3. Con l'API REST, utilizzi le richieste HTTP standard per creare, recuperare ed eliminare bucket e oggetti.

Per utilizzare l'API REST, puoi servirti di qualunque kit di strumenti in grado di supportare HTTP. Puoi anche utilizzare un browser per recuperare gli oggetti, purché siano leggibili in modo anonimo.

Poiché l'API REST utilizza codici di stato e intestazioni HTTP standard, i kit di strumenti e i browser standard funzionano come previsto. In alcune aree sono state aggiunte funzionalità ad HTTP, ad esempio le intestazioni per il supporto del controllo accessi. Le nuove funzionalità sono state in tali casi aggiunte in modo da essere conformi allo stile di utilizzo di HTTP standard.

Se effettui chiamate API REST direttamente dall'applicazione in uso, devi scrivere il codice per calcolare la firma e aggiungerlo alla richiesta. Per ulteriori informazioni su come effettuare richieste ad Amazon S3, consulta [Esecuzione di richieste](#) nella documentazione di riferimento delle API Amazon S3.

Note

Il supporto API SOAP su HTTP è obsoleto ma è ancora disponibile su HTTPS. Le funzioni più recenti di Amazon S3 non sono supportate per SOAP. Ti consigliamo di utilizzare l'API REST o gli AWS SDK.

Prezzi di Amazon S3

La determinazione dei prezzi di Amazon S3 è stata concepita in modo da non dover pianificare requisiti di storage per la tua applicazione. La maggior parte dei provider di archiviazione richiede l'acquisto di una quantità predeterminata di capacità di archiviazione e di trasferimento di rete. In questi casi, se superi questa capacità, il servizio viene disattivato o ti vengono addebitati costi aggiuntivi elevati. Se non si supera tale capacità, si pagherà comunque l'importo per l'intera capacità.

Con Amazon S3 si paga esclusivamente ciò che si utilizza, senza costi nascosti o aggiuntivi. Questo modello ti offre un servizio a costo variabile che può crescere con la tua azienda, offrendoti al contempo i vantaggi in termini di costi dell'infrastruttura. AWS Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Quando ti registri AWS, il tuo Account AWS viene automaticamente registrato per tutti i servizi in AWS, incluso Amazon S3. Tuttavia, vengono addebitati solo i servizi che utilizzi. Se sei un nuovo cliente Amazon S3, puoi iniziare a utilizzare Amazon S3 gratuitamente. Per ulteriori informazioni, consulta [Piano gratuito AWS](#).

Per vedere la tua fattura, vai sul Pannello di controllo Gestione fatturazione e costi nella [console Gestione costi e fatturazione AWS](#). Per ulteriori informazioni sulla Account AWS fatturazione, consulta la Guida per l'[AWS Billing utente](#). In caso di domande relative alla AWS fatturazione e Account AWS, contatta l'[AWS assistenza](#).

Conformità PCI DSS

Amazon S3 supporta l'elaborazione, l'archiviazione e la trasmissione di dati di carte di credito da parte di un esercente o di un provider di servizi, oltre a essere conforme allo standard Payment Card

Industry Data Security Standard (PCI DSS). Per ulteriori informazioni su PCI DSS, incluso come richiedere una copia del PCI AWS Compliance Package, vedere [PCI](#) DSS Level 1.

Modifica della disponibilità di Lambda per oggetti Amazon S3

Dopo un'attenta valutazione, S3 Object Lambda a partire dal 7 novembre 2025 è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner Partner Network (APN). I clienti esistenti di S3 Object Lambda, così come i clienti che utilizzano o implementano soluzioni partner APN, possono continuare a utilizzare il servizio come al solito. AWS daremo priorità ai miglioramenti della sicurezza e della disponibilità per S3 Object Lambda, ma non prevediamo di introdurre nuove funzionalità.

Esistono diversi servizi e progetti alternativi che consentono di modificare ed elaborare i dati a cui si accede da S3 per soddisfare le esigenze di varie applicazioni client o utenti che accedono ai dati. Queste alternative includono la AWS Solution Dynamic Image Transformation for Amazon CloudFront, che richiama AWS Lambda con altri mezzi (tramite CloudFront API Gateway o URL di funzioni) o elabora i dati nell'applicazione client. Tutte queste alternative continuano a utilizzare Amazon S3 per l'archiviazione sottostante, quindi non è necessaria la migrazione dei dati.

In questa sezione viene illustrato come scegliere l'opzione migliore per il proprio caso d'uso.

Trasformazione dinamica delle immagini per Amazon CloudFront

Questa AWS soluzione consente l'elaborazione delle immagini in tempo reale tramite la rete globale di distribuzione dei contenuti (CDN) di Amazon CloudFront utilizzando API Gateway e Lambda. Supporta una varietà di trasformazioni, come le modifiche al formato, le dimensioni, i metodi di adattamento, le rotazioni e i filtri. Se già utilizzi Lambda per oggetti S3 per la trasformazione delle immagini, questa soluzione può essere una buona alternativa. La [panoramica della soluzione](#) contiene maggiori dettagli sulle funzionalità e su come iniziare a utilizzarla. Assicurati di modificare il parametro del modello Abilita Lambda per oggetti S3 su "No" quando implementi la soluzione nell'account.

Per ulteriori informazioni, consulta [Dynamic Image Transformation for Amazon. CloudFront](#)

Elaborazione dei dati in AWS Lambda

Puoi continuare a utilizzarli AWS Lambda per il trattamento dei tuoi dati, ma richiamarli direttamente o tramite altri AWS servizi. La logica di elaborazione dei dati può rimanere uguale, ma la funzione Lambda dovrà essere aggiornata in base al modo in cui si sceglie di invocarla. Questa opzione è ideale per casi d'uso quali l'oscuramento di dati sensibili e le modifiche di formato o per le situazioni in cui l'applicazione che invoca Lambda per oggetti S3 si basa sulla ricezione di dati elaborati. Questa

opzione riduce al minimo anche le modifiche necessarie se si sceglie di migrare da Lambda per oggetti S3.

Se utilizzi un punto di accesso S3 Object Lambda come origine di una CloudFront distribuzione, puoi creare una nuova origine utilizzando gli URL della funzione Lambda o l'API Gateway. [Questo blog](#) spiega come configurare un URL di una funzione Lambda in modo che funga da origine per la distribuzione. CloudFront

Se attualmente si invoca direttamente Lambda per oggetti S3 dal codice client, è possibile utilizzare gli URL della funzione Lambda per invocare direttamente la funzione Lambda oppure è possibile utilizzare Gateway API. In caso di incertezza su quale sia il metodo migliore per il caso d'uso, consulta [Selezionare un metodo per invocare la funzione Lambda tramite una richiesta HTTP](#) nella Guida per gli sviluppatori di AWS Lambda . Dopo aver deciso quale metodo per invocare Lambda è il migliore per il caso d'uso in uso e aver configurato la funzione Lambda di conseguenza, è necessario anche aggiornare l'applicazione chiamante per invocare la funzione Lambda anziché chiamare Lambda per oggetti S3.

Elaborazione dei dati nell'applicazione client

È anche possibile spostare la logica di elaborazione dei dati da Lambda per oggetti S3 all'applicazione client. Questo approccio funziona meglio se si utilizza Lambda per oggetti S3 come parte di un'applicazione che già esegue ulteriori elaborazioni o analisi dei dati restituiti da Lambda per oggetti S3. Ad esempio, se il punto di accesso Lambda per oggetti S3 era responsabile del reindirizzamento a particolari oggetti o versioni di oggetti, tale logica di reindirizzamento può essere spostata nell'applicazione chiamante che quindi accede direttamente ai dati nel bucket S3.

Se hai bisogno di assistenza o desideri comunicare un feedback, contatta il [Supporto AWS](#).

Nozioni di base su Amazon S3

Puoi iniziare con Amazon S3 lavorando con bucket e oggetti. Un bucket è un container per oggetti o file. Un oggetto è un file e tutti i metadati che descrivono tale file.

Per memorizzare un oggetto in Amazon S3, crei un bucket e quindi carichi l'oggetto in un bucket. Quando l'oggetto si trova nel bucket, è possibile aprirlo, scaricarlo e spostarlo. Quando non hai più bisogno di un oggetto o di un bucket, puoi ripulire le tue risorse.

Con Amazon S3 paghi solo per le risorse utilizzate. Per ulteriori informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Amazon S3](#). Se sei un nuovo cliente Amazon S3, puoi iniziare a utilizzare Amazon S3 gratuitamente. Per ulteriori informazioni, consulta [Piano gratuito AWS](#).

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Video: Nozioni di base su Amazon S3

[Guarda questo](#)

Prerequisiti

Prima di iniziare, devi accertarti di avere completato le fasi in [Configurazione di Amazon S3](#).

Configurazione di Amazon S3

Quando ti iscrivi AWS, ti iscrivi Account AWS automaticamente a tutti i servizi in AWS, incluso Amazon S3. Ti vengono addebitati solo i servizi che utilizzi.

Con Amazon S3 paghi solo per le risorse utilizzate. Per ulteriori informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Amazon S3](#). Se sei un nuovo cliente Amazon S3, puoi iniziare a utilizzare Amazon S3 gratuitamente. Per ulteriori informazioni, consulta [Piano gratuito AWS](#).

Per configurare Amazon S3, segui la procedura descritta nelle sezioni seguenti.

Quando ti registri AWS e configuri Amazon S3, puoi facoltativamente cambiare la lingua di visualizzazione in. Console di gestione AWS Per ulteriori informazioni, consulta [Modifica della lingua della Console di gestione AWS](#) nella Guida introduttiva di Console di gestione AWS .

Argomenti

- [Registrati per un Account AWS](#)

Registrati per un Account AWS

Per iniziare AWS, hai bisogno di un Account AWS. Per informazioni sulla creazione di un Account AWS, vedere Guida [introduttiva a Account AWS](#) nella Guida Gestione dell'account AWS di riferimento.

Fase 1: creare il primo bucket S3

Dopo esserti registrato AWS, sei pronto per creare un bucket in Amazon S3 utilizzando. Console di gestione AWS Ogni oggetto in Amazon S3 viene archiviato in un bucket. Prima di poter archiviare dati in Amazon S3, devi creare un bucket.

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Note

Non è previsto alcun addebito per la creazione di un bucket. Vengono addebitati solo i costi per lo storage degli oggetti nel bucket e per il trasferimento degli oggetti all'interno e all'esterno del bucket. I costi che vengono addebitati sulla base agli esempi riportati nella seguente guida sono minimi (meno di \$1). Per ulteriori informazioni sui costi di storage, consulta [Prezzi di Amazon S3](#).

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare un bucket.

Note

- Una volta creato, non è possibile modificarne la regione.
- Scegli una regione nelle tue vicinanze per ridurre al minimo la latenza e i costi o essere conforme ai requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione. Per un elenco di Amazon S3 Regioni AWS, consulta gli [Servizio AWS endpoint](#) in. Riferimenti generali di Amazon Web Services

3. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
4. Scegliere Create bucket (Crea bucket). Viene visualizzata la pagina Create bucket (Crea bucket).
5. In Nome bucket, immettere il nome del bucket.

Il nome del bucket deve:

- Essere univoco all'interno di una partizione. Una partizione è un raggruppamento di regioni. AWS attualmente ha tre partizioni: aws (regioni commerciali), aws-cn (regioni cinesi) e aws-us-gov (AWS GovCloud (US) Regions).
- Deve contenere da 3 a 63 caratteri
- Essere costituito solo da lettere minuscole, numeri, punti (.) e trattini (-). Per una migliore compatibilità, è consigliabile evitare l'utilizzo di punti (.) nei nomi dei bucket, ad eccezione dei bucket utilizzati solo per l'hosting di siti web statici.
- Iniziare e finire con una lettera o un numero.
- Per l'elenco completo delle regole di denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#).

Important

- Una volta creato il bucket, non è possibile modificarne il nome.
- Non includere informazioni sensibili nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

6. (Facoltativo) In Configurazione generale è possibile scegliere di copiare le impostazioni di un bucket esistente nel nuovo bucket. Se non desideri copiare le impostazioni di un bucket esistente, procedi al passaggio successivo.

 Note

Questa opzione:

- Non è disponibile nella AWS CLI ed è disponibile solo nella console Amazon S3
- Non copia la policy di bucket dal bucket esistente nel nuovo bucket

Per copiare le impostazioni di un bucket esistente, in Copia impostazioni da un bucket esistente, seleziona Scegli bucket. Viene visualizzata la finestra Scegli bucket. Individua il bucket con le impostazioni da copiare e seleziona Scegli bucket. La finestra Scegli bucket si chiude e si riapre la finestra Crea bucket.

In Copia impostazioni da un bucket esistente, ora viene visualizzato il nome del bucket selezionato. Le impostazioni del nuovo bucket ora corrispondono alle impostazioni del bucket selezionato. Se desideri rimuovere le impostazioni copiate, scegli Ripristina le impostazioni predefinite. Esamina le restanti impostazioni del bucket nella pagina Crea bucket. Se non desideri apportare modifiche, puoi passare alla fase finale.

7. Alla voce Proprietà oggetto, per disabilitare o abilitare le ACL e controllare la proprietà degli oggetti caricati nel bucket, scegliere una delle seguenti impostazioni:

ACL disabilitate

- Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket ha automaticamente il controllo completo di ogni oggetto di proprietà nel bucket per uso generico. Le liste di controllo degli accessi (ACL) non influiscono più sulle autorizzazioni di accesso ai dati nel bucket per uso generico S3. Il bucket utilizza esclusivamente le policy per definire il controllo degli accessi.

Per impostazione predefinita, le ACL sono disabilitate. La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne in circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

ACL abilitati

- Proprietario del bucket preferito - Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono sul bucket con l'ACL `bucket-owner-full-control` predefinita.

Se applichi l'impostazione Proprietario del bucket preferito, per richiedere che tutti i caricamenti di Amazon S3 includano l'ACL predefinita `bucket-owner-full-control`, puoi [aggiungere una policy del bucket](#) che consenta solo il caricamento di oggetti che utilizzano questa ACL.

- Autore di oggetti: chi carica un oggetto possiede l'oggetto, ne ha il pieno controllo e può concedere ad altri utenti l'accesso ad esso tramite ACL. Account AWS

Note

L'impostazione predefinita è Proprietario del bucket applicato. Per applicare l'impostazione predefinita e mantenere gli ACL disabilitati, è necessaria solo l'autorizzazione `s3:CreateBucket`. Per abilitare gli ACL, è necessario disporre dell'autorizzazione `s3:PutBucketOwnershipControls`.

8. In Impostazioni di blocco dell'accesso pubblico per questo bucket scegli le impostazioni di blocco dell'accesso pubblico che vuoi applicare al bucket.

Per impostazione predefinita, tutte e quattro le impostazioni Blocco dell'accesso pubblico sono abilitate. È consigliabile mantenere tutte le impostazioni abilitate, a meno che non sia necessario disattivarne una o più di una per il caso d'uso specifico. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Note

Per abilitare tutte le impostazioni Blocco dell'accesso pubblico, è richiesta solo l'autorizzazione `s3:CreateBucket`. Per disattivare le impostazioni Blocco dell'accesso pubblico, è necessario disporre dell'autorizzazione `s3:PutBucketPublicAccessBlock`.

9. (Facoltativo) Per impostazione predefinita, la funzionalità Controllo delle versioni del bucket è disabilitata. La funzione Controllo delle versioni è un modo per conservare più versioni di un oggetto nello stesso bucket. Si può utilizzare questa funzione per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket. Con il controllo delle versioni puoi eseguire facilmente il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Per abilitare il controllo delle versioni sul bucket, scegli Abilita.

10. (Facoltativo) In Tags (Tag), puoi scegliere di aggiungere tag al bucket. Con l'allocazione dei costi di AWS è possibile utilizzare i tag dei bucket per annotare nella fatturazione l'utilizzo di un bucket. Un tag è una coppia chiave-valore che rappresenta un'etichetta assegnata a un bucket. Per ulteriori informazioni, consulta [the section called "Utilizzo dei tag per l'allocazione dei costi"](#).

Per aggiungere un tag al bucket, inserisci un valore in Key (Chiave) e facoltativamente un valore in Value (Valore), quindi scegli Add Tag (Aggiungi tag).

11. Per configurare Crittografia predefinita, in Tipo di crittografia scegli una delle seguenti opzioni:
- Server-side crittografia con chiavi gestite da Amazon S3 () SSE-S3
 - Server-side crittografia con AWS Key Management Service chiavi () SSE-KMS
 - Dual-layer crittografia lato server con chiavi AWS Key Management Service (AWS KMS) () DSSE-KMS

 Important

Se si utilizza l' DSSE-KMS opzione SSE-KMS or per la configurazione di crittografia predefinita, si è soggetti alla quota di richieste al secondo (RPS) di AWS KMS. Per ulteriori informazioni sulle AWS KMS quote e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli AWS Key Management Service sviluppatori.

I bucket e i nuovi oggetti sono crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) come livello base di configurazione della crittografia. Per ulteriori informazioni sulla crittografia predefinita, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#). Per ulteriori informazioni su SSE-S3, consultare [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).

Per ulteriori informazioni sull'utilizzo della crittografia lato server per crittografare i dati, consulta [the section called “Crittografia dei dati”](#).

12. Se hai scelto Server-side la crittografia con AWS Key Management Service chiavi (SSE-KMS) o la Dual-layer crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (DSSE-KMS), procedi come segue:

- a. In Chiave AWS KMS specifica la tua chiave KMS in uno dei seguenti modi:

- Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS keys e scegli la tua chiave KMS dall'elenco delle chiavi disponibili.

Sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente vengono visualizzate in questo elenco. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per specificare l'ARN della chiave KMS, scegli Inserisci l'ARN della AWS KMS key e quindi specifica l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

Important

È possibile utilizzare solo le chiavi KMS disponibili nello Regione AWS stesso bucket. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, è necessario inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione richiesta per l'uso della chiave e quindi inserire l'ARN della chiave KMS. Per ulteriori informazioni sulle autorizzazioni multi-account per le chiavi KMS, consulta [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service . Per ulteriori informazioni su SSE-KMS, consulta. [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#) Per ulteriori informazioni su

DSSE-KMS, vedere [the section called “Dual-layer crittografia lato server \(\) DSSE-KMS”](#).

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- b. Quando configuri il bucket per utilizzare la crittografia predefinita con SSE-KMS, puoi anche utilizzare S3 Bucket Keys. Le chiavi S3 Bucket riducono il costo della crittografia diminuendo il traffico di richieste da Amazon S3 a AWS KMS. Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#). Le chiavi S3 Bucket non sono supportate per DSSE-KMS.

Per impostazione predefinita, le chiavi del bucket S3 sono abilitate nella console Amazon S3. È consigliabile lasciare abilitate le chiavi del bucket S3 per ridurre i costi. Per disabilitare le chiavi del bucket S3 per il bucket in uso, scegli Disabilita in Chiave del bucket.

- 13. (Facoltativo) Object Lock S3 aiuta a proteggere i nuovi oggetti dall'eliminazione o dalla sovrascrittura. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#). Se desideri abilitare Object Lock S3, procedi come segue:

- a. Scegli Impostazioni avanzate.

 Important

Abilitando Object Lock si abilita automaticamente il controllo delle versioni per il bucket. Dopo aver abilitato e creato il bucket, è necessario anche configurare le impostazioni predefinite di conservazione e blocco legale di Object Lock nella scheda Proprietà del bucket.

- b. Se desideri attivare Object Lock, scegli Abilita, leggi l'avviso che appare e confermallo.

 Note

Per creare un bucket abilitato per Object Lock, sono necessarie le seguenti autorizzazioni: `s3:CreateBucket`, `s3:PutBucketVersioning` e `s3:PutBucketObjectLockConfiguration`.

14. Scegliere Create bucket (Crea bucket).

È stato creato un bucket in Amazon S3.

Approfondimenti

Per aggiungere un oggetto al bucket, consulta [Fase 2: Carica un oggetto nel tuo bucket](#).

Fase 2: Carica un oggetto nel tuo bucket

Dopo aver creato un bucket in Amazon S3, sei pronto per caricare un oggetto nel bucket. Un oggetto può essere qualsiasi tipo di file: file di testo, immagine, video e così via.

 Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Per caricare un oggetto in un bucket

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket seleziona il nome del bucket in cui desideri caricare l'oggetto.
3. Nella scheda Oggetti del bucket seleziona Carica.
4. In File e cartelle, seleziona Aggiungi file.
5. Seleziona un file da caricare, quindi scegli Apri.
6. Scegli Carica.

Hai caricato correttamente un oggetto nel bucket.

Approfondimenti

Per visualizzare l'oggetto, consulta [Fase 3: download di un oggetto](#).

Fase 3: download di un oggetto

Dopo avere caricato un oggetto in un bucket, è possibile visualizzare le informazioni sull'oggetto e scaricare l'oggetto nel computer locale.

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Utilizzo della console S3

In questa sezione viene illustrato come utilizzare la console Amazon S3 per scaricare un oggetto da un bucket S3.

Note

- Puoi scaricare un solo oggetto alla volta.
- Se utilizzi la console di Amazon S3 per scaricare un oggetto il cui nome della chiave termina con un punto (.), il punto viene rimosso dal nome della chiave dell'oggetto scaricato. Per mantenere il punto alla fine del nome dell'oggetto scaricato, devi utilizzare AWS Command Line Interface (AWS CLI), AWS SDK o l'API REST di Amazon S3.

Per scaricare un oggetto da un bucket S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.

3. Nell'elenco dei bucket scegli il nome del bucket dal quale desideri scaricare un oggetto.
4. È possibile scaricare un oggetto da un bucket S3 in uno qualsiasi dei modi seguenti:
 - Seleziona la casella di controllo accanto all'oggetto e scegli Scarica. Se desideri scaricare l'oggetto in una cartella specifica, nel menu Azioni, scegli Scarica come.
 - Se desideri scaricare una versione specifica dell'oggetto, attiva Mostra versioni (che si trova accanto alla casella di ricerca). Seleziona la casella di controllo accanto alla versione dell'oggetto desiderato e scegli Scarica. Se desideri scaricare l'oggetto in una cartella specifica, nel menu Azioni, scegli Scarica come.

Hai scaricato correttamente il tuo oggetto.

Approfondimenti

Per copiare e incollare il tuo oggetto in Amazon S3, consulta [Fase 4: copiare l'oggetto in una cartella](#).

Fase 4: copiare l'oggetto in una cartella

Hai aggiunto un oggetto a un bucket e hai scaricato l'oggetto. Ora, crei una cartella e copi l'oggetto, quindi lo incolli nella cartella.

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Per copiare un oggetto in una cartella

1. Nell'elenco Buckets (Bucket), scegliere il nome del bucket.
2. Scegliere Create folder (Crea cartella) e configurare una nuova cartella:
 - a. Immettere un nome di cartella (ad esempio, favorite-pics).
 - b. Per le impostazioni di crittografia della cartella, scegliere Disable (Disabilita).
 - c. Selezionare Salva.

3. Accedere al bucket o alla cartella Amazon S3 che contiene gli oggetti da copiare.
4. Selezionare la casella di controllo a sinistra dei nomi degli oggetti da copiare.
5. Scegliere Actions (Operazioni) e quindi Copy (Copia) nell'elenco di opzioni visualizzato.

In alternativa, scegli **Copia** tra le opzioni visualizzate.

6. Scegliere la cartella di destinazione:
 - a. Seleziona Sfoglia S3.
 - b. Scegliere il pulsante di opzione a sinistra del nome della cartella.

Per passare a un'altra cartella e scegliere una sottocartella come destinazione, scegliere il nome della cartella.

- c. Scegliere Choose destination (Scegli destinazione).

Il percorso della cartella di destinazione viene visualizzato nella casella Destination (Destinazione). In Destinazione, puoi inserire alternativamente il percorso di destinazione, ad esempio `s3:///bucket-name/. folder-name`

7. Scegli Copia.

Amazon S3 copia gli oggetti nella cartella di destinazione.

Approfondimenti

Per eliminare un oggetto e un bucket in Amazon S3, consulta [Fase 5: eliminare gli oggetti e il bucket](#).

Fase 5: eliminare gli oggetti e il bucket

Quando non hai più bisogno di un oggetto o di un bucket, ti consigliamo di eliminarlo per evitare ulteriori addebiti. Se hai completato questa procedura dettagliata iniziale come esercizio di apprendimento e non hai intenzione di utilizzare il bucket o gli oggetti, ti consigliamo di eliminare il bucket in modo che non si accumulino più addebiti.

Prima di eliminare il bucket, devi svuotare il bucket o eliminare gli oggetti nel bucket. Una volta eliminati gli oggetti e il bucket non sono più disponibili.

Se desideri continuare a utilizzare lo stesso nome di bucket, è consigliabile eliminare gli oggetti o svuotare il bucket senza eliminarlo. Dopo aver eliminato un bucket, il nome diventa disponibile per il

riutilizzo. Tuttavia, un altro Account AWS potrebbe creare un bucket con lo stesso nome prima che tu abbia la possibilità di riutilizzarlo.

Note

Per ulteriori informazioni sull'uso della classe di storage Amazon S3 Express One Zone con i bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Argomenti

- [Eliminazione di un oggetto](#)
- [Svuotamento del bucket](#)
- [Eliminazione del bucket](#)

Eliminazione di un oggetto

Se desideri scegliere quali oggetti eliminare senza svuotare tutti gli oggetti dal bucket, puoi eliminare un oggetto.

1. Nell'elenco Buckets (Bucket) scegliere il nome del bucket dal quale si desidera eliminare un oggetto.
2. Seleziona l'oggetto da eliminare.
3. Scegli **Elimina** tra le opzioni visualizzate.
4. Nella pagina Elimina oggetti, digita **delete** per confermare l'eliminazione degli oggetti.
5. Scegliere Delete objects (Elimina oggetti).

Svuotamento del bucket

Se pensi di eliminare il bucket, devi prima svuotarlo, eliminando così tutti gli oggetti nel bucket.

Per svuotare un bucket

1. Nell'elenco Buckets (Bucket) selezionare il bucket che si desidera svuotare e quindi scegliere Empty (Svuota).

2. Per confermare che si desidera svuotare il bucket ed eliminare tutti gli oggetti in esso contenuti, in Svuota bucket, digita **permanently delete**.

 Important

Lo svuotamento del bucket non può essere annullato. Gli oggetti aggiunti al bucket mentre l'azione di svuotamento del bucket è in corso verranno eliminati.

3. Per svuotare il bucket ed eliminare tutti gli oggetti in esso contenuti, scegliere Empty (Svuota).

Viene visualizzata la pagina sullo stato dello svuotamento del bucket che è possibile utilizzare per esaminare un riepilogo delle eliminazioni di oggetti non riuscite e riuscite.

4. Per tornare all'elenco dei bucket, scegliere Exit (Esci).

Eliminazione del bucket

Dopo aver svuotato il bucket o eliminato tutti gli oggetti dal bucket, è possibile eliminarlo.

1. Per eliminare un bucket, nell'elenco Buckets (Bucket) selezionare il bucket.
2. Scegliere Elimina.
3. Per confermare l'eliminazione, in Elimina bucket, specifica il nome del bucket.

 Important

L'eliminazione di un bucket non può essere annullata. I nomi dei bucket sono univoci. Se elimini il bucket, un altro AWS utente può utilizzare il nome. Se desideri continuare a utilizzare lo stesso nome di bucket, non eliminare il bucket. Invece, svuota il bucket e conservalo.

4. Per eliminare il bucket, scegliere Delete bucket (Elimina bucket).

Fasi successive

Negli esempi precedenti hai imparato a eseguire alcuni processi di base di Amazon S3.

I seguenti argomenti illustrano i percorsi di apprendimento che puoi sfruttare per acquisire una maggiore conoscenza di Amazon S3 in modo da implementarlo nelle tue applicazioni.

 Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Argomenti

- [Conoscere i casi d'uso comuni](#)
- [Controllo dell'accesso a bucket e oggetti](#)
- [Proteggere e monitorare lo storage](#)
- [Sviluppo con Amazon S3](#)
- [Informazioni sui tutorial](#)
- [Esplora la formazione e il supporto](#)

Conoscere i casi d'uso comuni

Puoi utilizzare Amazon S3 per supportare il tuo caso d'uso specifico. La [AWS Libreria di soluzioni](#) e il [Blog AWS](#) forniscono informazioni e tutorial specifici per i casi d'uso. Di seguito sono elencati alcuni casi d'uso comuni per Amazon S3:

- Backup e archiviazione – Utilizza le caratteristiche di gestione dell'archiviazione di Amazon S3 per gestire i costi, soddisfare i requisiti normativi, ridurre la latenza e salvare più copie distinte dei dati per i requisiti di conformità.
- Hosting di applicazioni: distribuisce, installa e gestisci applicazioni Web affidabili, altamente scalabili e a basso costo. Per esempio, è possibile configurare il bucket di Amazon S3 per l'hosting di siti Web statici. Per ulteriori informazioni, consulta [Hosting di un sito Web statico tramite Amazon S3](#).
- Hosting di file multimediali: crea un'infrastruttura ad alta disponibilità per l'hosting di video, foto o per caricare e scaricare file musicali.
- Distribuzione di software: esegui l'hosting di applicazioni software che i clienti possono scaricare.

Controllo dell'accesso a bucket e oggetti

Amazon S3 offre una varietà di funzionalità e strumenti di sicurezza. Per una panoramica, consulta [Controllo degli accessi in Amazon S3](#).

Per impostazione predefinita, i bucket S3 e gli oggetti al loro interno sono privati. Puoi accedere solo alle risorse S3 che hai creato. Puoi utilizzare le seguenti caratteristiche per concedere autorizzazioni granulari delle risorse che supportano il tuo caso d'uso specifico o per verificare le autorizzazioni delle tue risorse Amazon S3.

- [Blocco dell'accesso pubblico di S3](#): blocca l'accesso pubblico a bucket S3 e oggetti. Per impostazione predefinita, le impostazioni Blocco dell'accesso pubblico sono attivate a livello di bucket.
- [AWS Identity and Access Management Identità \(IAM\)](#): utilizza IAM o Centro identità AWS IAM crea identità IAM nelle tue Account AWS per gestire l'accesso alle tue risorse Amazon S3. Ad esempio, puoi utilizzare IAM con Amazon S3 per controllare il tipo di accesso di un utente o gruppo di utenti a un bucket Amazon S3 di tua proprietà. Account AWS Per ulteriori informazioni sulle identità IAM e sulle best practice, consulta [Identità IAM \(utenti, gruppi di utenti e ruoli\)](#) nella Guida per l'utente di IAM.
- [Policy dei bucket](#): utilizza il linguaggio delle IAM-based policy per configurare le autorizzazioni basate sulle risorse per i bucket S3 e gli oggetti in essi contenuti.
- [Liste di controllo degli accessi \(ACL\)](#): concedi autorizzazioni di lettura e scrittura per singoli bucket e oggetti agli utenti autorizzati. Come regola generale, è consigliabile utilizzare policy basate sulle risorse S3 (policy di bucket e policy dei punti di accesso) o policy utente IAM per il controllo degli accessi anziché ACL. Le policy sono un'opzione di controllo degli accessi semplificata e più flessibile. Con le policy di bucket e le policy dei punti di accesso, è possibile definire regole valide globalmente per tutte le richieste alle risorse Amazon S3. Per ulteriori informazioni su casi specifici quando desideri utilizzare le ACL anziché le policy basate sulle risorse o le policy utente IAM, consultare [Identity and Access Management per Amazon S3](#).
- [S3 Proprietà dell'oggetto](#): consente di assumere la proprietà di ogni oggetto nel bucket, semplificando la gestione degli accessi per i dati archiviati in Amazon S3. S3 Proprietà dell'oggetto è un'impostazione a livello di bucket di Amazon S3 che puoi utilizzare per disabilitare o abilitare le ACL. Per impostazione predefinita, le ACL sono disabilite. Con le ACL disabilite, il proprietario del bucket possiede tutti gli oggetti nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy di gestione dell'accesso.
- [IAM Access Analyzer per S3](#): valuta e monitora le policy di accesso al bucket S3, assicurando che forniscano solo l'accesso previsto alle risorse S3.

Proteggere e monitorare lo storage

- [Protezione dello storage](#): dopo aver creato i bucket e caricato gli oggetti in Amazon S3, è possibile proteggere lo storage degli oggetti. Ad esempio, puoi utilizzare i controlli di failover S3 Versioning, S3 Replication e Multi-Region Access Point per il disaster recovery, per eseguire il backup dei dati e S3 Object Lock per impostare i periodi di conservazione, prevenire eliminazioni e sovrascritture e soddisfare i requisiti di conformità. AWS Backup
- [Monitoraggio dello storage](#): il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità e delle prestazioni di Amazon S3 e delle tue soluzioni. AWS Puoi monitorare l'attività e i costi di archiviazione. È consigliabile raccogliere i dati sul monitoraggio da tutte le parti della soluzione AWS per consentire un debug più facile di eventuali guasti in più punti.

È inoltre possibile utilizzare analisi e informazioni dettagliate in Amazon S3 per comprendere, analizzare e ottimizzare l'utilizzo dello storage. Ad esempio, utilizza [Amazon S3 Storage Lens](#) per comprendere, analizzare e ottimizzare l'archiviazione. S3 Storage Lens fornisce oltre 29 parametri di utilizzo e attività e dashboard interattivi per aggregare i dati per l'intera organizzazione, account specifici, regioni, bucket o prefissi. Utilizza l'[analisi della classe di archiviazione](#) per analizzare i modelli di accesso all'archiviazione e decidere quando è il momento di spostare i dati in una classe di archiviazione più conveniente. Per gestire i costi, è possibile utilizzare il [ciclo di vita S3](#).

Sviluppo con Amazon S3

Amazon S3 è un servizio REST. Puoi inviare richieste ad Amazon S3 utilizzando l'API REST o le librerie AWS SDK, che racchiudono l'API REST di Amazon S3 sottostante, semplificando le attività di programmazione. Puoi anche utilizzare AWS Command Line Interface (AWS CLI) per effettuare chiamate API Amazon S3. Per ulteriori informazioni, consulta [Esecuzione di richieste](#) nella documentazione di riferimento delle API Amazon S3.

L'API REST Amazon S3 è un'interfaccia HTTP per Amazon S3. Con l'API REST, utilizzi le richieste HTTP standard per creare, recuperare ed eliminare bucket e oggetti. Per utilizzare l'API REST, puoi servirti di qualunque kit di strumenti in grado di supportare HTTP. Puoi anche utilizzare un browser per recuperare gli oggetti, purché siano leggibili in modo anonimo. Per ulteriori informazioni, consulta [Sviluppo con Amazon S3](#) nella documentazione di riferimento delle API Amazon S3.

Per ottenere aiuto nella creazione di applicazioni mediante il linguaggio preferito, puoi fare riferimento alle seguenti risorse.

AWS CLI

Puoi accedere alle caratteristiche di Amazon S3 utilizzando AWS CLI. Per scaricare e configurare l'API AWS CLI, consulta [Sviluppo con Amazon S3 utilizzando l'interfaccia a riga di comando](#) nell'API AWS Reference di Amazon S3.

AWS CLI Fornisce due livelli di comandi per accedere ad Amazon S3: comandi (s3) e High-level (s3api e comandi). API-level <https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-apicommands.html> s3control I comandi S3 di livello alto semplificano le operazioni di uso frequente, ad esempio la creazione, la modifica e l'eliminazione di oggetti e bucket. I comandi s3api e s3control espongono l'accesso diretto a tutte le operazioni tramite API di Amazon S3, che puoi utilizzare per eseguire operazioni avanzate che potrebbero non essere possibili solo con i comandi di livello alto.

Per un elenco dei AWS CLI comandi Amazon S3, consulta s3, s3api e <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3/index.html> s3control. <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/index.html> <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3control/index.html>

AWS SDK ed Explorer

Puoi utilizzare gli AWS SDK per sviluppare applicazioni con Amazon S3. Tali SDK AWS semplificano le attività di programmazione tramite il wrapping dell'API REST sottostante. Gli SDK AWS per dispositivi mobili e la JavaScript libreria Amplify sono disponibili anche per la creazione di applicazioni mobili e web connesse utilizzando AWS.

Oltre agli AWS SDK, sono disponibili AWS Explorer per Visual Studio ed Eclipse per Java IDE. In questo caso, gli SDK e gli explorer sono raggruppati come Toolkit. AWS

Per ulteriori informazioni, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Librerie e codice di esempio

Il [Centro Developer di AWS](#) e il [Catalogo dei codici di esempio di AWS](#) contengono codici di esempio e librerie compilati appositamente per Amazon S3. È possibile utilizzare tali codici di esempio per comprendere le modalità di implementazione dell'API di Amazon S3. Puoi anche visualizzare l'[Documentazione di riferimento delle API di Amazon Simple Storage Service](#) per comprendere in dettaglio le operazioni API di Amazon S3.

Informazioni sui tutorial

Puoi usare i tutorial e le esercitazioni dettagliate per imparare a usare Amazon S3. I tutorial presentati sono solo esempi con nomi di società e utenti fittizi destinati a essere usati in un ambiente di laboratorio. Il loro scopo è di fornire linee guida di carattere generico. Non devono essere utilizzati direttamente nell'ambiente di produzione, senza un'accurata opera di revisione e adattamento alle necessità esclusive del tuo ambiente lavorativo.

Nozioni di base

- [Tutorial: Archiviazione e recupero di file con Amazon S3](#)
- [Tutorial: Guida introduttiva a S3 Intelligent-Tiering](#)
- [Tutorial: Nozioni di base sull'utilizzo delle classi di archiviazione di S3 Glacier](#)

Ottimizzazione dei costi di archiviazione

- [Tutorial: Guida introduttiva a S3 Intelligent-Tiering](#)
- [Tutorial: Nozioni di base sull'utilizzo delle classi di archiviazione di S3 Glacier](#)
- [Tutorial: Ottimizzazione dei costi e acquisizione di visibilità sull'utilizzo con S3 Storage Lens](#)

Gestione dello storage

- [Tutorial: Guida introduttiva agli access point Amazon S3 Multi-Region](#)
- [Tutorial: Replicating existing objects in your Amazon S3 buckets with S3 Batch Replication](#) (Replica di oggetti esistenti nei bucket Amazon S3 con S3 Batch Replication)

Hosting di video e siti Web

- [Tutorial: Hosting di video in streaming su richiesta con Amazon S3 CloudFront, Amazon e Amazon Route 53](#)
- [Esercitazione: configurazione di un sito Web statico su Amazon S3](#)
- [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#)

Elaborazione di dati

- [Tutorial: trasformazione dei dati per l'applicazione con S3 Object Lambda](#)
- [Tutorial: rilevamento e oscuramento dei dati PII con S3 Object Lambda e Amazon Comprehend](#)
- [Tutorial: utilizzo di S3 Object Lambda per aggiungere filigrane alle immagini in modo dinamico man mano che vengono recuperate](#)
- [Tutorial: video con S3 Batch Operations Batch-transcoding](#)

Protezione dei dati

- [Tutorial: Verifica dell'integrità dei dati in Amazon S3 con checksum aggiuntivi](#)
- [Tutorial: Replica dei dati all'interno e tra di essi Regioni AWS utilizzando S3 Replication](#)
- [Tutorial: Protezione dei dati su Amazon S3 da eliminazioni accidentali o bug delle applicazioni mediante le funzionalità S3 di controllo delle versioni, blocco degli oggetti e replica](#)
- [Tutorial: Replicating existing objects in your Amazon S3 buckets with S3 Batch Replication](#) (Replica di oggetti esistenti nei bucket Amazon S3 con S3 Batch Replication)

Esplora la formazione e il supporto

Puoi imparare dagli AWS esperti per migliorare le tue competenze e ottenere assistenza da esperti per raggiungere i tuoi obiettivi.

- **Formazione:** le risorse per la formazione offrono un approccio pratico all'apprendimento di Amazon S3. Per ulteriori informazioni, consulta [AWS Training and Certification](#) e [colloqui tecnologici online di AWS](#).
- **Forum di discussione:** nel forum, puoi rivedere i post per capire quali sono le operazioni supportate da Amazon S3. Puoi anche pubblicare domande. Per ulteriori informazioni, consulta [Forum di discussione](#).
- **Supporto tecnico:** in caso di ulteriori domande, puoi contattare il [Supporto tecnico](#).

Guida introduttiva ad Amazon S3 utilizzando AWS CLI

Puoi iniziare a usare Amazon S3 utilizzando AWS Command Line Interface (AWS CLI) per lavorare con bucket e oggetti generici. Un bucket è un container per oggetti o file. Un oggetto è un file e tutti i metadati che descrivono tale file.

Per memorizzare un oggetto in Amazon S3, crei un bucket e quindi carichi l'oggetto in un bucket. Quando l'oggetto si trova nel bucket, è possibile aprirlo, scaricarlo e spostarlo. Quando non hai più bisogno di un oggetto o di un bucket, puoi ripulire le tue risorse.

Con Amazon S3 paghi solo per le risorse utilizzate. Per ulteriori informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Amazon S3](#). Se sei un nuovo cliente Amazon S3, puoi iniziare a utilizzare Amazon S3 gratuitamente. Per ulteriori informazioni, consulta [Piano gratuito AWS](#).

Note

Per ulteriori informazioni sull'uso della classe di storage Amazon S3 Express One Zone con i bucket di directory, consulta [Esercitazione: nozioni di base su S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Configurazione

Prima di iniziare a utilizzarlo AWS CLI con Amazon S3, assicurati di avere:

- Hai creato un AWS account. Per istruzioni, consulta l'argomento [Configurazione di Amazon S3](#).
- Creazione di un utente con le autorizzazioni s3:*. Per istruzioni, consulta l'argomento [Configurazione di Amazon S3](#).
- Installato e configurato il AWS CLI. Per le istruzioni, consulta [Installazione o aggiornamento dell'ultima versione della AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface .

Per verificare che AWS CLI sia configurato correttamente, esegui il seguente comando:

```
aws sts get-caller-identity
```

Per ulteriori informazioni, consulta [get-caller-identity](#) nella documentazione di riferimento dei comandi della AWS CLI .

Questo comando visualizza un elenco dei comandi Amazon S3 disponibili se AWS CLI è installato e configurato correttamente.

Fase 1: creare il primo bucket Amazon S3

Dopo aver configurato AWS CLI, sei pronto per creare un bucket in Amazon S3. Ogni oggetto in Amazon S3 viene archiviato in un bucket. Prima di poter archiviare dati in Amazon S3, devi creare un bucket.

Note

Non è previsto alcun addebito per la creazione di un bucket. Vengono addebitati solo i costi per lo storage degli oggetti nel bucket e per il trasferimento degli oggetti all'interno e all'esterno del bucket. I costi che vengono addebitati sulla base agli esempi riportati nella seguente guida sono minimi (meno di \$1). Per ulteriori informazioni sui costi di storage, consulta [Prezzi di Amazon S3](#).

Per creare un bucket

1. Crea un bucket utilizzando il comando `s3api create-bucket`. Sostituisci *amzn-s3-demo-bucket* con un nome di bucket univoco e `us-east-1` con la Regione desiderata:

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1
```

Per le Regioni diverse da `us-east-1`, è necessario specificare il vincolo di posizione:

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-west-2 --create-bucket-configuration LocationConstraint=us-west-2
```

Note

- Una volta creato, non è possibile modificarne la regione.
- Scegli una regione nelle tue vicinanze per ridurre al minimo la latenza e i costi o essere conforme ai requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione. Per un elenco delle AWS regioni Amazon S3, consulta gli endpoint [AWS](#) di servizio in [Riferimenti generali di Amazon Web Services](#)
- Il nome del bucket deve:

- Essere univoco all'interno di una partizione. Una partizione è un raggruppamento di regioni. AWS attualmente ha tre partizioni: `aws` (Regioni commerciali), `aws-cn` (Regioni cinesi) e `aws-us-gov` (AWS GovCloud (US) Regioni).
- Deve contenere da 3 a 63 caratteri
- Essere costituito solo da lettere minuscole, numeri, punti (.) e trattini (-). Per una migliore compatibilità, è consigliabile evitare l'utilizzo di punti (.) nei nomi dei bucket, ad eccezione dei bucket utilizzati solo per l'hosting di siti web statici.
- Iniziare e finire con una lettera o un numero.
- Una volta creato il bucket, non è possibile modificarne il nome.
- Non includere informazioni sensibili nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

2. Verifica che il bucket sia stato creato elencando tutti i bucket:

```
aws s3 ls
```

3. Per [Proprietà dell'oggetto](#) è possibile disabilitare o abilitare le ACL e controllare la proprietà degli oggetti caricati nel bucket.

ACL disattivati

Per Proprietario del bucket applicato (impostazione predefinita), le ACL sono disabilitate e il proprietario del bucket diventa automaticamente il proprietario e ha il controllo completo di ogni oggetto nel bucket.

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

Note

Per impostazione predefinita, le ACL sono disabilitate. La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne in circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

ACL abilitati

- Per Proprietario del bucket preferito, il proprietario del bucket diventa il proprietario e ha il pieno controllo dei nuovi oggetti che altri account scrivono nel bucket con l'ACL `bucket-owner-full-control` predefinita.

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerPreferred}]"
```

Se si applica l'impostazione Proprietario del bucket preferito ed è necessario che tutti i caricamenti di Amazon S3 includano l'ACL `bucket-owner-full-control`, è possibile [Richiedere l'ACL predefinito con controllo completo dal proprietario del bucket per le operazioni PUT di Amazon S3 \(preferibilmente il proprietario del bucket\)](#) che consenta solo il caricamento di oggetti che utilizzano questa ACL.

- Per Autore dell'oggetto, l'account AWS che carica un oggetto ne diventa il proprietario, ne ha il pieno controllo e può concedere ad altri utenti l'accesso tramite ACL:

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=ObjectWriter}]"
```

Note

L'impostazione predefinita è Proprietario del bucket applicato. Per applicare l'impostazione predefinita e mantenere gli ACL disabilitati, è necessaria solo l'autorizzazione `s3:CreateBucket`. Per abilitare gli ACL, è necessario disporre dell'autorizzazione `s3:PutBucketOwnershipControls`.

Per verificare la corrente impostazione Proprietà dell'oggetto per il bucket:

```
aws s3api get-bucket-ownership-controls --bucket amzn-s3-demo-bucket
```

4. Per verificare che il Blocco dell'accesso pubblico sia abilitato (è abilitato per impostazione predefinita per i nuovi bucket):

```
aws s3api get-public-access-block --bucket amzn-s3-demo-bucket
```

Per impostazione predefinita, tutte e quattro le impostazioni Blocca accesso pubblico sono abilitate per i nuovi bucket. È consigliabile mantenere tutte le impostazioni abilitate, a meno che non sia necessario disattivarne una o più di una per il caso d'uso specifico. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Per abilitare Blocca accesso pubblico, utilizza il seguente comando:

```
aws s3api put-public-access-block --bucket amzn-s3-demo-bucket --public-access-block-configuration "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true"
```

Note

Per abilitare tutte le impostazioni Blocco dell'accesso pubblico, è richiesta solo l'autorizzazione `s3:CreateBucket`. Per disattivare le impostazioni Blocco dell'accesso pubblico, è necessario disporre dell'autorizzazione `s3:PutBucketPublicAccessBlock`.

5. Per abilitare il controllo delle versioni per il bucket:

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket --versioning-configuration Status=Enabled
```

Per impostazione predefinita, la funzione Controllo delle versioni per il bucket è disabilitata. La funzione Controllo delle versioni è un modo per conservare più versioni di un oggetto nello stesso bucket. Si può utilizzare questa funzione per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket. Con il controllo delle versioni puoi eseguire facilmente il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

6. Amazon S3 Object Lock protegge i nuovi oggetti dall'eliminazione o dalla sovrascrittura. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#). Per abilitare [Blocco di oggetti con Object Lock](#) (richiede il controllo delle versioni del bucket):

Per un nuovo bucket:

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1 --object-lock-enabled-for-bucket
```

Per un bucket esistente:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket --object-lock-configuration '{"ObjectLockEnabled": "Enabled"}'
```

Per impostare un [Blocco di oggetti con Object Lock](#) predefinito e abilitare Object Lock, puoi utilizzare:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket --object-lock-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {"DefaultRetention": {"Mode": "COMPLIANCE", "Days": 30}}}'
```

È possibile sostituire "COMPLIANCE" con "GOVERNANCE" per una modalità meno restrittiva e regolare il numero di giorni in base alle esigenze.

Note

Per creare un bucket abilitato per Object Lock, sono necessarie le seguenti autorizzazioni: `s3:CreateBucket`, `s3:PutBucketVersioning` e `s3:PutBucketObjectLockConfiguration`.

7. È possibile aggiungere tag al bucket. Con l'allocazione AWS dei costi, puoi utilizzare i bucket tag per annotare la fatturazione relativa all'utilizzo di un bucket. Un tag è una coppia chiave-valore che rappresenta un'etichetta assegnata a un bucket. Per ulteriori informazioni, consulta [Utilizzo dei tag per l'allocazione dei costi per i bucket S3](#).

Per aggiungere tag al bucket:

```
aws s3api put-bucket-tagging --bucket amzn-s3-demo-bucket --tagging 'TagSet=[{Key=Purpose,Value=Testing},{Key=Environment,Value=Development}]'
```

8. I bucket e i nuovi oggetti sono crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) come livello base di configurazione della crittografia. Per verificare la crittografia predefinita del bucket, utilizza il seguente comando:

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket
```

Puoi anche configurare la crittografia lato server con AWS KMS chiavi (SSE-KMS) e la crittografia lato server a doppio livello con chiavi () per il tuo bucket. AWS KMS DSSE-KMS Sia la chiave AWS gestita (aws/s3) che le chiavi gestite dal cliente possono essere utilizzate come chiave per la configurazione della crittografia. AWS KMS SSE-KMS DSSE-KMS Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta Chiavi e AWS chiavi del [cliente](#) nella Guida per gli AWS Key Management Service sviluppatori. Per ulteriori informazioni sulla creazione di una chiave AWS KMS , consulta [Creazione di chiavi](#) nella Guida per gli sviluppatori di AWS Key Management Service .

 Important

La AWS KMS chiave deve trovarsi nella stessa AWS regione del bucket Amazon S3. Cross-region Le chiavi KMS non sono supportate per la crittografia dei bucket Amazon S3.

Quando configuri il bucket per utilizzare la crittografia predefinita con SSE-KMS, puoi anche utilizzare Amazon S3 Bucket Keys. Le chiavi Amazon S3 Bucket riducono il costo della crittografia diminuendo il traffico di richieste da Amazon S3 a AWS KMS Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#). Le chiavi Bucket Amazon S3 non sono supportate per. DSSE-KMS In AWS CLI, le chiavi Amazon S3 Bucket NON sono abilitate per impostazione predefinita quando si crea un nuovo bucket. Questo comportamento è diverso da quello della console in cui sono abilitate per impostazione predefinita.

Per configurare SSE-KMS e abilitare le chiavi del bucket Amazon S3:

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgorithm":"aws:kms","KMSMasterKeyID":"YOUR-KMS-KEY-ARN"},"BucketKeyEnabled":true}]}'
```

Per verificare se le chiavi del bucket Amazon S3 sono abilitate per un bucket:

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket
```

L'output include un campo `BucketKeyEnabled` impostato su `true` o `false`.

Per configurare DSSE-KMS, utilizza il seguente comando:

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":{"SSEAlgorithm":"aws:kms:dsse","KMSEMasterKeyID":"YOUR-KMS-KEY-ARN"}}]}'
```

Per ulteriori informazioni sulla crittografia predefinita, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#). Per ulteriori informazioni su SSE-S3, consulta [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#)

Important

Se si utilizza l'opzione DSSE-KMS o per la configurazione di crittografia predefinita, si è soggetti alla quota di richieste al secondo (RPS) di AWS KMS. Puoi ridurre le chiamate all'API KMS abilitando Amazon S3 Bucket Keys, che riduce il numero di richieste inviate a AWS KMS. Per ulteriori informazioni sulle quote AWS KMS e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli sviluppatori di AWS Key Management Service.

È stato creato un bucket in Amazon S3. La prossima fase consiste nel caricamento di un oggetto nel bucket.

Fase 2: Carica un oggetto nel tuo bucket

Dopo aver creato un bucket in Amazon S3, sei pronto per caricare un oggetto nel bucket. Un oggetto può essere qualsiasi tipo di file: file di testo, immagine, video e così via.

Per caricare un oggetto in un bucket

1. Crea un file di testo semplice da caricare. È anche possibile utilizzare un editor di testo o eseguire il seguente comando:

```
echo 'Hello, Amazon S3!' > example.txt
```

2. Carica il file nel bucket utilizzando il comando `s3 cp`:

```
aws s3 cp example.txt s3://amzn-s3-demo-bucket/
```

Se il caricamento viene completato, vedrai un output simile al seguente:

```
upload: ./example.txt to s3://amzn-s3-demo-bucket/example.txt
```

3. Verifica che l'oggetto sia stato caricato elencando il contenuto del bucket:

```
aws s3 ls s3://amzn-s3-demo-bucket/
```

Hai caricato correttamente un oggetto nel bucket. La prossima fase consiste nel download di un oggetto.

Fase 3: donwload di un oggetto

Dopo avere caricato un oggetto in un bucket, è possibile visualizzare le informazioni sull'oggetto e scaricare l'oggetto nel computer locale.

Come scaricare un oggetto da un bucket Amazon S3

1. Per ottenere le informazioni sull'oggetto:

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key example.txt
```

Questo comando restituisce i metadati sull'oggetto, tra cui il tipo di contenuto, la lunghezza del contenuto e la data dell'ultima modifica.

2. Scarica l'oggetto sul computer locale:

```
aws s3 cp s3://amzn-s3-demo-bucket/example.txt downloaded-example.txt
```


Se il download viene completato, vedrai un output simile al seguente:

```
download: s3://amzn-s3-demo-bucket/example.txt to ./downloaded-example.txt
```

3. Verifica il contenuto del file scaricato:

```
cat downloaded-example.txt
```

Note

- A differenza della console, AWS CLI può scaricare più oggetti contemporaneamente utilizzando caratteri jolly o il flag. `--recursive`
- Quando si scaricano oggetti con AWS CLI, i punti (.) alla fine dei nomi delle chiavi degli oggetti vengono mantenuti, a differenza della console in cui vengono rimossi. Questa considerazione è importante se le chiavi degli oggetti terminano con il punto.

Esempio di download di più oggetti:

Per scaricare più oggetti da un bucket Amazon S3 con estensioni di file specifiche, utilizza il comando di copia ricorsiva con i filtri `exclude` e `include` come mostrato nell'esempio.

```
aws s3 cp s3://amzn-s3-demo-bucket/ . --recursive --exclude "*" --include "*.txt"
```

Hai scaricato correttamente il tuo oggetto. La prossima fase consiste nella copia dell'oggetto in una cartella.

Fase 4: copiare l'oggetto in una cartella

Hai aggiunto un oggetto a un bucket e hai scaricato l'oggetto. Ora, crei una cartella e copi l'oggetto nella cartella.

Per copiare un oggetto in una cartella

1. In Amazon S3, le cartelle sono rappresentate dai prefissi nelle chiavi degli oggetti. Crea una "cartella" copiando un oggetto con prefisso:

```
aws s3 cp s3://amzn-s3-demo-source-bucket/example.txt s3://amzn-s3-demo-destination-bucket/favorite-files/example.txt
```

Se la copia viene completata, vedrai un output simile al seguente:

```
copy: s3://amzn-s3-demo-source-bucket/example.txt to s3://amzn-s3-demo-destination-bucket/favorite-files/example.txt
```

2. Verifica che l'oggetto sia stato copiato elencando il contenuto della cartella:

```
aws s3 ls s3://amzn-s3-demo-destination-bucket/favorite-files/
```

Hai copiato correttamente l'oggetto in una cartella. La prossima fase consiste nell'eliminare gli oggetti e il bucket.

Fase 5: eliminare gli oggetti e il bucket

Quando non hai più bisogno di un oggetto o di un bucket, ti consigliamo di eliminarlo per evitare ulteriori addebiti. Se hai completato questa procedura dettagliata iniziale come esercizio di apprendimento e non hai intenzione di utilizzare il bucket o gli oggetti, ti consigliamo di eliminare il bucket in modo che non si accumulino più addebiti.

Prima di eliminare il bucket, devi svuotare il bucket o eliminare gli oggetti nel bucket. Una volta eliminati gli oggetti e il bucket non sono più disponibili.

Se desideri continuare a utilizzare lo stesso nome di bucket, è consigliabile eliminare gli oggetti o svuotare il bucket senza eliminarlo. Dopo aver eliminato un bucket, il nome diventa disponibile per il riutilizzo. Tuttavia, un altro AWS account potrebbe creare un bucket con lo stesso nome prima che tu abbia la possibilità di riutilizzarlo.

Eliminazione di un oggetto

Se desideri scegliere quali oggetti eliminare senza svuotare tutti gli oggetti dal bucket, puoi eliminare un oggetto.

Elimina un oggetto specifico:

```
aws s3 rm s3://amzn-s3-demo-bucket/example.txt
```

Se l'eliminazione viene completata, vedrai un output simile al seguente:

```
delete: s3://amzn-s3-demo-bucket/example.txt
```

Svuotamento del bucket

Se intendi eliminare il bucket, è necessario prima svuotarlo, eliminando così tutti gli oggetti, le versioni e gli indicatori di eliminazione presenti al suo interno.

Per svuotare un bucket

Important

Lo svuotamento del bucket non può essere annullato. Gli oggetti aggiunti al bucket mentre l'azione di svuotamento del bucket è in corso verranno eliminati.

1. Opzione 1: per i bucket più piccoli, utilizza il comando `rm` con il flag `--recursive` per eliminare tutti gli oggetti presenti nel bucket:

```
aws s3 rm s3://amzn-s3-demo-bucket --recursive
```

Questo comando elimina tutti gli oggetti nel bucket, inclusi quelli nelle cartelle.

Note

Se il bucket contiene molti oggetti o oggetti di grandi dimensioni, questo comando potrebbe restituire un timeout. Per i bucket con grandi quantità di dati, utilizza la regola del ciclo di vita Amazon S3 per far scadere gli oggetti nei bucket.

Opzione 2: utilizza le regole del ciclo di vita Amazon S3 (consigliate per bucket di grandi dimensioni).

Per i bucket con molti oggetti oppure oggetti di grandi dimensioni, utilizza una regola del ciclo di vita Amazon S3 per far scadere ed eliminare automaticamente tutti gli oggetti. Attendi l'elaborazione della regola del ciclo di vita (questa operazione può richiedere fino a 24 ore). Per ulteriori informazioni sull'utilizzo delle regole del ciclo di vita per eliminare il contenuto dei bucket,

consulta [Come posso svuotare un bucket Amazon S3 utilizzando una regola di configurazione del ciclo di vita?](#)

2. Verifica che il bucket sia vuoto:

```
aws s3 ls s3://amzn-s3-demo-bucket
```

3. Se il bucket ha il controllo delle versioni abilitato, utilizza i seguenti comandi per eliminare gli oggetti con controllo delle versioni e gli indicatori di eliminazione.

Rimuovi gli oggetti con controllo delle versioni:

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete "$(aws s3api list-object-versions --bucket amzn-s3-demo-bucket --output json --query='{Objects: Versions[].{Key:Key,VersionId:VersionId}}')"
```

Rimuovi gli indicatori di eliminazione:

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete "$(aws s3api list-object-versions --bucket amzn-s3-demo-bucket --output json --query='{Objects: DeleteMarkers[].{Key:Key,VersionId:VersionId}}')"
```

4. Verifica che il bucket sia vuoto, senza gli oggetti con controllo delle versioni e gli indicatori di eliminazione:

```
aws s3api list-object-versions --bucket amzn-s3-demo-bucket
```

L'output non deve mostrare alcun oggetto con controllo delle versioni o indicatore di eliminazione rimanente.

Eliminazione del bucket

Dopo aver svuotato il bucket o eliminato tutti gli oggetti dal bucket, è possibile eliminarlo.

Important

L'eliminazione di un bucket non può essere annullata. I nomi dei bucket sono univoci. Se elimini il bucket, un altro AWS utente può utilizzare il nome. Se desideri continuare a utilizzare lo stesso nome di bucket, non eliminare il bucket. Invece, svuota il bucket e conservalo.

Come eliminare il bucket

1. Elimina il bucket:

```
aws s3api delete-bucket --bucket amzn-s3-demo-bucket
```

2. Verifica che il bucket sia stato eliminato elencando tutti i bucket:

```
aws s3 ls
```

Fasi successive

Negli esempi precedenti hai appreso come eseguire alcune attività di base di Amazon S3 utilizzando la AWS CLI.

I seguenti argomenti illustrano i percorsi di apprendimento che puoi sfruttare per acquisire una maggiore conoscenza di Amazon S3 in modo da implementarlo nelle tue applicazioni.

- [Conoscere i casi d'uso comuni](#)
- [Controllo dell'accesso a bucket e oggetti](#)
- [Proteggere e monitorare lo storage](#)
- [Sviluppo con Amazon S3](#)
- [Conoscere i casi d'uso comuni](#)
- [Esplora la formazione e il supporto](#)

L'elenco seguente mostra AWS CLI i comandi più comuni per Amazon S3:

- [cp](#): copia file o oggetti tra il file system locale e Amazon S3 o tra posizioni di Amazon S3
- [ls](#): elenca gli oggetti Amazon S3 e i prefissi comuni in un bucket e un prefisso specificati
- [mb](#): crea un bucket Amazon S3
- [mv](#): sposta file o oggetti tra il file system locale e Amazon S3 o tra posizioni di Amazon S3
- [presign](#): genera un URL prefirmato per un oggetto Amazon S3 che consente l'accesso temporaneo senza credenziali AWS
- [rb](#): rimuove un bucket Amazon S3 vuoto. È possibile utilizzare il flag `--force` per svuotare ed eliminare automaticamente un bucket con contenuti in un unico comando. Questa azione non può essere annullata.

- [rm](#): elimina oggetti da Amazon S3
- [sync](#): sincronizza le directory e i prefissi Amazon S3 copiando in modo ricorsivo i file nuovi e aggiornati dalla directory di origine alla destinazione.
- [website](#): configura un bucket come sito web statico

Per ulteriori informazioni sui AWS CLI comandi per Amazon S3, consulta le seguenti risorse:

- [s3](#) — Comandi High-level Amazon S3 che semplificano le operazioni comuni
- [s3api](#): accesso diretto a tutte le operazioni API Amazon S3
- [s3control](#): accesso diretto a tutte le operazioni API Amazon S3 Control

Creazione, configurazione e utilizzo di bucket per uso generico Amazon S3

Per memorizzare i tuoi dati in Amazon S3, lavori con risorse denominate bucket e oggetti. Un bucket è un container per oggetti o file. Un oggetto è un file e tutti i metadati che descrivono tale file.

Per memorizzare un oggetto in Amazon S3, crei un bucket e quindi carichi l'oggetto in un bucket. Quando l'oggetto si trova nel bucket, è possibile aprirlo, scaricarlo e spostarlo. Quando non hai più bisogno di un oggetto o di un bucket, puoi ripulire le tue risorse.

Gli argomenti di questa sezione forniscono una panoramica dell'utilizzo dei bucket per uso generico in Amazon S3. Includono informazioni sulla denominazione, sulla creazione, sull'accesso e sull'eliminazione di bucket per uso generico. Per ulteriori informazioni sulla visualizzazione degli oggetti in un bucket, consulta [Organizzare, elencare e utilizzare gli oggetti](#).

Sono disponibili diversi tipi di bucket Amazon S3. Prima di creare un bucket, accertati di scegliere il tipo di bucket più adatto ai requisiti dell'applicazione e delle prestazioni. Per ulteriori informazioni sui vari tipi di bucket e sui casi d'uso appropriati per ogni tipo, consulta [Bucket](#).

Note

Per ulteriori informazioni sull'uso della classe di storage Amazon S3 Express One Zone con i bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Note

Con Amazon S3 paghi solo per le risorse utilizzate. Per ulteriori informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Amazon S3](#). Se sei un nuovo cliente Amazon S3, puoi iniziare a utilizzare Amazon S3 gratuitamente. Per ulteriori informazioni, consulta [Piano gratuito AWS](#).

Argomenti

- [Panoramica dei bucket per uso generico](#)
- [Namespace per bucket generici](#)

- [Modelli comuni di bucket per uso generico per la creazione di applicazioni su Amazon S3](#)
- [Regole di denominazione dei bucket per uso generico](#)
- [Quote, restrizioni e limitazioni dei bucket per uso generico](#)
- [Accesso a un bucket per uso generico Amazon S3](#)
- [Creazione di un bucket per uso generico](#)
- [Visualizzazione delle proprietà di un bucket per uso generico S3](#)
- [Elenco di bucket per uso generico Amazon S3](#)
- [Eliminazione del contenuto di un bucket per uso generico](#)
- [Eliminazione di un bucket per uso generico](#)
- [Montaggio di un bucket Amazon S3 come file system locale](#)
- [Operazioni con Storage Browser per Amazon S3](#)
- [Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#)
- [Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati](#)

Panoramica dei bucket per uso generico

Per caricare i dati (foto, video, documenti ecc.) su Amazon S3, è necessario creare prima un bucket S3 in una delle Regioni AWS.

Sono disponibili diversi tipi di bucket Amazon S3. Prima di creare un bucket, accertati di scegliere il tipo di bucket più adatto ai requisiti dell'applicazione e delle prestazioni. Per ulteriori informazioni sui vari tipi di bucket e sui casi d'uso appropriati per ogni tipo, consulta [Bucket](#).

Le sezioni seguenti forniscono ulteriori informazioni sui bucket per uso generico, comprese le regole di denominazione dei bucket, le quote e i dettagli di configurazione dei bucket. Per un elenco di restrizioni e limitazioni relative ai bucket Amazon S3, consulta [Quote, restrizioni e limitazioni dei bucket per uso generico](#).

Argomenti

- [Panoramica dei bucket per uso generico](#)
- [Modelli comuni di bucket per uso generico](#)
- [Permissions](#)
- [Gestione dell'accesso pubblico ai bucket per uso generico](#)

- [Gestione dell'accesso pubblico ai bucket per uso generico](#)
- [Opzioni di configurazione dei bucket per uso generico](#)
- [Operazioni su bucket per uso generico](#)
- [Monitoraggio delle prestazioni dei bucket per uso generico](#)

Panoramica dei bucket per uso generico

Ogni oggetto è contenuto in un bucket. Ad esempio, se l'oggetto denominato `photos/puppy.jpg` è archiviato nel bucket per uso generico `amzn-s3-demo-bucket` nella Regione Stati Uniti occidentali (Oregon), è indirizzabile tramite l'URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg`. Per ulteriori informazioni, consulta [Accesso a un bucket](#).

- Le quote dei bucket per uso generico per le Regioni commerciali possono essere visualizzate e gestite solo da Stati Uniti orientali (Virginia settentrionale).
- Le quote dei bucket generici per AWS GovCloud (US) possono essere visualizzate e gestite solo da AWS GovCloud (US)-West.

In termini di implementazione, i bucket e gli oggetti sono AWS risorse e Amazon S3 fornisce API per gestirli. Ad esempio, è possibile creare un bucket e caricare oggetti utilizzando l'API di Amazon S3. Per eseguire queste operazioni è possibile utilizzare anche la console di Amazon S3. La console utilizza le API di Amazon S3 per inviare richieste ad Amazon S3.

Questa sezione descrive come utilizzare i bucket per uso generico. Per informazioni sull'utilizzo di oggetti, consulta [Panoramica degli oggetti di Amazon S3](#).

Per impostazione predefinita, i bucket generici esistono in uno spazio dei nomi globale, il che significa che ogni nome di bucket deve essere univoco in tutto Account AWS l'interno di una partizione. Regioni AWS Una partizione è un raggruppamento di regioni. AWS attualmente ha quattro partizioni: `aws` (Regioni standard), `aws-cn` (Regioni cinesi), `()` e `aws-us-gov` `aws-eusc` (European Sovereign Cloud AWS GovCloud (US)). Dopo aver creato un bucket generico nello spazio dei nomi globale condiviso, il nome del bucket non può essere creato da nessun altro all'interno della partizione. Quando il proprietario di un bucket elimina il proprio bucket, il nome del bucket diventa nuovamente disponibile nello spazio dei nomi globale per essere ricreato da chiunque.

In alternativa, puoi creare bucket nello spazio dei nomi regionale del tuo account riservato per creare facilmente nomi di bucket prevedibili con la certezza che i nomi che desideri siano sempre disponibili

per l'uso. Il namespace regionale del tuo account è una suddivisione del namespace globale che solo il tuo account può utilizzare. Creando nuovi bucket nel namespace regionale del tuo account, hai la certezza che i nomi dei bucket desiderati saranno sempre disponibili per l'uso. Per ulteriori informazioni sui namespace regionali degli account, consulta [Namespace per bucket generici](#)

Una volta creato il bucket per uso generico, il nome del bucket non può essere utilizzato da un altro Account AWS nella stessa partizione fino a quando il bucket non viene eliminato. Non dovresti fare affidamento su specifiche convenzioni di denominazione dei bucket per scopi di verifica della disponibilità o della sicurezza. Per le linee guida sulla denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#).

Amazon S3 crea i bucket nella regione specificata. Per ridurre la latenza, minimizzare i costi o soddisfare i requisiti normativi, scegli una Regione AWS che sia geograficamente vicino a te. Ad esempio, se risiedi in Europa, potrebbe risultare vantaggiosa la creazione di bucket nella regione Europa (Irlanda) o Europa (Francoforte). Per un elenco delle regioni di Amazon S3, consulta [Regioni ed endpoint](#) in Riferimenti generali AWS .

Note

Gli oggetti che appartengono a un bucket creato in una regione specifica Regione AWS non lasciano mai quella regione, a meno che non vengano trasferiti esplicitamente in un'altra regione. Ad esempio, gli oggetti archiviati nella regione Europa (Irlanda) non lasceranno mai tale regione.

Modelli comuni di bucket per uso generico

Quando si costruiscono applicazioni su Amazon S3, è possibile utilizzare bucket univoci per uso generico per separare diversi set di dati o carichi di lavoro. A seconda del caso d'uso, esistono diversi modelli di progettazione e best practice per l'utilizzo dei bucket per uso generico. Per ulteriori informazioni, consulta [Modelli comuni di bucket per uso generico per la creazione di applicazioni su Amazon S3](#).

Permissions

Puoi utilizzare Utente root dell'account AWS le tue credenziali per creare un bucket generico ed eseguire qualsiasi altra operazione di Amazon S3. Tuttavia, si consiglia di non utilizzare le credenziali utente root dell' Account AWS per effettuare richieste, ad esempio per creare un bucket. Crea

invece un utente AWS Identity and Access Management (IAM) e concedigli accesso completo (per impostazione predefinita, gli utenti non hanno autorizzazioni).

Questi utenti sono indicati come amministratori. Puoi utilizzare le credenziali dell'utente amministratore, anziché le credenziali dell'utente root del tuo account, per interagire AWS ed eseguire attività, come creare un bucket, creare utenti e concedere loro le autorizzazioni.

Per ulteriori informazioni, consulta [Credenziali di Utente root dell'account AWS e credenziali utente IAM](#) nelle sezioni Riferimenti generali AWS e [Best practice relative alla sicurezza di IAM](#) della Guida per l'utente di IAM.

Chi crea una risorsa possiede Account AWS tale risorsa. Ad esempio, se crei un utente IAM nel tuo Account AWS e concedi all'utente il permesso di creare un bucket, l'utente può creare un bucket. Tuttavia, l'utente non è il proprietario del bucket: il bucket è di proprietà dell' Account AWS a cui appartiene l'utente. L'utente necessita di un'autorizzazione aggiuntiva da parte del proprietario delle risorse per eseguire qualsiasi altra operazione sul bucket. Per ulteriori informazioni sulla gestione delle autorizzazioni per le risorse Amazon S3, consulta [Identity and Access Management per Amazon S3](#).

Gestione dell'accesso pubblico ai bucket per uso generico

L'accesso pubblico a un bucket per uso generico e relativi oggetti viene fornito tramite policy di bucket, liste di controllo degli accessi (ACL) o entrambi. Amazon S3 offre impostazioni per il blocco dell'accesso pubblico per semplificare la gestione dell'accesso pubblico alle risorse Amazon S3. Le impostazioni di blocco dell'accesso pubblico di Amazon S3 possono sostituire ACL e policy dei bucket in modo da poter imporre limiti uniformi sull'accesso pubblico a queste risorse. Puoi applicare le impostazioni di blocco dell'accesso pubblico a singoli bucket o a tutti i bucket nell'account.

Per garantire che l'accesso pubblico sia bloccato per tutti i bucket per uso generico Amazon S3 e relativi oggetti, tutte e quattro le impostazioni di blocco dell'accesso pubblico sono abilitate per impostazione predefinita quando si crea un nuovo bucket. Ti consigliamo di attivare tutte e quattro le impostazioni per Blocco dell'accesso pubblico anche per il tuo account. Queste impostazioni bloccano l'accesso pubblico per tutti i bucket correnti e futuri.

Prima di applicare queste impostazioni, verifica che le applicazioni funzionino correttamente senza accesso pubblico. Se è richiesto un certo livello di accesso pubblico ai bucket o agli oggetti, ad esempio per ospitare un sito Web statico come descritto in [Hosting di un sito Web statico tramite Amazon S3](#), puoi personalizzare le impostazioni individuali in funzione dei casi d'uso di storage. Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Tuttavia, è altamente consigliabile mantenere l'impostazione Blocco dell'accesso pubblico abilitata. Se desideri mantenere abilitate tutte e quattro le impostazioni di Block Public Access e ospitare un sito Web statico, puoi utilizzare Amazon CloudFront origin Access Control (OAC). Amazon CloudFront fornisce le funzionalità necessarie per configurare un sito Web statico sicuro. I siti Web statici Amazon S3 supportano solo gli endpoint HTTP. Amazon CloudFront utilizza lo storage durevole di Amazon S3 fornendo al contempo impostazioni di sicurezza aggiuntive, come HTTPS. HTTPS aggiunge sicurezza crittografando una normale richiesta HTTP e proteggendo contro o più comuni attacchi informatici.

Per ulteriori informazioni, consulta [Getting started with a secure static website](#) nella Amazon CloudFront Developer Guide.

Note

Se viene visualizzato Error quando si elencano i bucket per uso generico e le relative impostazioni di accesso pubblico, è possibile che non siano disponibili le autorizzazioni necessarie. Assicurati di disporre delle seguenti autorizzazioni aggiunte alla policy utente o del ruolo:

```
s3:GetAccountPublicAccessBlock
s3:GetBucketPublicAccessBlock
s3:GetBucketPolicyStatus
s3:GetBucketLocation
s3:GetBucketAcl
s3:ListAccessPoints
s3:ListAllMyBuckets
```

In alcuni rari casi, le richieste possono anche non riuscire a causa di un'interruzione della Regione AWS .

Gestione dell'accesso pubblico ai bucket per uso generico

Puoi aggiungere tag ai tuoi bucket Amazon S3 per classificare e tenere traccia dei AWS costi o per il controllo degli accessi. Puoi utilizzare i tag come tag di allocazione dei costi per tenere traccia dei costi di archiviazione in AWS Fatturazione e gestione dei costi. Puoi anche utilizzare i tag per il controllo degli accessi basato sugli attributi (ABAC), per scalare le autorizzazioni di accesso e concedere l'accesso ai bucket S3 in base ai relativi tag.

Per ulteriori informazioni, consulta [Utilizzo di tag con bucket S3 per uso generico](#)

Opzioni di configurazione dei bucket per uso generico

Amazon S3 supporta varie opzioni di configurazione del bucket per uso generico. Ad esempio, è possibile configurare il bucket per l'hosting di siti Web, aggiungere una configurazione per la gestione del ciclo di vita degli oggetti nel bucket e configurare il bucket per la registrazione di tutti gli accessi al bucket. Amazon S3 supporta risorse secondarie per l'archiviazione e la gestione delle informazioni di configurazione del bucket. È possibile utilizzare l'API Amazon S3 per creare e gestire queste risorse secondarie. Tuttavia, puoi anche utilizzare la console o gli SDK. AWS

Note

Sono disponibili anche configurazioni a livello di oggetto. Ad esempio, è possibile configurare autorizzazioni a livello di oggetto configurando la lista di controllo accessi (ACL) specifica per quell'oggetto.

In questo caso, si parla di risorse secondarie in quanto esistono nel contesto di un bucket o oggetto specifico. Nella tabella sottostante sono elencate le risorse secondarie che consentono di gestire le configurazioni specifiche per bucket.

Risorsa secondaria	Descrizione
cors (cross-origin resource sharing)	<p>È possibile configurare il bucket per consentire richieste multiorigine.</p> <p>Per ulteriori informazioni, consulta Utilizzo della funzionalità Cross-Origin Resource Sharing (CORS).</p>
event notification	<p>È possibile abilitare il bucket per l'invio di notifiche di specifici eventi del bucket.</p> <p>Per ulteriori informazioni, consulta Notifiche di eventi Amazon S3.</p>
lifecycle	<p>È possibile definire le regole del ciclo di vita per gli oggetti nel bucket che hanno un ciclo di vita ben definito. Ad esempio, è possibile definire una regola per archiviare gli oggetti un anno dopo la creazione o eliminare un oggetto 10 anni dopo la creazione.</p>

Risorsa secondaria	Descrizione
	Per ulteriori informazioni, consulta Gestione del ciclo di vita degli oggetti .
posizione	Quando crei un bucket, specifichi Regione AWS dove desideri che Amazon S3 crei il bucket. Amazon S3 archivia queste informazioni nella risorsa secondaria della posizione e fornisce un'API per il recupero di queste informazioni.
logging	<p>La registrazione consente di tenere traccia delle richieste di accesso al bucket. Ogni record del log di accesso contiene i dettagli su una singola richiesta di accesso, ad esempio il richiedente, il nome del bucket, l'ora della richiesta, l'operazione della richiesta, lo stato della risposta e un eventuale codice di errore. Il log di accesso può essere utile nei controlli di accesso e di sicurezza. Può essere utile anche per comprendere la base clienti e la fattura Amazon S3.</p> <p>Per ulteriori informazioni, consulta Registrazione delle richieste con registrazione dell'accesso al server.</p>
blocco degli oggetti	<p>Per utilizzare il blocco oggetti S3, è necessario abilitarlo per un bucket. Facoltativamente, è anche possibile configurare una modalità e un periodo di conservazione predefiniti che verranno applicati ai nuovi oggetti inseriti nel bucket.</p> <p>Per ulteriori informazioni, consulta Blocco di oggetti con Object Lock.</p>
policy e ACL (lista di controllo accessi)	<p>Tutte le risorse (come bucket e oggetti) sono private per impostazione predefinita. Amazon S3 supporta opzioni di policy del bucket e liste di controllo accessi (ACL) per la concessione e la gestione delle autorizzazioni a livello di bucket. Amazon S3 archivia le informazioni sulle autorizzazioni nelle risorse secondarie di policy e acl.</p> <p>Per ulteriori informazioni, consulta Identity and Access Management per Amazon S3.</p>

Risorsa secondaria	Descrizione
replica	La replica è la copia asincrona e automatica degli oggetti di vari bucket nelle stesse o in diverse Regioni AWS. Per ulteriori informazioni, consulta Replica di oggetti all'interno e tra le Regioni .
requestPayment	<p>Per impostazione predefinita, chi crea Account AWS il bucket (il proprietario del bucket) paga i download dal bucket. Attraverso questa risorsa secondaria, il proprietario del bucket può specificare che il download sarà addebitato alla persona che lo richiede. Amazon S3 fornisce un'API per la gestione di questa risorsa secondaria.</p> <p>Per ulteriori informazioni, consulta Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati.</p>
tagging	<p>Puoi aggiungere tag ai tuoi bucket Amazon S3 per classificare e tenere traccia dei costi o per il AWS controllo degli accessi. Puoi utilizzare i tag come tag di allocazione dei costi per tenere traccia dei costi di archiviazione in AWS Fatturazione e gestione dei costi. Puoi anche utilizzare i tag per il controllo degli accessi basato sugli attributi (ABAC), per scalare le autorizzazioni di accesso e concedere l'accesso ai bucket S3 in base ai relativi tag.</p> <p>Per ulteriori informazioni, consulta Utilizzo di tag con bucket S3 per uso generico.</p>
transfer acceleration	<p>Transfer Acceleration permette di trasferire i file in modo rapido, semplice e sicuro su lunghe distanze tra il client e un bucket S3. Transfer Acceleration sfrutta le edge location distribuite a livello globale di Amazon. CloudFront</p> <p>Per ulteriori informazioni, consulta Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration.</p>

Risorsa secondaria	Descrizione
versioning	<p>La funzione Versioni multiple aiuta a eseguire il ripristino in caso di sovrascritture ed eliminazioni accidentali.</p> <p>Si consiglia l'uso della funzione Versioni multiple come best practice per ripristinare gli oggetti eliminati o sovrascritti per errore.</p> <p>Per ulteriori informazioni, consulta Conservazione di più versioni degli oggetti con Controllo delle versioni S3.</p>
website	<p>È possibile configurare il bucket per l'hosting di siti Web statici. Amazon S3 archivia questa configurazione creando una risorsa secondaria website.</p> <p>Per ulteriori informazioni, consulta Hosting di un sito Web statico tramite Amazon S3.</p>

Operazioni su bucket per uso generico

La progettazione ad alta disponibilità di Amazon S3 si basa sulle operazioni get, put, list e delete. Poiché le operazioni sui bucket per uso generico funzionano su uno spazio di risorse globale e centralizzato, è consigliabile evitare di creare, eliminare o configurare i bucket sul percorso del codice ad alta disponibilità dell'applicazione. È preferibile creare, eliminare o configurare i bucket durante le distinte attività di routine di inizializzazione o di configurazione, che vengono eseguite con frequenza minore.

Monitoraggio delle prestazioni dei bucket per uso generico

Quando si utilizzano applicazioni e processi aziendali critici che si basano su risorse AWS, è importante monitorare e ricevere gli avvisi per il sistema. [Il monitoraggio dei dati](#) può aiutare a mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon S3 e delle tue AWS soluzioni. Esistono diversi AWS servizi che puoi utilizzare per raccogliere e aggregare metriche e log per i tuoi bucket S3.

A seconda del caso d'uso, puoi scegliere il AWS servizio più adatto alle esigenze della tua organizzazione per eseguire il debug dei problemi, monitorare i dati, ottimizzare i costi di archiviazione o risolvere problemi multipli. Ad esempio:

- Per migliorare le prestazioni delle applicazioni che utilizzano S3: [impostare CloudWatch allarmi](#) per monitorare i dati di storage, le metriche di replica o le metriche delle richieste.
- Per pianificare l'utilizzo dell'archiviazione, ottimizzare i costi di archiviazione o per conoscere la quantità di spazio di archiviazione disponibile nell'intera organizzazione: [utilizzare Amazon S3 Storage Lens](#). In alternativa, è possibile [utilizzare S3 Storage Lens per migliorare i dati delle prestazioni](#), abilitando i parametri avanzati o utilizzando le metriche dei codici di stato dettagliati per ottenere i numeri delle richieste riuscite o non riuscite.
- Per una vista unificata dell'integrità operativa: [pubblicare le metriche di utilizzo e attività di S3 Storage Lens](#) in una [dashboard Amazon CloudWatch](#).

Note

L'opzione di Amazon CloudWatch pubblicazione è disponibile per i dashboard di S3 Storage Lens aggiornati a metriche e raccomandazioni avanzate. Puoi abilitare l'opzione di CloudWatch pubblicazione per una configurazione del dashboard nuova o esistente in S3 Storage Lens.

- Per ottenere una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio: imposta [AWS CloudTrail i log](#). Puoi anche utilizzare AWS CloudTrail i log per esaminare le chiamate API per Amazon S3 come eventi.
- Per ricevere le notifiche relative a quando si verificano determinati eventi nel bucket S3: [configurare le notifiche eventi di Amazon S3](#).
- Per ottenere registrazioni dettagliate delle richieste effettuate a un bucket S3: [configurare i log di accesso S3](#).

Per un elenco di tutti i diversi AWS servizi che puoi utilizzare per monitorare i tuoi dati, consulta [Registrazione e monitoraggio in Amazon S3](#).

Namespace per bucket generici

Per impostazione predefinita, i bucket generici esistono in un namespace globale. Ciò significa che il nome di ogni bucket deve essere univoco per tutti gli AWS account in tutte le AWS regioni all'interno di una partizione. Una partizione è un raggruppamento di regioni. AWS attualmente ha quattro partizioni: aws (Regioni standard), aws-cn (regioni cinesi), (Stati Uniti) e aws-us-govAWS GovCloud aws-eusc (European Sovereign Cloud). Quando crei un bucket generico, puoi scegliere di creare un bucket nel namespace globale condiviso. Puoi anche scegliere di creare un bucket nel

namespace regionale del tuo account. Il namespace regionale del tuo account è una suddivisione del namespace globale in cui solo il tuo account può creare bucket.

Argomenti

- [Bucket globali per uso generico](#)
- [Bucks generici con namespace regionali dell'account](#)
- [Restrizioni e considerazioni](#)
- [AWS Formato del codice regionale](#)
- [Richiesta della creazione di bucket nel namespace regionale del tuo account](#)
- [Creazione di un bucket nel namespace regionale del tuo account](#)

Bucket globali per uso generico

Per impostazione predefinita, si creano bucket globali per uso generico nello spazio dei nomi globale condiviso. Dopo aver creato un bucket generico nello spazio dei nomi globale condiviso, il nome del bucket non può essere creato da nessun altro all'interno della partizione. Quando elimini un bucket globale per uso generico, il nome del bucket diventa nuovamente disponibile nello spazio dei nomi globale per essere ricreato da chiunque.

Quando crei bucket globali per uso generico, puoi richiedere qualsiasi nome che rispetti le regole di denominazione dei bucket. Queste regole includono la specificazione di un nome composto da 3 (minimo) e 63 (massimo) caratteri. Il nome può essere composto solo da lettere minuscole, numeri, punti (.) e trattini (-). I nomi dei bucket devono iniziare e terminare con una lettera o un numero e non possono contenere due punti adiacenti. Per ulteriori informazioni sulle regole di denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#)

Quando si specifica un nome di bucket generico globale, è necessario selezionare un nome univoco che non sia già in uso per la partizione. Se tenti di creare un bucket già esistente e di proprietà di qualcun altro, riceverai un errore HTTP 409. BucketAlreadyExists Se tenti di creare un bucket già esistente e di tua proprietà, riceverai un errore HTTP 409. BucketAlreadyOwnedByYou

Puoi creare bucket globali per uso generico per avere la massima flessibilità nella selezione dei nomi dei bucket richiesti. Poiché si tratta di un namespace globale condiviso, altri account possono creare nomi di bucket simili. Anche altri account possono ricreare i nomi dei bucket che hai eliminato in precedenza. Non dovresti fare affidamento su specifiche convenzioni di denominazione dei bucket per scopi di verifica della disponibilità o della sicurezza. Non scrivere il

codice presupponendo che il nome del bucket scelto sia disponibile a meno il bucket non sia stato personalmente creato. Un metodo per creare nomi di bucket non prevedibili consiste nell'aggiungere un identificatore univoco globale (GUID) al nome del bucket. Ad esempio, `amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-example11111`. Per ulteriori informazioni, consulta [Creazione di un bucket che utilizza un GUID nel nome del bucket](#).

Bucks generici con namespace regionali dell'account

Sebbene i bucket Amazon S3 generici esistano in uno spazio dei nomi globale condiviso, puoi facoltativamente creare bucket nello spazio dei nomi regionale del tuo account. Il namespace regionale dell'account è una suddivisione riservata dello spazio dei nomi dei bucket globale. Solo il tuo account può creare bucket generici in questo namespace. I nuovi bucket generici creati nel namespace regionale del tuo account sono unici per il tuo account. Questi bucket non possono mai essere ricreati da un altro account. Questi bucket supportano tutte le funzionalità e i AWS servizi S3 già supportati dai bucket generici nel namespace globale condiviso. Le tue applicazioni non richiedono modifiche per interagire con i bucket nel namespace regionale del tuo account.

Note

Puoi creare bucket nel namespace regionale del tuo account in tutte le AWS regioni tranne Medio Oriente (Bahrain) e Medio Oriente (Emirati Arabi Uniti).

La creazione di bucket nel namespace regionale del tuo account è una best practice in materia di sicurezza. Questi nomi di bucket possono essere utilizzati solo dal tuo account. Puoi creare bucket nello spazio dei nomi regionale del tuo account per creare facilmente modelli di nomi di bucket generici in più regioni. AWS Puoi essere certo che nessun altro account può creare nomi di bucket nel tuo namespace. Se un altro account tenta di creare un bucket con il suffisso regionale del tuo account, la richiesta verrà rifiutata. CreateBucket

Convenzione di denominazione dei namespace regionali dell'account

I bucket generici nel namespace regionale del tuo account devono seguire una convenzione di denominazione specifica. Questi bucket sono costituiti da un prefisso per il nome del bucket creato dall'utente e da un suffisso che contiene l'ID AWS account di 12 cifre, il codice regionale e termina con. AWS -an

bucket-name-prefix-accountId-region-an

Ad esempio, il seguente bucket generico esiste nello spazio dei nomi regionale dell'account 111122223333 nella regione us-west-2: AWS

```
amzn-s3-demo-bucket-111122223333-us-west-2-an
```

Per creare un bucket nel namespace regionale del tuo account, fai una richiesta. CreateBucket Specifica l'intestazione della x-amz-bucket-namespace richiesta con il valore impostato su. account-regional Specifica anche il nome del bucket formattato nello spazio dei nomi regionale dell'account: <customer-chosen-name>-<AWS-Account-ID>-<AWS-Region>-an

Note

Quando crei un bucket generico nello spazio dei nomi regionale del tuo account utilizzando la console, viene aggiunto automaticamente un suffisso al prefisso del nome del bucket fornito. Questo suffisso include l'ID AWS dell'account e la AWS regione in cui hai selezionato per creare il bucket. Quando crei un bucket generico nel namespace regionale del tuo account utilizzando l' CreateBucket API, devi fornire il suffisso completo. Ciò include l'ID AWS dell'account e la AWS regione nella richiesta. Per un elenco dei codici AWS regionali, consulta [AWS Formato del codice regionale](#).

Integrazione del namespace regionale dell'account nel tuo CloudFormation modelli

Puoi aggiornare gli strumenti infrastructure-as-code, ad esempio per semplificare la creazione di bucket nel namespace regionale del tuo CloudFormation account. CloudFormation offre AWS::AccountId gli AWS::Region pseudo parametri e. Questi parametri semplificano la creazione di CloudFormation modelli che creano bucket di namespace regionali degli account. Per ulteriori informazioni, consulta [Ottenere AWS valori utilizzando pseudo parametri](#).

Esempio 1 di utilizzo BucketName con Sub:

```
BucketName: !Sub "amzn-s3-demo-bucket-${AWS::AccountId}-${AWS::Region}-an"
BucketNamespace: "account-regional"
```

Esempio 2 utilizzando BucketNamePrefix:

```
BucketNamePrefix: 'amzn-s3-demo-bucket'
BucketNamespace: "account-regional"
```

In alternativa, puoi anche utilizzare la `BucketNamePrefix` proprietà per aggiornare il CloudFormation modello. Ti `BucketNamePrefix` consente di fornire semplicemente la parte del nome del bucket definita dal cliente. Quindi aggiunge automaticamente il suffisso dello spazio dei nomi regionale dell'account in base all'account richiesto e alla regione specificati. AWS AWS

Utilizzando queste opzioni, puoi creare un CloudFormation modello personalizzato per creare facilmente bucket generici nel namespace regionale del tuo account. Per ulteriori informazioni, consulta [AWS: :S3: :Bucket](#) nella Guida per l'utente. CloudFormation

Restrizioni e considerazioni

Quando si creano bucket nello spazio dei nomi globale condiviso, valgono le seguenti considerazioni:

- Il nome di un bucket nello spazio dei nomi globale condiviso non può essere utilizzato da un altro AWS account nella stessa partizione finché il bucket non viene eliminato. Dopo aver eliminato un bucket nello spazio dei nomi globale condiviso, tieni presente che un altro AWS account nella stessa partizione può utilizzare lo stesso nome di bucket per un nuovo bucket e quindi può potenzialmente ricevere richieste destinate al bucket eliminato.
- Quando crei applicazioni che creeranno bucket nello spazio dei nomi globale condiviso, assicurati di considerare che i nomi dei bucket desiderati potrebbero essere già stati utilizzati da un altro account e che altri account potrebbero avere nomi di bucket simili ai tuoi.
- Poiché Amazon S3 identifica i bucket in base ai loro nomi, un'applicazione che utilizza un nome di bucket errato in una richiesta potrebbe inavvertitamente eseguire operazioni su un bucket diverso da quello previsto. Per evitare interazioni del bucket involontarie in situazioni come questa, puoi utilizzare la condizione proprietario del bucket. Per ulteriori informazioni, consulta [Verifica della proprietà del bucket con condizione del proprietario del bucket](#).

Quando si creano bucket nel namespace regionale dell'account, si applicano le seguenti restrizioni e considerazioni:

- Qualsiasi tentativo di ricreare un bucket dello spazio dei nomi regionale dell'account che già possiedi in qualsiasi AWS regione restituirà un errore HTTP 409. `BucketAlreadyOwnedByYou`
- Dovresti utilizzare gli endpoint regionali S3 per creare bucket nel namespace regionale del tuo account. Per la [compatibilità con le versioni precedenti](#), puoi utilizzare l'endpoint globale legacy per creare bucket nel namespace regionale del tuo account nella regione Stati Uniti orientali (Virginia settentrionale).

- Il suffisso regionale del tuo account viene conteggiato ai fini del numero massimo di 63 caratteri consentito nei nomi di bucket generici. Quindi, se il suffisso regionale del tuo account è `-012345678910-us-east-1-an`, allora hai 37 caratteri disponibili per il prefisso del nome del bucket.

AWS Formato del codice regionale

Per creare un bucket nel namespace regionale del tuo account, devi includere la AWS Regione nel suffisso in cui desideri creare il bucket generico. È necessario specificare il codice AWS regionale completo (ad esempio, `us-west-2`) nel suffisso. Vedi [AWS Regioni](#) per un elenco completo dei codici AWS regionali. I seguenti nomi di bucket mostrano due esempi del formato del codice AWS regionale da utilizzare quando crei i bucket nello spazio dei nomi regionale del tuo account:

- `amzn-s3-demo-bucket-012345678910-ap-southeast-1-an`
- `amzn-s3-demo-bucket-987654321012-eu-north-1-an`

Richiesta della creazione di bucket nel namespace regionale del tuo account

Puoi far sì che i tuoi IAM principali creino bucket solo nel namespace regionale del tuo account. Usa la chiave condizionale. `s3:x-amz-bucket-namespace` Gli esempi seguenti mostrano come è possibile imporre la creazione di bucket regionali di account in una IAM policy, Resource Control Policy o Service Control Policy.

IAM policy

La seguente IAM policy nega l'`CreateBucket` autorizzazione `s3`: al IAM principale se la richiesta non include l'intestazione `x-amz-bucket-namespace` impostata su `account-regional`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireAccountRegionalBucketCreation",
      "Effect": "Deny",
      "Action": "s3:CreateBucket",
      "Resource": "*",
      "Condition": {
```

```

        "StringNotEquals": {
            "s3:x-amz-bucket-namespace": "account-regional"
        }
    }
}
]
}

```

Politica di controllo delle risorse

La seguente politica di controllo delle risorse nega l>CreateBucket autorizzazione s3: a tutti se la richiesta non include l'intestazione x-amz-bucket-namespace impostata su account-regional.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OnlyCreateBucketsInAccountRegionalNamespace",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:CreateBucket",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-bucket-namespace": "account-regional"
        }
      }
    }
  ]
}

```

Policy di controllo dei servizi

La seguente politica di controllo dei servizi nega l>CreateBucket autorizzazione s3: a tutti se la richiesta non include l'intestazione x-amz-bucket-namespace impostata su account-regional.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireAccountRegionalBucketCreation",
      "Effect": "Deny",

```

```
{
  "Action": "s3:CreateBucket",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "s3:x-amz-bucket-namespace": "account-regional"
    }
  }
}
```

Creazione di un bucket nel namespace regionale del tuo account

Gli esempi seguenti mostrano come creare un bucket generico nel namespace regionale del tuo account.

Utilizzo di AWS CLI

L'AWS CLI esempio seguente crea un bucket generico nello spazio dei nomi regionale dell'account per l'AWS account 012345678910 nella regione Stati Uniti occidentali (California settentrionale) (us-west-1). Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3api create-bucket \
  --bucket amzn-s3-demo-bucket-012345678910-us-west-1-an \
  --bucket-namespace account-regional
  --region us-west-1 \
  --create-bucket-configuration LocationConstraint=us-west-1
```

Modelli comuni di bucket per uso generico per la creazione di applicazioni su Amazon S3

Quando si costruiscono applicazioni su Amazon S3, è possibile utilizzare bucket univoci per uso generico per separare diversi set di dati o carichi di lavoro. Quando crei applicazioni che servono agli utenti finali o a diversi gruppi di utenti, utilizza le nostre best practice per creare applicazioni che possano sfruttare al meglio le funzionalità e la scalabilità di Amazon S3.

⚠ Important

È consigliabile creare nomi di bucket per uso generico che non siano prevedibili. Non scrivere codice ipotizzando che il nome del bucket scelto sia disponibile, a meno che tu non abbia già creato il bucket. Ti consigliamo di creare bucket nello spazio dei nomi regionale del tuo account per assicurarti che solo il tuo account possa mai possedere questi nomi di bucket, vedi. [Namespace per bucket generici](#) Per ulteriori informazioni sulle regole di denominazione dei bucket per uso generico, consulta [Regole di denominazione dei bucket per uso generico](#).

Argomenti

- [Multi-tenant modello di bucket per uso generico](#)
- [Bucket-per-use modello](#)

Multi-tenant modello di bucket per uso generico

Con i bucket multi-tenant, si crea un singolo bucket per uso generico per un team o un carico di lavoro. Si utilizzano [prefissi S3 univoci](#) per organizzare gli oggetti memorizzati nel bucket. Un prefisso è una stringa di caratteri all'inizio del nome della chiave dell'oggetto. Un prefisso può essere di qualsiasi lunghezza, soggetto alla lunghezza massima del nome della chiave dell'oggetto (1.024 byte). Puoi pensare ai prefissi come un modo per organizzare i dati in modo simile alle directory. Tuttavia, i prefissi non sono directory.

Ad esempio, per memorizzare le informazioni sulle città, si potrebbe organizzarle per continente, poi per paese, quindi per provincia o stato. Poiché questi nomi in genere non contengono punteggiatura, è possibile selezionare la barra (/) come delimitatore. Gli esempi seguenti mostrano l'uso di prefissi per organizzare i nomi delle città in base al continente, al paese e poi alla provincia o allo stato, utilizzando un delimitatore a barra (/).

- Europe/France/NouvelleA-Aquitaine/Bordeaux
- Nord America/Canada/Quebec/Montreal
- Nord America/USA/Washington/Bellevue
- Nord America/USA/Washington/Seattle

Questo modello scala in modo ottimale quando si hanno centinaia di set di dati univoci all'interno di un bucket per uso generico. Con i prefissi è possibile organizzare e raggruppare facilmente questi set di dati.

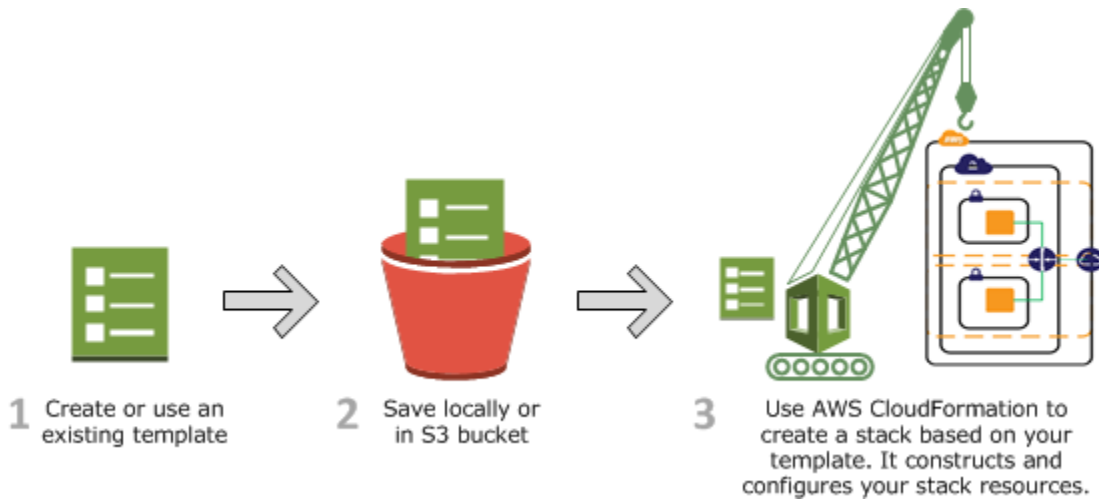
Tuttavia, un potenziale svantaggio del modello di bucket per uso generico multi-tenant è dato dal fatto che molte funzionalità a livello di bucket S3, come la [crittografia predefinita del bucket](#), il [controllo delle versioni S3](#) e i [pagamenti a carico del richiedente S3](#), sono impostate a livello di bucket e non a livello di prefisso. Se i diversi set di dati all'interno del bucket multi-tenant hanno requisiti unici, l'impossibilità di configurare a livello di prefisso molte funzionalità che sono a livello di bucket S3 può rendere difficile specificare le impostazioni corrette per ciascun set di dati. Inoltre, in un bucket multi-tenant, l'[allocazione dei costi](#) può diventare complessa in quanto si dedica tempo a comprendere l'archiviazione, le richieste e il trasferimento dei dati associati a prefissi specifici.

Bucket-per-use modello

Con il modello bucket-per-use, si crea un bucket per uso generico per ogni set di dati, utente finale o team distinto. Poiché è possibile configurare le caratteristiche a livello di bucket S3 per ciascuno di questi bucket, è possibile utilizzare questo modello per configurare impostazioni uniche a livello di bucket. Ad esempio, è possibile configurare funzioni come la [crittografia predefinita del bucket](#), il [controllo delle versioni S3](#) e i [pagamenti a carico del richiedente S3](#) in modo personalizzato per il set di dati in ciascun bucket. L'utilizzo di un bucket per ciascun set di dati, utente finale o team distinto può anche aiutare a semplificare le strategie di gestione degli accessi e di allocazione dei costi.

Un potenziale svantaggio di questa strategia è la necessità di gestire potenzialmente migliaia di bucket. Tutti Account AWS hanno una quota predefinita di 10.000 bucket per uso generico. È possibile aumentare la quota del bucket di un account inviando una richiesta di aumento della quota. Per richiedere un aumento per i bucket per uso generico, visita la [console Service Quotas](#).

Per gestire il modello bucket-per-use e semplificare la gestione dell'infrastruttura, si può utilizzare [AWS CloudFormation](#). Puoi creare un CloudFormation modello personalizzato per il tuo pattern che definisca già tutte le impostazioni desiderate per i tuoi bucket generici S3 in modo da poter implementare e tenere traccia di eventuali modifiche all'infrastruttura con facilità. Per ulteriori informazioni, consulta [AWS::S3::Bucket](#) nella Guida all'utente AWS CloudFormation .



Quando crei un carico di lavoro con un modello bucket per use, ti consigliamo di creare i bucket nel namespace regionale del tuo account. Creando bucket nello spazio dei nomi regionale del tuo account, eviti di competere per i nomi dei bucket con altri e hai la certezza che solo il tuo account potrà mai creare bucket con la convenzione di denominazione selezionata. Per ulteriori informazioni sui namespace regionali degli account, consulta [Namespace per bucket generici](#)

Regole di denominazione dei bucket per uso generico

Quando si crea un bucket per uso generico, è necessario considerare la lunghezza, i caratteri validi, la formattazione e l'univocità dei nomi dei bucket. Le sezioni seguenti forniscono informazioni sulla denominazione generica dei bucket, comprese le regole di denominazione, le best practice e un esempio di come creare bucket nel namespace regionale del proprio account. Un esempio per la creazione di un bucket per uso generico con un nome che include un identificatore univoco globale (GUID).

Per informazioni sui nomi delle chiavi di oggetti, consulta [Creazione di nomi di chiavi di oggetti](#).

Per creare un bucket per uso generico, consulta [the section called “Creazione di un bucket per uso generico”](#).

Argomenti

- [Regole di denominazione dei bucket per uso generico](#)
- [Regole di denominazione dei namespace regionali degli account](#)
- [Esempi di nomi di bucket per uso generico](#)
- [Best practice](#)
- [Creazione di un bucket che utilizza un GUID nel nome del bucket](#)

- [Creazione di un bucket nel namespace regionale del tuo account](#)

Regole di denominazione dei bucket per uso generico

Per la denominazione dei bucket per uso generico si applicano le seguenti regole.

- I nomi dei bucket devono avere una lunghezza compresa tra 3 (minimo) e 63 (massimo) caratteri.
- I nomi dei bucket possono essere costituiti solo da lettere minuscole, numeri, punti (.) e trattini (-).
- I nomi dei bucket devono iniziare e terminare con una lettera o un numero.
- I nomi dei bucket non devono contenere punti adiacenti.
- I nomi dei bucket non devono avere il formato di un indirizzo IP (ad esempio 192.168.5.4).
- I nomi dei bucket non devono iniziare con il prefisso xn--.
- I nomi dei bucket non devono iniziare con il prefisso sthree-.
- I nomi dei bucket non devono iniziare con il prefisso amzn-s3-demo-.
- I nomi dei bucket non devono terminare con il suffisso-s3alias. Questo suffisso è riservato ai nomi alias dei punti di accesso. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).
- I nomi dei bucket non devono terminare con il suffisso--o1-s3. Questo suffisso è riservato ai nomi alias dei punti di accesso Lambda per oggetti. Per ulteriori informazioni, consulta [Come utilizzare un alias in stile bucket per il punto di accesso Lambda per oggetti del bucket S3](#).
- I nomi dei bucket non devono terminare con il suffisso.mrap. Questo suffisso è riservato ai nomi degli Multi-Region Access Point. Per ulteriori informazioni, consulta [Regole per la denominazione degli Access Point di Amazon S3 Multi-Region](#).
- I nomi dei bucket non devono terminare con il suffisso--x-s3. Questo suffisso è riservato ai bucket di directory. Per ulteriori informazioni, consulta [Regole di denominazione dei bucket di directory](#).
- I nomi dei bucket non devono terminare con il suffisso--table-s3. Questo suffisso è riservato ai bucket di tabelle S3. Per ulteriori informazioni, consulta [Regole di denominazione di bucket di tabelle, tabelle e spazio dei nomi di Amazon S3](#).
- I nomi dei bucket possono terminare con il suffisso solo -an quando si creano bucket nello spazio dei nomi regionale dell'account. Per ulteriori informazioni, consulta [Namespace per bucket generici](#).
- I bucket utilizzati con Accelerazione del trasferimento Amazon S3 non possono contenere punti (.) nel nome. Per ulteriori informazioni su Transfer Acceleration, consulta [Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#).

 Important

- I bucket generici esistono in uno spazio dei nomi globale, il che significa che ogni nome di bucket deve essere univoco in tutto l'interno di una partizione. Account AWS Regioni AWS Una partizione è un raggruppamento di regioni. AWS attualmente ha quattro partizioni: aws (Regioni standard), aws-cn (Regioni cinesi), () e aws-us-gov aws-eusc (European Sovereign Cloud AWS GovCloud (US)). Dopo aver creato un bucket generico nello spazio dei nomi globale condiviso, il nome del bucket non può essere creato da nessun altro all'interno di una partizione. Quando il proprietario di un bucket elimina il proprio bucket, il nome del bucket potrebbe tornare disponibile nello spazio dei nomi globale per essere ricreato da chiunque. Tuttavia, il nome potrebbe non essere disponibile immediatamente e in alcuni casi potrebbe non esserlo affatto.
- Il nome di un bucket nello spazio dei nomi globale condiviso non può essere utilizzato da un altro Account AWS nella stessa partizione finché il bucket non viene eliminato. Dopo aver eliminato un bucket nello spazio dei nomi globale condiviso, tieni presente che un altro Account AWS nella stessa partizione può utilizzare lo stesso nome di bucket per un nuovo bucket e può quindi potenzialmente ricevere richieste destinate al bucket eliminato. Per evitare che ciò accada o continuare a utilizzare lo stesso nome del bucket, non eliminare il bucket. È consigliabile eliminare il contenuto del bucket e conservarlo, bloccando le richieste di bucket in base alle esigenze. Per i bucket non più in uso, è consigliabile eliminare tutti gli oggetti del bucket per ridurre al minimo i costi e mantenere il bucket stesso.
- Ti consigliamo di creare bucket nello spazio dei nomi regionale del tuo account per assicurarti che solo il tuo account possa possedere questi nomi di bucket.
- Quando crei un bucket generico, ne scegli il nome e il nome in cui crearlo. Regione AWS Dopo aver creato un bucket per uso generico, non è possibile modificarne il nome o la Regione.
- Non includere informazioni sensibili nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

 Note

Prima del 1° marzo 2018, i bucket creati nella regione Stati Uniti orientali (Virginia settentrionale) potevano avere nomi lunghi fino a 255 caratteri e con lettere maiuscole e

caratteri di sottolineatura. A partire dal 1° marzo 2018, i nuovi bucket nella regione Stati Uniti orientali (Virginia settentrionale) devono essere conformi alle stesse regole applicate in tutte le altre regioni.

Regole di denominazione dei namespace regionali degli account

Sebbene i bucket generici di Amazon S3 esistano in uno spazio dei nomi globale condiviso, puoi facoltativamente creare bucket nello spazio dei nomi regionale del tuo account. Il namespace regionale dell'account è una suddivisione riservata dello spazio dei nomi dei bucket globale in cui solo il tuo account può creare bucket generici. I nuovi bucket generici creati nel namespace regionale del tuo account sono unici per il tuo account e non possono mai essere ricreati da un altro account. Questi bucket supportano tutte le funzionalità e i AWS servizi di S3 già supportati dai bucket generici nel namespace globale condiviso. Le tue applicazioni non richiedono modifiche per interagire con i bucket nello spazio dei nomi regionale del tuo account.

I bucket generici nel namespace regionale dell'account devono seguire una convenzione di denominazione specifica. Questi bucket sono costituiti da un prefisso per il nome del bucket creato dall'utente e da un suffisso che contiene l'ID di 12 cifre Account AWS, il codice e termina con. Regione AWS -an

```
bucket-name-prefix-accountId-region-an
```

Ad esempio, il seguente bucket generico esiste nello spazio dei nomi regionale dell'account per 111122223333 nella regione us-west-2: Account AWS

```
amzn-s3-demo-bucket-111122223333-us-west-2-an
```

Per creare un bucket nello spazio dei nomi regionale del tuo account, fai una CreateBucket richiesta e specifica l'intestazione della richiesta con il valore impostato su `account-regional` insieme a specificare il `x-amz-bucket-name-space` nome del bucket formattato con lo spazio dei nomi regionale dell'account: *customer-chosen-name*-AWS-Account-ID-AWS-Region-an. Ad esempio, puoi specificare di creare un bucket denominato: dove si trova il suffisso regionale del tuo account. *amzn-s3-demo-bucket*-111122223333-us-east-1-an -111122223333-us-east-1-an Per ulteriori informazioni sui namespace regionali degli account, consulta [Namespace per bucket generici](#)

Esempi di nomi di bucket per uso generico

I seguenti sono esempi di nomi di bucket per uso generico con i caratteri consentiti: a-z, 0-9 e trattini (-). Il prefisso riservato `amzn-s3-demo-` viene qui utilizzato solo a scopo illustrativo. Il prefisso è riservato, pertanto non è possibile creare nomi di bucket che iniziano con `amzn-s3-demo-`.

- `amzn-s3-demo-bucket1-a1b2c3d4-5678-90ab-cdef-example11111`
- `amzn-s3-demo-bucket`

Gli esempi seguenti mostrano i nomi dei bucket nello spazio dei nomi regionale del tuo account. Questi bucket devono rispettare la specifica convenzione di denominazione dello spazio dei nomi regionale dell'account: *customer-chosen-name*-AWS-Account-ID-AWS-Region-an

- `amzn-s3-demo-bucket-111122223333-us-west-2-an`
- `amzn-s3-demo-bucket-012345678910-ap-southeast-2-an`

I seguenti nomi di bucket di esempio sono validi ma non consigliati per usi diversi dall'hosting di siti web statici perché contengono punti (.):

- `example.com`
- `www.example.com`
- `my.example.s3.bucket`

I nomi dei bucket di esempio seguenti non sono validi:

- `amzn_s3_demo_bucket` (contiene caratteri di sottolineatura)
- `AmznS3DemoBucket` (contiene lettere maiuscole)
- `amzn-s3-demo-bucket-` (inizia con il prefisso `amzn-s3-demo-` e termina con un trattino)
- `example..com` (contiene due punti consecutivi)
- `192.168.5.4` (corrisponde al formato di un indirizzo IP)

Best practice

Tieni in considerazione le seguenti best practice per la denominazione dei bucket quando assegni i nomi ai bucket per uso generico.

Crea bucket nel namespace regionale del tuo account

Ti consigliamo di creare bucket nel namespace regionale del tuo account per assicurarti che solo il tuo account possa mai possedere questi nomi di bucket. Con i namespace regionali degli account, puoi creare nomi di bucket prevedibili su più account Regioni AWS con la certezza che nessun altro account possa creare nomi di bucket nel tuo namespace.

Scegliere uno schema di denominazione dei bucket che difficilmente possa causare conflitti di denominazione

Se l'applicazione crea bucket automaticamente, scegli lo schema di denominazione dei bucket con meno probabilità di creare conflitti di denominazione. Assicurati che la logica dell'applicazione scelga un nome del bucket diverso nel caso in cui il nome del bucket sia già in uso.

Aggiungere identificatori univoci globali (GUID) ai nomi dei bucket

È consigliabile creare nomi di bucket non prevedibili. Non scrivere il codice presupponendo che il nome del bucket scelto sia disponibile a meno il bucket non sia stato personalmente creato. Un metodo per creare nomi di bucket non prevedibili consiste nell'aggiungere un identificatore univoco globale (GUID) al nome del bucket, ad esempio `amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-example11111`. Per ulteriori informazioni, consulta [the section called “Creazione di un bucket che utilizza un GUID nel nome del bucket”](#).

Evita di utilizzare i punti (.) nei nomi dei bucket

Per una migliore compatibilità, è consigliabile evitare l'utilizzo di punti (.) nei nomi dei bucket, ad eccezione dei bucket utilizzati solo per l'hosting di siti web statici. Se includi punti nel nome di un bucket, non potrai utilizzare l'indirizzamento in stile host virtuale su HTTPS, a meno che non esegui la convalida del certificato. I certificati di sicurezza utilizzati per l'hosting virtuale dei bucket non funzionano per i bucket con punti nei nomi.

Questa limitazione non influisce sui bucket utilizzati per l'hosting di siti web statici, poiché l'hosting di siti web statici è disponibile solo su HTTP. Per ulteriori informazioni sull'indirizzamento in stile hosting virtuale, consulta [Hosting virtuale di bucket per uso generico](#). Per ulteriori informazioni sull'hosting di siti Web statici, consulta [Hosting di un sito Web statico tramite Amazon S3](#).

Scegli un nome pertinente

Quando assegni un nome a un bucket, ti consigliamo di scegliere un nome che sia rilevante per te o la tua attività. Evita di utilizzare nomi associati ad altri. Ad esempio, evita di utilizzare AWS o Amazon nel nome del bucket.

Non eliminare i bucket in modo da poter riutilizzare i nomi dei bucket

Se un bucket è vuoto, puoi eliminarlo. Dopo l'eliminazione di un bucket, il nome diventa disponibile per un nuovo utilizzo. Tuttavia, non è garantito che si possa riutilizzare il nome immediatamente o in futuro. Dopo aver eliminato un bucket nello spazio dei nomi globale condiviso, potrebbe passare del tempo prima di poter riutilizzare il nome. Inoltre, un altro Account AWS potrebbe creare un bucket con lo stesso nome prima che tu possa riutilizzare il nome.

Dopo aver eliminato un bucket generico nello spazio dei nomi globale condiviso, tieni presente che un altro Account AWS nella stessa partizione può utilizzare lo stesso nome di bucket generico per un nuovo bucket e quindi può potenzialmente ricevere richieste destinate al bucket generico eliminato. Per evitare che ciò accada o continuare a utilizzare lo stesso nome del bucket per uso generico, non eliminare il bucket per uso generico. È consigliabile eliminare il contenuto del bucket e conservarlo, bloccando le richieste di bucket in base alle esigenze.

Creazione di un bucket che utilizza un GUID nel nome del bucket

Gli esempi seguenti mostrano come creare un bucket per uso generico che utilizza un GUID alla fine del nome del bucket.

Utilizzo di AWS CLI

L'AWS CLI esempio seguente crea un bucket generico nella regione () degli Stati Uniti occidentali (California settentrionale) con un nome di bucket di esempio che utilizza un identificatore univoco globale (GUIDus-west-1). Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3api create-bucket \
  --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
  --region us-west-1 \
  --create-bucket-configuration LocationConstraint=us-west-1
```

Utilizzo di AWS SDK per Java

L'esempio seguente mostra come creare un bucket con un GUID alla fine del nome del bucket nella Regione Stati Uniti orientali (Virginia settentrionale) (us-east-1) utilizzando AWS SDK per Java. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate. Per informazioni su altri AWS SDK, consulta Tools to Build on. [AWS](#)

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
        final AmazonS3 s3 =
            AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
            UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
        System.out.println(bucketName);
        s3.createBucket(createRequest);
    }
}
```

Creazione di un bucket nel namespace regionale del tuo account

Gli esempi seguenti mostrano come creare un bucket generico nel namespace regionale del tuo account.

Utilizzo di AWS CLI

L' AWS CLI esempio seguente crea un bucket generico nello spazio dei nomi regionale dell'account per Account AWS 012345678910 nella regione Stati Uniti occidentali (California settentrionale) Region (). us-west-1 Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3api create-bucket \
  --bucket amzn-s3-demo-bucket-012345678910-us-west-1-an \
  --bucket-namespace account-regional
  --region us-west-1 \
  --create-bucket-configuration LocationConstraint=us-west-1
```

Quote, restrizioni e limitazioni dei bucket per uso generico

Un bucket per uso generico Amazon S3 è di proprietà di chi lo ha creato. Account AWS La proprietà del bucket non è trasferibile ad un altro account.

Quote dei bucket

Per impostazione predefinita, puoi creare fino a 10.000 bucket per uso generico. Account AWS Per richiedere un aumento della quota per i bucket per uso generico, visita la [console Service Quotas](#).

Important

Si consiglia vivamente di utilizzare solo richieste `ListBuckets` impaginate. Le richieste non impaginate di `ListBuckets` sono supportate solo per Account AWS impostato sulla quota predefinita di 10.000 bucket per uso generico. Se si dispone di una quota di bucket per uso generico approvata superiore a 10.000, è necessario inviare richieste `ListBuckets` impaginate per elencare i bucket del proprio account. Tutte le `ListBuckets` richieste non impaginate verranno rifiutate Account AWS con una quota di bucket per uso generico superiore a 10.000.

Note

È necessario utilizzare quanto segue Regioni AWS per visualizzare la quota, l'utilizzo dei bucket o richiedere un aumento per i bucket per uso generico presenti nel tuo Account AWS

- Le quote dei bucket per uso generico per le Regioni commerciali possono essere visualizzate e gestite solo da Stati Uniti orientali (Virginia settentrionale).
- Le quote dei bucket per uso generico per AWS GovCloud (US) possono essere visualizzate e gestite solo da (). AWS GovCloud US-West

Per informazioni sulle quote di servizio, consulta [Quote di servizio AWS](#) in Riferimenti generali di Amazon Web Services.

Limiti su oggetti e bucket

Non esiste alcun limite alle dimensioni massime del bucket o al numero di oggetti che è possibile archiviare in un bucket. È possibile archiviare tutti gli oggetti in un unico bucket oppure organizzarli in diversi bucket. Tuttavia, non puoi creare un bucket da un altro bucket.

Regole di denominazione dei bucket

Quando crei un bucket, ne scegli il nome e l'indirizzo in cui Regione AWS crearlo. Una volta creato, non potrai più modificarne il nome o la regione. Per ulteriori informazioni sulla denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#).

Accesso a un bucket per uso generico Amazon S3

Puoi accedere ai tuoi bucket generici Amazon S3 utilizzando la console Amazon S3 AWS Command Line Interface, gli AWS SDK o l'API REST di Amazon S3. Ogni metodo di accesso a un bucket per uso generico S3 supporta casi d'uso specifici. Per ulteriori informazioni, consultare le sezioni indicate di seguito.

Argomenti

- [Casi d'uso](#)
- [Console Amazon S3](#)
- [AWS CLI](#)
- [AWS SDK](#)
- [API REST di Amazon S3](#)
- [Hosting virtuale di bucket per uso generico](#)

Casi d'uso

A seconda del caso d'uso del bucket per uso generico Amazon S3, esistono diversi metodi consigliati per accedere ai dati sottostanti nei bucket. L'elenco seguente include casi d'uso comuni per l'accesso ai dati.

- **Siti Web statici:** con Amazon S3 puoi ospitare un sito Web statico. Per questo caso d'uso, configuri un bucket per uso generico S3 in modo che funzioni come un sito web. Per un esempio che illustra

le fasi di hosting di un sito Web su Amazon S3, consulta [Esercitazione: configurazione di un sito Web statico su Amazon S3](#).

Per ospitare un sito Web statico con impostazioni di sicurezza come Block Public Access abilitate, consigliamo di utilizzare Amazon CloudFront con Origin Access Control (OAC) e di implementare intestazioni di sicurezza aggiuntive, come HTTPS. Per ulteriori informazioni, consulta [Guida introduttiva a un sito Web statico protetto](#).

Note

Per l'accesso a un sito Web statico, Amazon S3 supporta sia gli [URL in stile hosting virtuale](#) sia quelli in [stile percorso](#). Poiché è possibile accedere ai bucket utilizzando URL in stile path e in stile host virtuale, ti consigliamo di creare bucket con nomi di bucket DNS-compliant. Per ulteriori informazioni, consulta [Quote, restrizioni e limitazioni dei bucket per uso generico](#).

- Set di dati condivisi: quando si scala su Amazon S3, è comune adottare un modello multi-tenant, in cui si assegnano diversi clienti finali o unità aziendali a prefissi univoci all'interno di un bucket per uso generico condiviso. Utilizzando i [Punti di accesso Amazon S3](#), puoi suddividere una policy bucket di grandi dimensioni in policy di punti di accesso separate e discrete per ogni applicazione che deve accedere al set di dati condiviso. Questo approccio rende più semplice concentrarsi sulla creazione della giusta policy di accesso per un'applicazione, senza interrompere le attività di tutte le altre applicazioni all'interno del set di dati condiviso. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).
- Navigazione e gestione dei dati: Storage Browser per Amazon S3 è un componente open source che puoi aggiungere alle tue applicazioni web per fornire agli utenti finali un'interfaccia semplice per sfogliare e gestire i dati di Amazon S3. Per ulteriori informazioni, consulta [Operazioni con Storage Browser per Amazon S3](#).
- High-throughput carichi di lavoro — Mountpoint for Amazon S3 è un client di file open source ad alto rendimento per il montaggio di un bucket Amazon S3 generico come file system locale. Con Mountpoint, le applicazioni possono accedere agli oggetti archiviati in Amazon S3 tramite operazioni sui file system, quali apertura e lettura. Mountpoint converte automaticamente queste operazioni in chiamate API a oggetti S3, offrendo alle applicazioni l'accesso all'archiviazione elastica e alla velocità di trasmissione effettiva di Amazon S3 tramite un'interfaccia di file. Per ulteriori informazioni, consulta [Montaggio di un bucket Amazon S3 come file system locale](#).
- Multi-Region applicazioni: i punti di Multi-Region accesso Amazon S3 forniscono un endpoint globale che le applicazioni possono utilizzare per soddisfare le richieste provenienti da bucket S3

generici che si trovano in più contenitori. Regioni AWS Puoi utilizzare gli Multi-Region Access Point per creare applicazioni multiregionali con la stessa architettura utilizzata in una singola regione e quindi eseguire tali applicazioni in qualsiasi parte del mondo. Invece di inviare richieste tramite Internet pubblico, gli Multi-Region Access Point forniscono una resilienza di rete integrata con l'accelerazione delle richieste basate su Internet ad Amazon S3. Per ulteriori informazioni, consulta [Gestione del traffico multiregionale con punti di Multi-Region accesso](#).

- Secure Shell (SSH) File Transfer Protocol (SFTP): se stai cercando di trasferire in modo sicuro dati sensibili su Internet, puoi utilizzare un SFTP-enabled server con il tuo bucket generico Amazon S3. AWS SFTP è un protocollo di rete che supporta tutte le funzionalità di sicurezza e autenticazione di SSH. Questo protocollo ti permette di avere un controllo granulare sull'identità, le autorizzazioni e le chiavi degli utenti, ma se preferisci puoi utilizzare le policy IAM per gestire gli accessi. Per associare un server abilitato per SFTP al tuo bucket Amazon S3, assicurati di creare prima il tuo server. SFTP-enabled Quindi, è possibile impostare gli account utente e associare il server a un bucket per uso generico Amazon S3. Per una panoramica di questo processo, consulta [AWS Transfer for SFTP — Servizio SFTP completamente gestito per Amazon S3 nei blog](#). AWS

Console Amazon S3

La console è un'interfaccia utente basata sul Web per la gestione di Amazon S3 e AWS delle risorse. Con la console Amazon S3 è possibile accedere facilmente a un bucket e modificarne le proprietà. Attraverso l'interfaccia utente della console, è possibile eseguire quasi tutte le operazioni sul bucket senza dover scrivere alcun codice.

Se ti sei registrato Account AWS, puoi accedere alla console Amazon S3 accedendo alla console Amazon S3 e scegliendo S3 dalla home page della console Amazon S3. Puoi anche utilizzare questo link per accedere direttamente a. <https://console.aws.amazon.com/s3/>

AWS CLI

Puoi usare AWS CLI to emettere comandi o creare script nella riga di comando del tuo sistema per eseguire attività AWS (incluso S3). Ad esempio, se devi accedere a più bucket, puoi risparmiare tempo utilizzando il programma AWS CLI per automatizzare le attività comuni e ripetitive. La possibilità di scrivere e di ripetere azioni comuni è una necessità che le aziende considerano frequentemente quando crescono.

[AWS CLI](#) Fornisce comandi per un ampio set di. Servizi AWS AWS CLI È supportato su Windows, macOS e Linux. Per iniziare, consulta la [Guida per l'utente di AWS Command Line Interface](#).

Per ulteriori informazioni sui comandi per Amazon S3, consulta [s3api](#) e [s3control](#) nella pagina di riferimento dei comandi della AWS CLI .

AWS SDK

AWS fornisce SDK (kit di sviluppo software) costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (Java, Python, Ruby, .NET, iOS, Android e così via). Gli AWS SDK forniscono un modo conveniente per creare un accesso programmatico a S3 e. AWS Amazon S3 è un servizio REST. Puoi inviare richieste ad Amazon S3 utilizzando le librerie AWS SDK, che racchiudono l'API REST di Amazon S3 sottostante e semplificano le attività di programmazione. Ad esempio, gli SDK si occupano di attività quali il calcolo delle firme, la firma crittografica delle richieste, la gestione degli errori e la ripetizione automatica delle richieste. Per informazioni sugli AWS SDK, incluso come scaricarli e installarli, consulta Strumenti per. [AWS](#)

Ogni interazione con Amazon S3 è autenticata o anonima. Se utilizzi gli AWS SDK, le librerie calcolano la firma per l'autenticazione dalle chiavi fornite. Per ulteriori informazioni su come effettuare richieste ad Amazon S3, consulta [Esecuzione di richieste](#).

API REST di Amazon S3

L'architettura di Amazon S3 è ideata per essere indipendente dal linguaggio di programmazione e per utilizzare le interfacce supportate da AWS per archiviare e recuperare oggetti. Puoi accedere a S3 e AWS a livello di programmazione utilizzando l'API REST di Amazon S3. L'API REST è un'interfaccia HTTP per Amazon S3. Con l'API REST, utilizzi le richieste HTTP standard per creare, recuperare ed eliminare bucket e oggetti.

Per utilizzare l'API REST, puoi servirti di qualunque kit di strumenti in grado di supportare HTTP. Puoi anche utilizzare un browser per recuperare gli oggetti, purché siano leggibili in modo anonimo.

Poiché l'API REST utilizza codici di stato e intestazioni HTTP standard, i kit di strumenti e i browser standard funzionano come previsto. In alcune aree sono state aggiunte funzionalità ad HTTP, ad esempio le intestazioni per il supporto del controllo accessi. Le nuove funzionalità sono state in tali casi aggiunte in modo da essere conformi allo stile di utilizzo di HTTP standard.

Se effettui chiamate API REST direttamente dall'applicazione in uso, devi scrivere il codice per calcolare la firma e aggiungerlo alla richiesta. Per ulteriori informazioni su come effettuare richieste ad Amazon S3, consulta [Esecuzione di richieste](#) nella documentazione di riferimento delle API Amazon S3.

Hosting virtuale di bucket per uso generico

L'hosting virtuale è la pratica di servire più siti Web da un unico server Web. Un modo per differenziare i siti nelle richieste dell'API REST di Amazon S3 consiste nell'utilizzare il nome host apparente della parte dell'URI Request-URI anziché solo il nome del percorso. Una normale richiesta REST di Amazon S3 specifica un bucket utilizzando il primo componente del percorso delimitato da barre. Request-URI È possibile invece utilizzare l'hosting virtuale di Amazon S3 per un bucket per uso generico in una chiamata REST API utilizzando l'intestazione HTTP Host. In pratica, Amazon S3 interpreta Host come se la maggior parte dei bucket fosse accessibile immediatamente per alcuni tipi di richieste all'indirizzo `https://bucket-name.s3.region-code.amazonaws.com`. Per un elenco completo degli endpoint e delle Regioni Amazon S3, consulta la sezione relativa a [endpoint e quote di Amazon S3](#) nella Riferimenti generali di Amazon Web Services.

L'hosting virtuale ha anche altri vantaggi. Assegnando al bucket il nome del dominio registrato e rendendo tale nome un alias DNS per Amazon S3, è possibile personalizzare completamente l'URL delle risorse Amazon S3, ad esempio, `http://my.bucket-name.com/`. Puoi anche pubblicare nella directory root del server virtuale del bucket. Questa possibilità può essere importante in quanto molte applicazioni esistenti cercano i file in questa ubicazione standard. Ad esempio, `favicon.ico`, `robots.txt` e `crossdomain.xml` dovrebbero trovarsi tutti nella directory root.

Important

Quando si utilizzano bucket per uso generico in stile hosting virtuale con SSL, il certificato jolly SSL esamina solo i bucket che non contengono punti (.). Per risolvere questa limitazione, utilizzare HTTP o scrivere una logica di verifica del certificato personalizzata. Per ulteriori informazioni, consulta [Amazon S3 Path Deprecation Plan \(Piano di obsolescenza del percorso Amazon S3\)](#) in AWS News Blog.

Argomenti

- [Path-style richieste](#)
- [Virtual-hosted—richieste di stile](#)
- [specificazione del bucket di intestazione HTTP Host](#)
- [Esempi](#)
- [Personalizzazione degli URL Amazon S3 con record CNAME](#)
- [Come associare un nome host a un bucket Amazon S3](#)

- [Limitazioni](#)
- [Compatibilità con le versioni precedenti](#)

Path-style richieste

Attualmente, Amazon S3 supporta sia gli URL in stile hosting virtuale che quelli in stile percorso in tutte le Regioni AWS. Tuttavia, gli URL in stile percorso non saranno più disponibili in futuro. Per ulteriori informazioni, consulta la seguente nota importante.

In Amazon S3, gli URL in stile percorso utilizzano il seguente formato.

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

Ad esempio, se hai creato un bucket denominato `amzn-s3-demo-bucket1` nella regione Stati Uniti occidentali (Oregon) e vuoi accedere all'oggetto `puppy.jpg` in quel bucket, puoi utilizzare il seguente URL in stile percorso:

```
https://s3.us-west-2.amazonaws.com/amzn-s3-demo-bucket1/puppy.jpg
```

Important

Aggiornamento (23 settembre 2020): per assicurare che i clienti abbiano il tempo necessario per eseguire la transizione agli URL in stile hosting virtuale, abbiamo deciso di posticipare l'obsolescenza degli URL in stile percorso. Per ulteriori informazioni, consulta [Piano di obsolescenza del percorso Amazon S3 - Il resto della storia](#) nel Blog AWS News.

Warning

In caso di hosting di contenuti di siti Web a cui sarà possibile accedere da un browser Web, evita di utilizzare URL in stile percorso, che potrebbero interferire con il modello di sicurezza di origine del browser. Per ospitare il contenuto del sito Web, ti consigliamo di utilizzare gli endpoint del sito Web S3 o una CloudFront distribuzione. Per ulteriori informazioni, consulta [Endpoint del sito Web](#) e [distribuisci un'applicazione React-based a pagina singola su Amazon S3 e CloudFront](#) nei Perspective Guidance Patterns. AWS

Virtual-hosted—richieste di stile

In un URI in stile hosting virtuale, il nome del bucket fa parte del nome del dominio nell'URL.

Gli URL in stile hosting virtuale di Amazon S3 utilizzano il seguente formato.

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

In questo esempio, `amzn-s3-demo-bucket1` è il nome del bucket, Stati Uniti occidentali (Oregon) è la regione e `puppy.png` è il nome della chiave:

```
https://amzn-s3-demo-bucket1.s3.us-west-2.amazonaws.com/puppy.png
```

specificazione del bucket di **intestazione HTTP Host**

Purché la richiesta GET non utilizzi l'endpoint SSL, è possibile specificare il bucket per la richiesta utilizzando l'intestazione HTTP Host. L'intestazione Host in una richiesta REST viene interpretata come indicato di seguito:

- Se l'Host intestazione viene omessa o il suo valore è `s3.region-code.amazonaws.com`, il bucket per la richiesta sarà il primo componente delimitato da una barra e la chiave per la Request-URI richiesta sarà il resto di. Request-URI Questo è il metodo ordinario, mostrato nel primo e nel secondo esempio di questa sezione. È possibile omettere l'intestazione Host solo per le richieste HTTP 1.0.
- Altrimenti, se il valore dell'intestazione Host termina con `.s3.region-code.amazonaws.com`, il nome del bucket è il componente principale del valore dell'intestazione Host fino a `.s3.region-code.amazonaws.com`. La chiave per la richiesta è la. Request-URI Questa interpretazione espone i bucket come sottodomini di `.s3.region-code.amazonaws.com`, come mostrano il terzo e il quarto esempio in questa sezione.
- Altrimenti, il bucket per la richiesta è il valore minuscolo dell'Host intestazione e la chiave per la richiesta è la. Request-URI Questa interpretazione è utile nei casi in cui il nome DNS è stato registrato come nome del bucket e configurato il nome come alias del nome canonico (CNAME) per Amazon S3. La procedura per registrare i nomi di dominio e configurare i record DNS CNAME esula dall'ambito di questa guida, ma il risultato è mostrato nell'esempio finale di questa sezione.

Esempi

Questa sezione fornisce URL e richieste di esempio.

Example— URL e richieste Path-style

In questo esempio viene utilizzato:

- Nome bucket - `example.com`
- Regione - Stati Uniti orientali (Virginia settentrionale)
- Nome chiave - `homepage.html`

Di seguito è riportato l'URL:

```
http://s3.us-east-1.amazonaws.com/example.com/homepage.html
```

Di seguito è riportata la richiesta:

```
GET /example.com/homepage.html HTTP/1.1  
Host: s3.us-east-1.amazonaws.com
```

Di seguito è riportata la richiesta con HTTP 1.0 e senza intestazione Host:

```
GET /example.com/homepage.html HTTP/1.0
```

Per informazioni sui DNS-compatible nomi, vedi [Limitazioni](#). Per ulteriori informazioni sulle chiavi, consultare [Chiavi](#).

Example Virtual-hosted— URL e richieste di stile

In questo esempio viene utilizzato:

- Nome bucket - `amzn-s3-demo-bucket1`
- Regione - Europa (Irlanda)
- Nome chiave - `homepage.html`

Di seguito è riportato l'URL:

```
http://amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com/homepage.html
```

Di seguito è riportata la richiesta:

```
GET /homepage.html HTTP/1.1
```

```
Host: amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com
```

Example- metodo alias CNAME

Per utilizzare questo metodo, è necessario configurare il nome DNS come un alias CNAME per *bucket-name*.s3.us-east-1.amazonaws.com. Per ulteriori informazioni, consulta [Personalizzazione degli URL Amazon S3 con record CNAME](#).

In questo esempio viene utilizzato:

- Nome bucket - example.com
- Nome chiave - homepage.html

Di seguito è riportato l'URL:

```
http://www.example.com/homepage.html
```

Di seguito è riportato l'esempio:

```
GET /homepage.html HTTP/1.1  
Host: www.example.com
```

Personalizzazione degli URL Amazon S3 con record CNAME

A seconda delle esigenze, è possibile che non desideri che *s3.region-code.amazonaws.com* venga visualizzato sul tuo sito Web o sul tuo servizio. Se ad esempio ospiti le immagini del sito Web su Amazon S3, è possibile che tu preferisca `http://images.example.com/` anziché `http://images.example.com.s3.us-east-1.amazonaws.com/`. È possibile fare riferimento a qualsiasi bucket con un DNS-compatible nome come segue: `http://BucketName.s3.Region.amazonaws.com/[Filename]`, ad esempio, `http://images.example.com.s3.us-east-1.amazonaws.com/mydog.jpg`. Utilizzando CNAME, è possibile associare `images.example.com` a un nome host Amazon S3 in modo che l'URL precedente diventi `http://images.example.com/mydog.jpg`.

Il nome del bucket deve corrispondere esattamente al CNAME. Ad esempio, se crei un CNAME per associare `images.example.com` a `images.example.com.s3.us-east-1.amazonaws.com`, `http://images.example.com/filename` e `http://images.example.com.s3.us-east-1.amazonaws.com/filename` saranno identici.

Il record DNS di CNAME dovrebbe assegnare al nome del dominio il nome host in stile hosting virtuale appropriato come alias. Se ad esempio il nome del bucket e il nome del dominio sono `images.example.com` e il bucket si trova nella regione Stati Uniti orientali (Virginia settentrionale), il record CNAME dovrebbe assegnare l'alias a `images.example.com.s3.us-east-1.amazonaws.com`.

```
images.example.com CNAME    images.example.com.s3.us-east-1.amazonaws.com.
```

Amazon S3 utilizza il nome host per determinare il nome del bucket. Quindi il nome del bucket e CNAME devono essere gli stessi. Si supponga ad esempio di avere configurato `www.example.com` come CNAME per `www.example.com.s3.us-east-1.amazonaws.com`. Quando accedi a `http://www.example.com`, Amazon S3 riceve una richiesta simile alla seguente:

Example

```
GET / HTTP/1.1
Host: www.example.com
Date: date
Authorization: signatureValue
```

Amazon S3 vede solo il nome host originale `www.example.com` e non rileva la mappatura CNAME usata per risolvere la richiesta.

È possibile utilizzare qualsiasi endpoint Amazon S3 in un alias CNAME. Ad esempio, `s3.ap-southeast-1.amazonaws.com` può essere utilizzato negli alias CNAME. Per ulteriori informazioni sugli endpoint, consulta [Endpoint della richiesta](#) nella Guida di riferimento delle API di Amazon S3. Per creare un sito Web statico utilizzando un dominio personalizzato, consulta [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#)

Important

Quando si utilizzano URL personalizzati con CNAME, è necessario assicurarsi che esista un bucket corrispondente per qualsiasi record o alias CNAME configurato. Ad esempio, se si creano voci DNS per `www.example.com` e `login.example.com` per pubblicare contenuti Web utilizzando S3, è necessario creare entrambi i bucket `www.example.com` e `login.example.com`.

Quando un record CNAME o alias è configurato che punta a un endpoint S3 senza un bucket corrispondente, qualsiasi AWS utente può creare quel bucket e pubblicare il contenuto con l'alias configurato, anche se la proprietà non è la stessa.

Per lo stesso motivo, si consiglia di modificare o rimuovere il CNAME o l'alias corrispondente quando si elimina un bucket.

Come associare un nome host a un bucket Amazon S3

Associazione di un nome host a un bucket Amazon S3 utilizzando un alias CNAME

1. Selezionare un nome host appartenente a un dominio sottoposto al proprio controllo.

In questo esempio viene utilizzato il sottodominio `images` del dominio `example.com`.

2. Creare un bucket che corrisponda al nome host.

In questo esempio i nomi host e del bucket sono `images.example.com`. Il nome del bucket deve corrispondere esattamente al nome host.

3. Creare un record DNS CNAME che definisca il nome host come un alias per il bucket Amazon S3.

Ad esempio:

`images.example.com CNAME images.example.com.s3.us-west-2.amazonaws.com`

Important

Per motivi di instradamento della richiesta, il record DNS del CNAME deve essere definito esattamente come mostrato nell'esempio precedente. In caso contrario, potrebbe mostrare un funzionamento corretto ma determinare un comportamento imprevisto.

La procedura per la configurazione dei record DNS CNAME dipende dal server o dal provider DNS. Per informazioni specifiche, consultare la documentazione del server o contattare il provider.

Limitazioni

Le API SOAP per Amazon S3 non sono disponibili per i nuovi clienti, con la fine del ciclo di vita prevista per il 31 agosto 2025. Ti consigliamo di utilizzare l'API REST o gli SDK. AWS

Compatibilità con le versioni precedenti

Le sezioni seguenti trattano vari aspetti della compatibilità con le versioni precedenti di Amazon S3 relativi a richieste URL in stile percorso e in stile hosting virtuale.

Endpoint legacy

Alcune regioni supportano gli endpoint legacy. Potresti vedere questi endpoint nei log o AWS CloudTrail nei log di accesso al server. Per ulteriori informazioni, consulta le informazioni riportate di seguito. Per un elenco completo degli endpoint e delle regioni Amazon S3, consultare la sezione relativa a [endpoint e quote di Amazon S3](#) nella Riferimenti generali di Amazon Web Services.

Important

Sebbene nei log siano presenti endpoint legacy, si consiglia di utilizzare sempre la sintassi standard dell'endpoint per accedere ai bucket.

Gli URL in stile hosting virtuale di Amazon S3 utilizzano il seguente formato.

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

In Amazon S3, gli URL in stile percorso utilizzano il seguente formato.

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

s3-Regione

Alcune regioni Amazon S3 meno recenti supportano endpoint che contengono un trattino (-) tra s3 e il codice della regione (ad esempio, s3-us-west-2) anziché un punto (ad esempio, s3.us-west-2). Se il tuo bucket si trova in una di queste regioni, potresti visualizzare il seguente formato di endpoint nei log o nei log di accesso al server: CloudTrail

```
https://bucket-name.s3-region-code.amazonaws.com
```

In questo esempio, il nome del bucket è amzn-s3-demo-bucket1 e la regione è Stati Uniti occidentali (Oregon):

```
https://amzn-s3-demo-bucket1.s3-us-west-2.amazonaws.com
```

Endpoint globale legacy

Per alcune regioni, puoi utilizzare l'endpoint globale legacy per creare richieste che non specificano un endpoint. Region-specific L'endpoint globale legacy è il seguente:

```
bucket-name.s3.amazonaws.com
```

Nei log o CloudTrail nei log di accesso al server, potresti visualizzare richieste che utilizzano l'endpoint globale legacy. In questo esempio, il nome del bucket è `amzn-s3-demo-bucket1` e l'endpoint globale legacy è:

```
https://amzn-s3-demo-bucket1.s3.amazonaws.com
```

Virtual-hosted—richieste di stile per Stati Uniti orientali (Virginia settentrionale)

Le richieste effettuate con l'endpoint globale legacy sono instradate negli Stati Uniti orientali (Virginia settentrionale) per impostazione predefinita. Pertanto, l'endpoint globale legacy viene talvolta utilizzato al posto dell'endpoint regionale per Stati Uniti orientali (Virginia settentrionale). Se crei un bucket in Stati Uniti orientali (Virginia settentrionale) e utilizzi l'endpoint globale, Amazon S3 instrada la richiesta a questa regione per impostazione predefinita.

Virtual-hosted—richieste di stile per altre regioni

L'endpoint globale legacy viene utilizzato anche per le richieste in stile hosting virtuale nelle altre regioni supportate. Se crei un bucket in una regione lanciata prima del 20 marzo 2019 e utilizzi l'endpoint globale legacy, Amazon S3 aggiorna il record DNS per reinstradare la richiesta alla posizione corretta. Questa operazione potrebbe richiedere del tempo. Nel frattempo, viene applicata la regola di default: la richiesta in stile hosting virtuale viene inviata alla regione Stati Uniti orientali (Virginia settentrionale). Amazon S3 quindi la reindirizza con un reindirizzamento HTTP 307 temporaneo alla regione corretta.

Per i bucket S3 nelle regioni lanciati dopo il 20 marzo 2019, il server DNS non indirizza la richiesta direttamente al Regione AWS luogo in cui risiede il bucket. Restituisce invece un errore HTTP 400 - Richiesta non valida. Per ulteriori informazioni, consulta [Esecuzione di richieste](#) nella documentazione di riferimento delle API Amazon S3.

Path-style richieste

Per la regione Stati Uniti orientali (Virginia settentrionale), è possibile utilizzare l'endpoint globale legacy per le richieste in stile percorso.

Per tutte le altre regioni, la sintassi in stile path richiede l'utilizzo dell'Region-specific endpoint quando si tenta di accedere a un bucket. Se tenti di accedere a un bucket con l'endpoint globale legacy o un altro endpoint diverso da quello della Regione in cui risiede il bucket, viene restituito un codice di risposta HTTP 301 di errore di reindirizzamento permanente e un messaggio che indica l'URI corretto della risorsa. Ad esempio, se utilizzi `https://s3.amazonaws.com/bucket-name` per un bucket creato nella Regione Stati Uniti occidentali (Oregon), verrà visualizzato HTTP 301 di errore di reindirizzamento permanente.

Creazione di un bucket per uso generico

Per caricare i dati su Amazon S3, innanzitutto è necessario creare un bucket per uso generico Amazon S3 in una delle Regioni AWS. Il bucket è di proprietà dell' Account AWS che lo crea. Quando si crea un bucket, è necessario scegliere il nome del bucket e una regione. Durante il processo di creazione, è possibile facoltativamente scegliere altre opzioni di gestione dell'archiviazione per il bucket.

Important

Dopo avere creato un bucket, non è possibile cambiare il nome del bucket, il proprietario del bucket o la Regione. Per ulteriori informazioni sulla denominazione dei bucket, consulta [the section called “Regole di denominazione”](#).

Per impostazione predefinita, puoi creare fino a 10.000 bucket generici per Account AWS. Per richiedere un aumento della quota per i bucket per uso generico, visita la [console Service Quotas](#).

È possibile memorizzare un numero qualsiasi di oggetti in un bucket. Per un elenco di restrizioni e limitazioni relative ai bucket per uso generico Amazon S3, consulta [Quote, restrizioni e limitazioni dei bucket per uso generico](#).

Impostazioni del bucket per uso generico

Quando crei un bucket generico, devi decidere se vuoi creare un bucket generico globale o un bucket per uso generico nel namespace regionale del tuo account. Questa decisione, insieme al nome e alla regione del bucket, non può essere modificata dopo la creazione.

Quando si crea un bucket generico, è possibile utilizzare le seguenti impostazioni per controllare vari aspetti del comportamento del bucket:

- **S3 Bucket Namespace:** per impostazione predefinita, i bucket generici di Amazon S3 esistono in uno spazio dei nomi globale. Quando crei un bucket generico, puoi scegliere di creare un bucket nel namespace globale condiviso oppure puoi scegliere di creare un bucket nello spazio dei nomi regionale del tuo account. Il namespace regionale del tuo account è una suddivisione del namespace globale in cui solo il tuo account può creare bucket. I nuovi bucket generici creati nel namespace regionale del tuo account sono unici per il tuo account e non possono mai essere ricreati da un altro account. Questi bucket supportano tutte le funzionalità e i AWS servizi di S3 già supportati dai bucket generici nel namespace globale condiviso. Le tue applicazioni non richiedono modifiche per interagire con i bucket nello spazio dei nomi regionale del tuo account. Per ulteriori informazioni sui namespace dei bucket, consulta [Namespace per bucket generici](#)
- **Proprietà dell'oggetto S3:** è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le ACL sono disabilitate. Con le ACL disabilitate, il proprietario del bucket dispone di ogni oggetto nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).
- **Object Lock S3:** può impedire che gli oggetti Amazon S3 vengano eliminati o sovrascritti per un determinato periodo di tempo o in modo indefinito. Object Lock utilizza un modello write-once-read-many (WORM) per archiviare gli oggetti. È possibile utilizzare Object Lock per soddisfare i requisiti normativi che richiedono un'archiviazione WORM o per aggiungere un ulteriore livello di protezione contro le modifiche e l'eliminazione degli oggetti. Per ulteriori informazioni, consulta [the section called "Blocco degli oggetti"](#).
- **Tag:** un AWS tag è una coppia chiave-valore che contiene metadati. I tag vengono associati alle risorse Amazon S3, ad esempio i bucket. Puoi aggiungere i tag quando crei la risorsa oppure gestire quelli di una risorsa esistente. Puoi utilizzare i tag per l'allocazione dei costi per tenere traccia dei costi di archiviazione tramite bucket tag in Fatturazione e gestione dei costi. AWS Puoi anche utilizzare i tag per il controllo degli accessi basato sugli attributi (ABAC), per scalare le autorizzazioni di accesso e concedere l'accesso alle risorse S3 in base ai relativi tag. Per ulteriori informazioni, consulta [Utilizzo di tag con bucket S3 per uso generico](#).

Dopo aver creato un bucket per uso generico o quando crei un bucket per uso generico utilizzando la console Amazon S3, puoi utilizzare le seguenti impostazioni per controllare altri aspetti del comportamento del bucket:

- **Blocco dell'accesso pubblico S3:** è una funzionalità che fornisce le impostazioni per i punti di accesso, i bucket e gli account per facilitare la gestione dell'accesso pubblico alle risorse Amazon S3. Per impostazione predefinita, nuovi bucket, access point e oggetti non consentono l'accesso pubblico. Tuttavia, gli utenti possono modificare le policy di bucket, le policy di access point o le autorizzazioni degli oggetti per consentire l'accesso pubblico. Le impostazioni di blocco dell'accesso pubblico in S3 sostituiscono le policy e le autorizzazioni, in modo da limitare l'accesso pubblico a queste risorse. Per ulteriori informazioni, consulta [the section called “Blocco dell'accesso pubblico”](#).
- **Controllo delle versioni S3:** è un modo per conservare più versioni di un oggetto nello stesso bucket. Si può utilizzare questa funzione per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket. Con la funzione Controllo delle versioni si può facilmente eseguire il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Per impostazione predefinita, il controllo delle versioni è disabilitato per i bucket. Per ulteriori informazioni, consulta [the section called “Conservazione più versioni degli oggetti”](#).
- **Crittografia predefinita:** puoi impostare il tipo di crittografia predefinito per tutti gli oggetti nel bucket. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è il livello base di configurazione della crittografia per ogni bucket in Amazon S3. Tutti i nuovi oggetti caricati in un bucket S3 vengono crittografati automaticamente utilizzando SSE-S3 come livello base di crittografia. Se desideri utilizzare un tipo diverso di crittografia predefinita, puoi specificare la crittografia lato server con () chiavi AWS Key Management Service (AWS KMS), la crittografia lato server a doppio livello con chiavi (SSE-KMS) o la crittografia lato server con AWS KMS chiavi fornite dal cliente (DSSE-KMS) per crittografare i dati. SSE-C Per ulteriori informazioni, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#).

Puoi utilizzare la console Amazon S3, l'API REST di Amazon S3 () o gli SDK per creare un bucket generico. AWS Command Line Interface AWS CLI AWS Per ulteriori informazioni sulle autorizzazioni necessarie per creare un bucket generico, consulta [CreateBucket](#) la sezione Amazon Simple Storage Service API Reference.

Se riscontri problemi nella creazione di un bucket Amazon S3, consulta [Come risolvere i problemi che si verificano durante la creazione di un bucket Amazon S3?](#) su AWS re:Post.

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare un bucket.

Note

- Una volta creato, non è possibile modificarne la regione.
- Scegli una regione nelle tue vicinanze per ridurre al minimo la latenza e i costi o essere conforme ai requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione. Per un elenco di Amazon S3 Regioni AWS, consulta gli [Servizio AWS endpoint](#) in. Riferimenti generali di Amazon Web Services

3. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
4. Scegliere Create bucket (Crea bucket). Viene visualizzata la pagina Create bucket (Crea bucket).
5. In Nome bucket, immettere il nome del bucket.

Il nome del bucket deve:

- Essere univoco all'interno di una partizione. Una partizione è un raggruppamento di regioni. AWS attualmente ha tre partizioni: aws (regioni commerciali), aws-cn (regioni cinesi) e aws-us-gov (AWS GovCloud (US) Regions).
- Deve contenere da 3 a 63 caratteri
- Essere costituito solo da lettere minuscole, numeri, punti (.) e trattini (-). Per una migliore compatibilità, è consigliabile evitare l'utilizzo di punti (.) nei nomi dei bucket, ad eccezione dei bucket utilizzati solo per l'hosting di siti web statici.
- Iniziare e finire con una lettera o un numero.
- Per l'elenco completo delle regole di denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#).

Important

- Una volta creato il bucket, non è possibile modificarne il nome.
- Non includere informazioni sensibili nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

6. (Facoltativo) In Configurazione generale è possibile scegliere di copiare le impostazioni di un bucket esistente nel nuovo bucket. Se non desideri copiare le impostazioni di un bucket esistente, procedi al passaggio successivo.

 Note

Questa opzione:

- Non è disponibile nella AWS CLI ed è disponibile solo nella console Amazon S3
- Non copia la policy di bucket dal bucket esistente nel nuovo bucket

Per copiare le impostazioni di un bucket esistente, in Copia impostazioni da un bucket esistente, seleziona Scegli bucket. Viene visualizzata la finestra Scegli bucket. Individua il bucket con le impostazioni da copiare e seleziona Scegli bucket. La finestra Scegli bucket si chiude e si riapre la finestra Crea bucket.

In Copia impostazioni da un bucket esistente, ora viene visualizzato il nome del bucket selezionato. Le impostazioni del nuovo bucket ora corrispondono alle impostazioni del bucket selezionato. Se desideri rimuovere le impostazioni copiate, scegli Ripristina le impostazioni predefinite. Esamina le restanti impostazioni del bucket nella pagina Crea bucket. Se non desideri apportare modifiche, puoi passare alla fase finale.

7. Alla voce Proprietà oggetto, per disabilitare o abilitare le ACL e controllare la proprietà degli oggetti caricati nel bucket, scegliere una delle seguenti impostazioni:

ACL disabilitate

- Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket ha automaticamente il controllo completo di ogni oggetto di proprietà nel bucket per uso generico. Le liste di controllo degli accessi (ACL) non influiscono più sulle autorizzazioni di accesso ai dati nel bucket per uso generico S3. Il bucket utilizza esclusivamente le policy per definire il controllo degli accessi.

Per impostazione predefinita, le ACL sono disabilitate. La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne in circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

ACL abilitati

- Proprietario del bucket preferito - Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono sul bucket con l'ACL `bucket-owner-full-control` predefinita.

Se applichi l'impostazione Proprietario del bucket preferito, per richiedere che tutti i caricamenti di Amazon S3 includano l'ACL predefinita `bucket-owner-full-control`, puoi [aggiungere una policy del bucket](#) che consenta solo il caricamento di oggetti che utilizzano questa ACL.

- Autore di oggetti: chi carica un oggetto possiede l'oggetto, ne ha il pieno controllo e può concedere ad altri utenti l'accesso ad esso tramite ACL. Account AWS

Note

L'impostazione predefinita è Proprietario del bucket applicato. Per applicare l'impostazione predefinita e mantenere gli ACL disabilitati, è necessaria solo l'autorizzazione `s3:CreateBucket`. Per abilitare gli ACL, è necessario disporre dell'autorizzazione `s3:PutBucketOwnershipControls`.

8. In Impostazioni di blocco dell'accesso pubblico per questo bucket scegli le impostazioni di blocco dell'accesso pubblico che vuoi applicare al bucket.

Per impostazione predefinita, tutte e quattro le impostazioni Blocco dell'accesso pubblico sono abilitate. È consigliabile mantenere tutte le impostazioni abilitate, a meno che non sia necessario disattivarne una o più di una per il caso d'uso specifico. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Note

Per abilitare tutte le impostazioni Blocco dell'accesso pubblico, è richiesta solo l'autorizzazione `s3:CreateBucket`. Per disattivare le impostazioni Blocco dell'accesso pubblico, è necessario disporre dell'autorizzazione `s3:PutBucketPublicAccessBlock`.

9. (Facoltativo) Per impostazione predefinita, la funzionalità Controllo delle versioni del bucket è disabilitata. La funzione Controllo delle versioni è un modo per conservare più versioni di un oggetto nello stesso bucket. Si può utilizzare questa funzione per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket. Con il controllo delle versioni puoi eseguire facilmente il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Per abilitare il controllo delle versioni sul bucket, scegli Abilita.

10. (Facoltativo) In Tags (Tag), puoi scegliere di aggiungere tag al bucket. Con l'allocazione dei costi di AWS è possibile utilizzare i tag dei bucket per annotare nella fatturazione l'utilizzo di un bucket. Un tag è una coppia chiave-valore che rappresenta un'etichetta assegnata a un bucket. Per ulteriori informazioni, consulta [the section called "Utilizzo dei tag per l'allocazione dei costi"](#).

Per aggiungere un tag al bucket, inserisci un valore in Key (Chiave) e facoltativamente un valore in Value (Valore), quindi scegli Add Tag (Aggiungi tag).

11. Per configurare Crittografia predefinita, in Tipo di crittografia scegli una delle seguenti opzioni:
- Server-side crittografia con chiavi gestite da Amazon S3 () SSE-S3
 - Server-side crittografia con AWS Key Management Service chiavi () SSE-KMS
 - Dual-layer crittografia lato server con chiavi AWS Key Management Service (AWS KMS) () DSSE-KMS

 Important

Se si utilizza l' DSSE-KMS opzione SSE-KMS or per la configurazione di crittografia predefinita, si è soggetti alla quota di richieste al secondo (RPS) di AWS KMS. Per ulteriori informazioni sulle AWS KMS quote e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli AWS Key Management Service sviluppatori.

I bucket e i nuovi oggetti sono crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) come livello base di configurazione della crittografia. Per ulteriori informazioni sulla crittografia predefinita, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#). Per ulteriori informazioni su SSE-S3, consultare [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).

Per ulteriori informazioni sull'utilizzo della crittografia lato server per crittografare i dati, consulta [the section called "Crittografia dei dati"](#).

12. Se hai scelto Server-side la crittografia con AWS Key Management Service chiavi (SSE-KMS) o la Dual-layer crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (DSSE-KMS), procedi come segue:

- a. In Chiave AWS KMS specifica la tua chiave KMS in uno dei seguenti modi:
- Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS keys e scegli la tua chiave KMS dall'elenco delle chiavi disponibili.
- Sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente vengono visualizzate in questo elenco. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .
- Per specificare l'ARN della chiave KMS, scegli Inserisci l'ARN della AWS KMS key e quindi specifica l'ARN della chiave KMS nel campo visualizzato.
 - Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

 Important

È possibile utilizzare solo le chiavi KMS disponibili nello Regione AWS stesso bucket. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, è necessario inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione richiesta per l'uso della chiave e quindi inserire l'ARN della chiave KMS. Per ulteriori informazioni sulle autorizzazioni multi-account per le chiavi KMS, consulta [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service . Per ulteriori informazioni su SSE-KMS, consulta. [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#) Per ulteriori informazioni su

DSSE-KMS, vedere [the section called “Dual-layer crittografia lato server \(\) DSSE-KMS”](#).

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- b. Quando configuri il bucket per utilizzare la crittografia predefinita con SSE-KMS, puoi anche utilizzare S3 Bucket Keys. Le chiavi S3 Bucket riducono il costo della crittografia diminuendo il traffico di richieste da Amazon S3 a AWS KMS. Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#). Le chiavi S3 Bucket non sono supportate per DSSE-KMS.

Per impostazione predefinita, le chiavi del bucket S3 sono abilitate nella console Amazon S3. È consigliabile lasciare abilitate le chiavi del bucket S3 per ridurre i costi. Per disabilitare le chiavi del bucket S3 per il bucket in uso, scegli Disabilita in Chiave del bucket.

- 13. (Facoltativo) Object Lock S3 aiuta a proteggere i nuovi oggetti dall'eliminazione o dalla sovrascrittura. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#). Se desideri abilitare Object Lock S3, procedi come segue:

- a. Scegli Impostazioni avanzate.

 Important

Abilitando Object Lock si abilita automaticamente il controllo delle versioni per il bucket. Dopo aver abilitato e creato il bucket, è necessario anche configurare le impostazioni predefinite di conservazione e blocco legale di Object Lock nella scheda Proprietà del bucket.

- b. Se desideri attivare Object Lock, scegli Abilita, leggi l'avviso che appare e confermallo.

 Note

Per creare un bucket abilitato per Object Lock, sono necessarie le seguenti autorizzazioni: `s3:CreateBucket`, `s3:PutBucketVersioning` e `s3:PutBucketObjectLockConfiguration`.

14. Seleziona Crea bucket.

Utilizzo di AWS SDK

Quando si utilizzano AWS gli SDK per creare un bucket generico, è necessario creare un client e quindi utilizzare il client per inviare una richiesta di creazione di un bucket. Come best practice, crea il client e il bucket nella stessa Regione AWS. Se non specifichi una regione quando crei un client o un bucket, Amazon S3 utilizza la regione predefinita Stati Uniti orientali (Virginia settentrionale). Se vuoi vincolare la creazione del bucket a uno specifico Regione AWS, usa la chiave di condizione.

[LocationConstraint](#)

Per creare un client per accedere a un endpoint dual-stack, devi specificare un. Regione AWS Per ulteriori informazioni, consulta [Utilizzo degli endpoint dual-stack Amazon S3](#) nella documentazione di riferimento delle API Amazon S3. Per un elenco degli endpoint e delle quote disponibili Regioni AWS, consulta gli endpoint e le quote di [Amazon Simple Storage Service nel](#). Riferimenti generali di AWS

Quando si crea un client, la regione viene mappata sull' Region-specific endpoint. Il client utilizza questo endpoint per comunicare con Amazon S3: `s3.region.amazonaws.com`. Se la tua regione è stata lanciata dopo il 20 marzo 2019, il tuo client e il tuo bucket devono trovarsi nella stessa regione. Puoi comunque utilizzare un client nella regione Stati Uniti orientali (Virginia settentrionale) per creare un bucket in qualsiasi regione lanciata prima del 20 marzo 2019. Per ulteriori informazioni, consulta [Endpoint legacy](#).

Questi esempi di codice AWS SDK eseguono le seguenti attività:

- Creare un client specificando esplicitamente una Regione AWS: nell'esempio, il client utilizza l'endpoint `s3.us-west-2.amazonaws.com` per comunicare con Amazon S3. Puoi specificare qualsiasi Regione AWS. Per un elenco di Regioni AWS, consulta [Regioni ed endpoint](#) nella Guida AWS generale.
- Inviare una richiesta di creazione di bucket specificando solo il nome del bucket: il client invia ad Amazon S3 la richiesta di creare il bucket nella regione in cui hai creato un client.

- Recuperare le informazioni sulla posizione del bucket: Amazon S3 memorizza le informazioni sulla posizione del bucket nella risorsa secondaria posizione associata al bucket.

Per ulteriori esempi di AWS SDK ed esempi in altre lingue, consulta [Use CreateBucket with an AWS SDK o CLI](#) nell'Amazon Simple Storage Service API Reference.

Java

Per esempi su come creare un bucket con l' AWS SDK per Java, consulta [Create a bucket](#) in Amazon S3 API Reference.

Quando si utilizza l' AWS SDK per Java v2, è possibile creare un bucket generico con un identificatore univoco globale (GUID) aggiunto al nome del bucket per garantire l'unicità. Utilizza `UUID.randomUUID().toString().replace("-", "")` per generare un GUID e concatenarlo al nome del bucket di base. Questo approccio aiuta a evitare conflitti di denominazione dei bucket in tutti gli account. AWS

.NET

Per informazioni su come creare e testare un campione funzionante, consulta [Guida di riferimento delle API AWS SDK per .NET versione 3](#).

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using Amazon.S3.Util;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CreateBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
        RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {

```

```
s3Client = new AmazonS3Client(bucketRegion);
CreateBucketAsync().Wait();
}

static async Task CreateBucketAsync()
{
    try
    {
        if (!(await AmazonS3Util.DoesS3BucketExistAsync(s3Client,
bucketName)))
        {
            var putBucketRequest = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true
            };

            PutBucketResponse putBucketResponse = await
s3Client.PutBucketAsync(putBucketRequest);
        }
        // Retrieve the bucket location.
        string bucketLocation = await FindBucketLocationAsync(s3Client);
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
}

static async Task<string> FindBucketLocationAsync(IAmazonS3 client)
{
    string bucketLocation;
    var request = new GetBucketLocationRequest()
    {
        BucketName = bucketName
    };
    GetBucketLocationResponse response = await
client.GetBucketLocationAsync(request);
    bucketLocation = response.Location.ToString();
}
```

```
        return bucketLocation;
    }
}
}
```

Ruby

Per informazioni su come creare e testare un esempio di utilizzo, consulta [AWS SDK per Ruby - Versione 3](#).

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
  # This is a client-side object until create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    end
  end
end
```

```

    else
      @bucket.client.get_bucket_location(bucket: @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__

```

Utilizzo di AWS CLI

L'AWS CLI esempio seguente crea un bucket generico nella regione degli Stati Uniti occidentali (California settentrionale) con un nome di bucket di esempio che utilizza un identificatore univoco globale (GUIDus-west-1). Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```

aws s3api create-bucket \
  --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
  --region us-west-1 \
  --create-bucket-configuration LocationConstraint=us-west-1

```

Per ulteriori informazioni ed esempi, consulta [create-bucket](#) nella documentazione di riferimento dei comandi della AWS CLI .

Visualizzazione delle proprietà di un bucket per uso generico S3

È possibile visualizzare le proprietà di qualsiasi bucket Amazon S3 posseduto. Queste impostazioni includono quanto segue:

- Versioni multiple per il bucket: consente di gestire più versioni di un oggetto in un unico bucket per uso generico utilizzando il controllo delle versioni. Per default, la funzione Versioni multiple è disabilitata per un nuovo bucket. Per informazioni sull'abilitazione della funzione Versioni multiple, consulta [Abilitazione della funzione Controllo delle versioni sui bucket](#).
- Tag: un AWS tag è una coppia chiave-valore che contiene metadati. I tag vengono associati alle risorse Amazon S3, ad esempio i bucket. Puoi aggiungere i tag quando crei la risorsa oppure gestire quelli di una risorsa esistente. Puoi utilizzare i tag per l'allocazione dei costi per tenere traccia dei costi di archiviazione tramite bucket tag in Fatturazione e gestione dei costi. AWS Puoi anche utilizzare i tag per il controllo degli accessi basato sugli attributi (ABAC), per scalare le autorizzazioni di accesso e concedere l'accesso alle risorse S3 in base ai relativi tag. Per ulteriori informazioni, consulta [Utilizzo di tag con bucket S3 per uso generico](#).
- Crittografia predefinita: l'abilitazione della crittografia predefinita fornisce la crittografia automatica lato server. Amazon S3 crittografa di un oggetto prima di salvarlo su disco e lo decrittifica quando lo scarichi. Per ulteriori informazioni, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#).
- Registrazione degli accessi al server: fornisce record dettagliati per le richieste effettuate al bucket per uso generico con la registrazione dei log degli accessi al server. Per impostazione predefinita, Amazon S3 non raccoglie i log di accesso al server. Per informazioni sull'abilitazione della registrazione degli accessi al server, consulta [Abilitazione della registrazione degli accessi al server Amazon S3](#).
- AWS CloudTrail eventi relativi ai dati: CloudTrail da utilizzare per registrare gli eventi relativi ai dati. Per impostazione predefinita, i trail non registrano gli eventi di dati. Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta [Registrazione di eventi di dati per i trail](#) nella Guida per l'utente di AWS CloudTrail.
- Notifiche degli eventi: è possibile abilitare determinati eventi di bucket per uso generico Amazon S3 per inviare messaggi di notifica a una destinazione ogni volta che si verificano gli eventi. Per ulteriori informazioni, consulta [Attivazione e configurazione delle notifiche di eventi tramite la console di Amazon S3](#).
- Accelerazione trasferimento: permette di trasferire i file in modo rapido, semplice e sicuro su lunghe distanze tra il client e un bucket S3. Per informazioni sull'abilitazione dell'accelerazione di trasferimento, consulta [Abilitazione e utilizzo di S3 Transfer Acceleration](#).
- Blocco oggetto: utilizza S3 Object Lock per impedire che un oggetto venga eliminato o sovrascritto per un periodo di tempo fisso o indefinito. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).

- Pagamento a carico del richiedente: questa funzione fa in modo che il pagamento delle richieste e dei trasferimenti dei dati sia a carico del richiedente anziché del proprietario del bucket per uso generico. Per ulteriori informazioni, consulta [Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati](#).
- Hosting sito Web statico: puoi ospitare un sito Web statico su Amazon S3. Per ulteriori informazioni, consulta [Hosting di un sito Web statico tramite Amazon S3](#).

È possibile visualizzare le proprietà del bucket utilizzando Console di gestione AWS, AWS CLI, o SDK AWS

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket del quale desideri visualizzare le proprietà.
4. Scegliere la scheda Properties (Proprietà).
5. Nella pagina Proprietà è possibile configurare le proprietà di cui sopra per il bucket.

Utilizzo di AWS CLI

Visualizza le proprietà del bucket con AWS CLI

I comandi seguenti mostrano come è possibile utilizzare AWS CLI per elencare diverse proprietà del bucket per uso generale.

Di seguito viene restituito l'insieme di tag associato al bucket *amzn-s3-demo-bucket1*. Per ulteriori informazioni sui tag dei bucket, consulta [Utilizzo dei tag per l'allocazione dei costi per i bucket S3](#).

```
aws s3api get-bucket-tagging --bucket amzn-s3-demo-bucket1
```

Per ulteriori informazioni ed esempi, consulta [get-bucket-tagging](#) nella documentazione di riferimento dei comandi della AWS CLI .

Di seguito viene restituito lo stato del controllo delle versioni associato al bucket *amzn-s3-demo-bucket1*. Per informazioni sul controllo delle versioni del bucket, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).


```
aws s3api get-bucket-versioning --bucket amzn-s3-demo-bucket1
```

Per ulteriori informazioni ed esempi, consulta [get-bucket-versioning](#) nella documentazione di riferimento dei comandi della AWS CLI .

Di seguito viene restituita la configurazione di crittografia predefinita associata al bucket *amzn-s3-demo-bucket1*. Per impostazione predefinita, tutti i bucket hanno una configurazione di crittografia predefinita che utilizza la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Per informazioni sulla crittografia predefinita dei bucket, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#).

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

Per ulteriori informazioni ed esempi, consulta [get-bucket-encryption](#) nella documentazione di riferimento dei comandi della AWS CLI .

Di seguito viene restituita la configurazione di notifica associata al bucket *amzn-s3-demo-bucket1*. Per informazioni sulle notifiche di eventi relativi ai bucket, consulta [Notifiche di eventi Amazon S3](#).

```
aws s3api get-bucket-notification-configuration --bucket amzn-s3-demo-bucket1
```

Per ulteriori informazioni ed esempi, consulta [get-bucket-notification-configuration](#) nella documentazione di riferimento dei comandi della AWS CLI .

Di seguito viene restituito lo stato di accesso associato al bucket *amzn-s3-demo-bucket1*. Per informazioni sul logging dei bucket, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

```
aws s3api get-bucket-logging --bucket amzn-s3-demo-bucket1
```

Per ulteriori informazioni ed esempi, consulta [get-bucket-logging](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo di AWS SDK

Per esempi su come restituire proprietà generiche dei bucket con gli AWS SDK, come il controllo delle versioni, i tag e altro, consulta Esempi [di](#) codice nell'Amazon S3 API Reference.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK nell'API Reference di Amazon S3](#).

Elenco di bucket per uso generico Amazon S3

Per restituire un elenco di bucket generici di tua proprietà, puoi utilizzare. [ListBuckets](#) Puoi elencare i tuoi bucket utilizzando la console Amazon S3, il AWS Command Line Interface, o gli SDK. AWS Per `ListBuckets` le richieste che utilizzano gli AWS CLI AWS SDK e l'API REST di Amazon S3, Account AWS che utilizzano la quota di servizio predefinita per i bucket (10.000 bucket), supportano richieste sia impaginate che non paginate. Indipendentemente dal numero di bucket presenti nell'account, è possibile creare pagine di dimensioni comprese tra 1 e 10.000 bucket per elencare tutti i bucket. Per le richieste impaginate, le `ListBuckets` richieste restituiscono sia i nomi dei bucket che i corrispondenti per ogni bucket. Regioni AWS I seguenti esempi AWS Command Line Interface e l' AWS SDK mostrano come utilizzare l'impaginazione nella richiesta. `ListBuckets` Si noti che alcuni SDK AWS consentono l'impaginazione.

Permissions

Per elencare tutti i bucket per uso generico, è necessario disporre dell'autorizzazione `s3:ListAllMyBuckets`. Se si verifica un errore HTTP Access Denied (403 Forbidden), consulta [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#).

Important

Si consiglia vivamente di utilizzare solo richieste `ListBuckets` impaginate. Le richieste non impaginate di `ListBuckets` sono supportate solo per Account AWS impostato sulla quota predefinita di 10.000 bucket per uso generico. Se si dispone di una quota di bucket per uso generico approvata superiore a 10.000, è necessario inviare richieste `ListBuckets` impaginate per elencare i bucket del proprio account. Tutte le `ListBuckets` richieste non impaginate verranno rifiutate se la quota di bucket per Account AWS uso generico è superiore a 10.000.

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.

3. Nella scheda Bucket per uso generico è possibile visualizzare un elenco dei bucket per uso generico.
4. Per trovare i bucket in base al nome, inserisci il nome di un bucket nel campo Trova bucket in base al nome.

Utilizzo di AWS CLI

AWS CLI Per generare un elenco di bucket generici, puoi utilizzare i comandi `ls` o `list-buckets`. Gli esempi seguenti mostrano come creare una richiesta `list-buckets` impaginata e una richiesta `ls` non impaginata. Per utilizzare questi esempi, sostituisci *user input placeholders*.

Example— Elenca tutti i bucket del tuo account usando `ls` (unpaginated)

Il seguente esempio di comando elenca tutti i bucket per uso generico dell'account in un'unica chiamata non impaginata. Questa chiamata restituisce un elenco di tutti i bucket dell'account (fino a 10.000 risultati):

```
$ aws s3 ls
```

Per ulteriori informazioni e esempi, consulta [Elenco di bucket e oggetti](#).

Example— Elenca tutti i bucket del tuo account usando `ls` (paginato)

Il seguente esempio di comando effettua una o più chiamate impaginate per elencare tutti i bucket per uso generico dell'account, restituendo 100 bucket per pagina:

```
$ aws s3 ls --page-size 100
```

Per ulteriori informazioni e esempi, consulta [Elenco di bucket e oggetti](#).

Example- Elenca tutti i bucket dell'account (con impaginazione)

L'esempio seguente fornisce un comando impaginato `list-buckets` per elencare tutti i bucket per uso generico dell'account. Le opzioni `--max-items` e `--page-size` limitano il numero di bucket elencati a 100 per pagina.

```
$ aws s3api list-buckets /  
  --max-items 100 /
```

```
--page-size 100
```

Se il numero di elementi in uscita (`--max-items`) è inferiore al numero totale di elementi restituiti dalle chiamate API sottostanti, l'output include un token di continuazione, specificato dall'argomento `starting-token`, che può essere trasmesso a un comando successivo per recuperare la serie successiva di elementi. L'esempio seguente mostra come utilizzare il valore `starting-token` restituito dall'esempio precedente. È possibile specificare `starting-code` per recuperare i 100 bucket successivi.

```
$ aws s3api list-buckets /
  --max-items 100 /
  --page-size 100 /
  --starting-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ==
```

Example— Elenca tutti i bucket in un Regione AWS (impaginato)

Il seguente esempio di comando utilizza il parametro `--bucket-region` per elencare fino a 100 bucket in un account che si trovano nella Regione `us-east-2`. Le richieste effettuate a un endpoint regionale diverso dal valore specificato nel parametro `--bucket-region` non sono supportate. Ad esempio, se si vuole limitare la risposta ai propri bucket in `us-east-2`, si deve fare la richiesta a un endpoint in `us-east-2`.

```
$ aws s3api list-buckets /
  --region us-east-2 /
  --max-items 100 /
  --page-size 100 /
  --bucket-region us-east-2
```

Example- Elenca tutti i bucket che iniziano con un prefisso specifico del nome del bucket (con impaginazione)

Il seguente esempio di comando elenca fino a 100 bucket che hanno un nome che inizia con il prefisso `amzn-s3-demo-bucket`.

```
$ aws s3api list-buckets /
  --max-items 100 /
  --page-size 100 /
  --prefix amzn-s3-demo-bucket
```

Utilizzo di AWS SDK

Gli esempi seguenti mostrano come elencare i bucket generici utilizzando gli SDK AWS

SDK for Python

Example— ListBuckets richiesta (impaginata)

```
import boto3

s3 = boto3.client('s3')
response = s3.list_buckets(MaxBuckets=100)
```

Example— ListBuckets risposta (impaginata)

```
import boto3

s3 = boto3.client('s3')
response =
    s3.list_buckets(MaxBuckets=1, ContinuationToken="eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9"
```

SDK for Java

Per esempi di come elencare i bucket con l' AWS SDK per Java, consulta [Elencare i bucket](#) nell'Amazon S3 API Reference.

SDK for Go

```
package main
import (
    "context"
    "fmt"
    "log"
    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
)
func main() {
    cfg, err := config.LoadDefaultConfig(context.TODO(), config.WithRegion("us-east-2"))
    if err != nil {
        log.Fatal(err)
    }
}
```

```
client := s3.NewFromConfig(cfg)
maxBuckets := 1000
resp, err := client.ListBuckets(context.TODO(), management
portals3.ListBucketsInput{MaxBuckets: aws.Int32(int32(maxBuckets))})
if err != nil {
    log.Fatal(err)
}
fmt.Println("S3 Buckets:")
for _, bucket := range resp.Buckets {
    fmt.Println("- Name:", *bucket.Name)
    fmt.Println("- BucketRegion", *bucket.BucketRegion)
}
fmt.Println(resp.ContinuationToken == nil)
fmt.Println(resp.Prefix == nil)
}
```

Eliminazione del contenuto di un bucket per uso generico

Puoi svuotare il contenuto di un bucket generico utilizzando la console Amazon S3, gli SDK o (). AWS AWS Command Line Interface AWS CLI Quando si elimina il contenuto di un bucket per uso generico, si eliminano tutti gli oggetti, ma si mantiene il bucket. Lo svuotamento di un bucket non è reversibile. Anche gli oggetti aggiunti al bucket mentre l'operazione di svuotamento del bucket è in corso potrebbero essere eliminati. Tutti gli oggetti (incluse tutte le versioni degli oggetti e i marker di eliminazione) nel bucket devono essere eliminati prima che possa essere eliminato il bucket stesso.

Quando si elimina il contenuto di un bucket per uso generico che ha il controllo delle versioni S3 abilitato o sospeso, tutte le versioni di tutti gli oggetti nel bucket vengono eliminate. Per ulteriori informazioni, consulta [Utilizzo di oggetti in un bucket che supporta la funzione Controllo delle versioni](#).

Durante l'eliminazione del contenuto del bucket, è consigliabile rimuovere anche tutti i caricamenti in più parti incompleti. Puoi utilizzare i caricamenti in più parti per caricare oggetti molto grandi (fino a 50 TB) come set di parti per migliorare la produttività e velocizzare il ripristino dai problemi di rete. Nei casi in cui il processo di caricamento in più parti non venga portato a termine, le parti incomplete rimangono nel bucket (in uno stato inutilizzabile). Queste parti incomplete comportano costi di archiviazione fino al termine del processo di caricamento o fino alla rimozione delle parti incomplete. Per ulteriori informazioni, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Come best practice, consigliamo di configurare le regole del ciclo di vita per far scadere gli oggetti e i caricamenti in più parti incompleti più vecchi di un determinato numero di giorni. Quando crei

la regola del ciclo di vita per far scadere i caricamenti in più parti incompleti, consigliamo il valore di 7 giorni come buon punto di partenza. Per ulteriori informazioni, consulta [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#).

La scadenza del ciclo di vita è un processo asincrono, pertanto l'esecuzione della regola potrebbe richiedere alcuni giorni prima che il bucket sia vuoto. Dopo la prima volta che Amazon S3 esegue la regola, tutti gli oggetti idonei alla scadenza vengono contrassegnati per l'eliminazione. Non vengono più addebitati costi per gli oggetti contrassegnati per l'eliminazione. Per ulteriori informazioni, consulta [Come posso svuotare un bucket Amazon S3 utilizzando una regola di configurazione del ciclo di vita?](#).

Utilizzo della console S3

È possibile utilizzare la console Amazon S3 per eliminare il contenuto di un bucket per uso generico, ossia eliminare tutti gli oggetti nel bucket senza eliminare il bucket.

Per svuotare un bucket S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli l'opzione accanto al nome del bucket di cui desideri eliminare il contenuto, quindi scegli Vuoto.
4. Nella pagina Empty bucket (Svuota bucket) confermare che si desidera svuotare il bucket immettendo il nome del bucket nel campo di testo e quindi scegliere Empty (Svuota).
5. Monitorare l'avanzamento del processo di svuotamento del bucket nella pagina Svuota bucket: stato.

Utilizzo di AWS CLI

Puoi svuotare un bucket generico utilizzando AWS CLI only se il bucket non ha il Bucket Versioning abilitato. Se il controllo delle versioni non è abilitato, puoi utilizzare il AWS CLI comando `rm` (remove) con il `--recursive` parametro per svuotare il bucket (o rimuovere un sottoinsieme di oggetti con un prefisso di nome chiave specifico).

Il comando `rm` rimuove gli oggetti con prefisso del nome della chiave `doc`, ad esempio `doc/doc1` e `doc/doc2`.

```
$ aws s3 rm s3://bucket-name/doc --recursive
```

Per rimuovere tutti gli oggetti senza specificare un prefisso, è necessario utilizzare il comando seguente.

```
$ aws s3 rm s3://bucket-name --recursive
```

Per ulteriori informazioni, consulta [Utilizzo dei comandi di alto livello S3 con la AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface .

Note

Non è possibile rimuovere oggetti da un bucket su cui è abilitata la funzione Versioni multiple. Con questo comando, Amazon S3 aggiunge un contrassegno di eliminazione quando elimini un oggetto. Per ulteriori informazioni sulla funzione Versioni multiple del bucket S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per svuotare un bucket generico o rimuovere un sottoinsieme di oggetti con un prefisso di nome chiave specifico.

Per un esempio di come svuotare un bucket usando, vedi. AWS SDK per Java [Eliminazione di un bucket per uso generico](#) Il codice elimina tutti gli oggetti, indipendentemente dal fatto che sul bucket sia abilitata la funzione Versioni multiple o meno, quindi elimina il bucket. Se vuoi soltanto svuotare il bucket, accertati di avere rimosso l'istruzione che lo elimina.

Per ulteriori informazioni sull'utilizzo di altri AWS SDK, consulta [Tools for Amazon Web Services](#).

Utilizzo di una configurazione del ciclo di vita

Per eliminare il contenuto di un bucket per uso generico di grandi dimensioni, ti consigliamo di utilizzare una regola di configurazione del ciclo di vita S3. La scadenza del ciclo di vita è un processo asincrono, pertanto l'esecuzione della regola potrebbe richiedere alcuni giorni prima che il bucket sia vuoto. Dopo la prima volta che Amazon S3 esegue la regola, tutti gli oggetti idonei alla scadenza vengono contrassegnati per l'eliminazione. Non vengono più addebitati costi per gli oggetti contrassegnati per l'eliminazione. Per ulteriori informazioni, consulta [Come posso svuotare un bucket Amazon S3 utilizzando una regola di configurazione del ciclo di vita?](#).

Se si utilizza una configurazione del ciclo di vita per svuotare il bucket, tale configurazione deve includere [versioni correnti e non correnti](#), [contrassegni di eliminazione](#) e [caricamenti in più parti incompleti](#).

È possibile aggiungere le regole di configurazione del ciclo di vita per predisporre la scadenza di tutti gli oggetti o di un sottogruppo degli stessi con uno specifico prefisso nel nome della chiave. Ad esempio, per eliminare tutti gli oggetti in un bucket, è possibile impostare una regola del ciclo di vita per predisporre la scadenza degli oggetti il giorno successivo alla creazione degli stessi.

Amazon S3 supporta una regola per il ciclo di vita del bucket che può essere utilizzata per interrompere i caricamenti multipart che non sono stati completati entro un determinato numero di giorni dopo l'avvio. Si consiglia di configurare questa regola del ciclo di vita per ridurre al minimo i costi di storage. Per ulteriori informazioni, consulta [Configurazione del ciclo di vita del bucket per l'eliminazione dei caricamenti in più parti incompleti](#).

Per ulteriori informazioni sull'utilizzo di una configurazione del ciclo di vita per svuotare un bucket, consulta [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#) e [Oggetti in scadenza](#).

Svuotare un secchio generico con AWS CloudTrail disposto

AWS CloudTrail tiene traccia degli eventi di dati a livello di oggetto in un bucket Amazon S3 per uso generico, ad esempio l'eliminazione di oggetti. Se utilizzi un bucket generico come destinazione per registrare i tuoi CloudTrail eventi e stai eliminando oggetti dallo stesso bucket, potresti creare nuovi oggetti mentre svuoti il bucket. Per evitare che ciò accada, interrompi i tuoi percorsi. AWS CloudTrail Per ulteriori informazioni su come impedire ai CloudTrail percorsi di registrare eventi, consulta [Disattivazione della registrazione di un percorso](#) nella Guida per l'AWS CloudTrail utente.

Un'altra alternativa per impedire che i CloudTrail percorsi vengano aggiunti al bucket è aggiungere una `s3:PutObject` dichiarazione di rifiuto alla politica del bucket. Se desideri memorizzare nuovi oggetti nel bucket in un secondo momento, dovrai rimuovere questa istruzione di negazione `s3:PutObject`. Per ulteriori informazioni, consulta [Operazioni con gli oggetti](#) ed [Elementi delle policy JSON IAM: Effect](#) nella Guida per l'utente IAM.

Eliminazione di un bucket per uso generico

Un bucket per uso generico Amazon S3 vuoto può essere eliminato. Per ulteriori informazioni sull'eliminazione del contenuto di un bucket per uso generico, consulta [the section called "Eliminazione del contenuto di un bucket per uso generico"](#).

Puoi eliminare un bucket utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

 Important

Prima di eliminare un bucket per uso generico, considera quanto segue:

- Se un bucket viene eliminato, non può essere ripristinato da AWS. Prima di eliminare un bucket, accertati di aver eseguito il backup o la replica dei dati.
- I nomi dei bucket per uso generico sono univoci all'interno di uno spazio dei nomi globale. Se elimini un bucket nello spazio dei nomi globale condiviso, tieni presente che un altro Account AWS può utilizzare lo stesso nome di bucket generico per un nuovo bucket e può quindi potenzialmente ricevere richieste destinate al bucket eliminato. Per evitare che ciò accada o continuare a utilizzare lo stesso nome del bucket, non eliminare il bucket. È consigliabile eliminare il contenuto del bucket e conservarlo, bloccando le richieste di bucket in base alle esigenze. Per i bucket non più in uso, è consigliabile eliminare tutti gli oggetti del bucket per ridurre al minimo i costi e mantenere il bucket stesso.
- Ti consigliamo di creare bucket nello spazio dei nomi regionale del tuo account per assicurarti che solo il tuo account possa possedere questi nomi di bucket. Per ulteriori informazioni, consulta [Namespace per bucket generici](#).
- Quando si elimina un bucket per uso generico, il bucket potrebbe non essere immediatamente rimosso. Amazon S3 mette in coda il bucket per l'eliminazione. Poiché Amazon S3 è distribuito su più livelli Regioni AWS, il processo di eliminazione richiede tempo per propagarsi completamente e raggiungere la coerenza in tutto il sistema.
- Se il bucket ospita un sito Web statico e hai creato e configurato una zona ospitata di Amazon Route 53 come descritto in [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#), devi ripulire le impostazioni della zona ospitata di Route 53 associate al bucket. Per ulteriori informazioni, consulta [Passaggio 2: eliminare la zona ospitata Route 53](#).
- Se il bucket riceve i dati di log da Elastic Load Balancing (ELB), è consigliabile arrestare la distribuzione dei log ELB al bucket prima dell'eliminazione. Dopo l'eliminazione del bucket, se un altro utente crea un bucket utilizzando lo stesso nome, i dati di log potrebbero potenzialmente essere consegnati a quel bucket. Per informazioni sui log di accesso ELB, consulta [Log di accesso per Classic Load Balancer](#) nella Guida per l'utente di Classic Load Balancer e [Log di accesso per Application Load Balancer](#) nella Guida per l'utente di Application Load Balancer.

Risoluzione dei problemi

Se non riesci a eliminare un bucket per uso generico Amazon S3, considera quanto segue:

- Assicurati che il bucket sia vuoto: puoi eliminare solo bucket che non hanno oggetti al loro interno. Assicurati che il bucket sia vuoto. Per ulteriori informazioni sull'eliminazione del contenuto di un bucket, consulta [the section called “Eliminazione del contenuto di un bucket per uso generico”](#).
- Assicurati che non vi siano punti di accesso collegati: puoi eliminare i bucket solo se non hanno punti di accesso o punti di accesso S3 collegati nello Multi-Region stesso account. Prima di eliminare il bucket, elimina tutti i punti di accesso dello stesso account collegati al bucket.
- Assicurati di disporre dell'autorizzazione **s3:DeleteBucket**: se non è possibile eliminare un bucket, chiedi all'amministratore IAM di confermare la presenza dell'autorizzazione **s3:DeleteBucket**. Per informazioni su come visualizzare o aggiornare le autorizzazioni IAM, consulta la sezione [Modifica delle autorizzazioni per un utente IAM](#) nella Guida per l'utente IAM. Per informazioni sulla risoluzione dei problemi, consulta [the section called “Risoluzione dei problemi relativi agli errori di accesso negato \(403 Forbidden\)”](#).
- Controlla la presenza di istruzioni **s3:DeleteBucket Deny** nelle policy di controllo dei servizi AWS Organizations e nelle policy di controllo delle risorse (RCP): le policy di controllo dei servizi e le policy di controllo delle risorse (RCP) possono negare l'autorizzazione all'eliminazione di un bucket. Per ulteriori informazioni, consulta le [policy di controllo dei servizi](#) e le [policy di controllo delle risorse](#) nella Guida all'utente AWS Organizations .
- Controlla la presenza di istruzioni **s3:DeleteBucket Deny** nella policy di bucket: se disponi delle autorizzazioni **s3:DeleteBucket** nella policy del ruolo o dell'utente IAM e non è possibile eliminare un bucket, la policy di bucket potrebbe includere un'istruzione Deny per **s3:DeleteBucket**. Per impostazione predefinita, i bucket creati da AWS Elastic Beanstalk hanno una policy contenente questa dichiarazione. Prima di poter eliminare il bucket, è necessario eliminare questa istruzione o la policy del bucket.

Prerequisiti

Prima di eliminare un bucket per uso generico, è necessario eliminarne il contenuto. Per ulteriori informazioni sull'eliminazione del contenuto di un bucket, consulta [the section called “Eliminazione del contenuto di un bucket per uso generico”](#).

Utilizzo della console S3

Per eliminare un bucket S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket, seleziona il pulsante di opzione accanto al nome del bucket che desideri eliminare, quindi scegli Elimina.
4. Nella pagina Delete bucket (Elimina bucket) conferma che desideri eliminare il bucket inserendone il nome nel campo di testo e quindi scegli Delete bucket (Elimina bucket).

Note

Se il bucket contiene oggetti, elimina il contenuto prima di eliminare il bucket scegliendo il pulsante Elimina il contenuto del bucket nell'avviso di errore Questo bucket non è vuoto e seguendo le istruzioni riportate nella pagina Elimina il contenuto del bucket. Quindi tornare alla pagina Delete bucket (Elimina bucket) ed eliminare il bucket.

5. Per verificare di aver eliminato il bucket, apri l'elenco Bucket per uso generico e inserisci il nome del bucket eliminato. Se il bucket non appare tra i risultati, la cancellazione si è conclusa correttamente.

Utilizzo di AWS SDK per Java

Per svuotare ed eliminare un bucket generico utilizzando l' AWS SDK per Java, devi prima eliminare tutti gli oggetti nel bucket generico, quindi eliminare il bucket.

Per esempi in altre lingue, consulta [Use DeleteBucket with an AWS SDK o CLI](#) nell'Amazon Simple Storage Service API Reference. Per informazioni sull'utilizzo di altri AWS SDK, consulta [Tools for Amazon Web Services](#).

Java

Per eliminare un bucket che contiene oggetti utilizzando l' AWS SDK per Java, devi prima eliminare tutti gli oggetti e poi eliminare il bucket. Questo approccio vale sia per i bucket che supportano il controllo delle versioni sia per quelli che non lo supportano.

 Note

Per i bucket che non supportano la funzione Controllo delle versioni, è possibile eliminare direttamente tutti gli oggetti e poi il bucket stesso. Per i bucket che supportano la funzione Controllo delle versioni, è necessario eliminare tutte le versioni degli oggetti prima di eliminare il bucket.

Per esempi di come eliminare un bucket con l' AWS SDK per Java, consulta [Eliminare un bucket](#) nell'Amazon S3 API Reference.

Utilizzo di AWS CLI

Puoi eliminare un bucket generico che contiene oggetti con l'opzione AWS CLI se il bucket non ha il controllo delle versioni abilitato. Quando elimini un bucket che contiene oggetti, tutti gli oggetti nel bucket vengono eliminati definitivamente, inclusi gli oggetti che sono passati alla classe di archiviazione S3 Glacier Flexible Retrieval.

Se il bucket non ha il controllo delle versioni abilitato, puoi usare il AWS CLI comando `rb` (remove bucket) con il `--force` parametro per eliminare il bucket e tutti gli oggetti in esso contenuti. Questo comando elimina prima tutti gli oggetti e quindi il bucket stesso.

Se il controllo delle versioni è abilitato, l'utilizzo del comando `rb` con il parametro `--force` non elimina gli oggetti con il controllo delle versioni, quindi l'eliminazione del bucket non riesce perché il bucket non è vuoto. Per ulteriori informazioni sull'eliminazione di oggetti con versione, consulta la sezione [Eliminazione delle versioni degli oggetti](#).

Per utilizzare il seguente comando, sostituisci *amzn-s3-demo-bucket* con il nome del bucket da eliminare:

```
$ aws s3 rb s3://amzn-s3-demo-bucket --force
```

Per ulteriori informazioni, consulta [Usare i comandi High-Level S3 con il nella Guida per l' AWS Command Line Interface](#)utente. AWS Command Line Interface

Montaggio di un bucket Amazon S3 come file system locale

Mountpoint per Amazon S3 è un client di file open source ad alta velocità di trasmissione effettiva per il montaggio di un bucket Amazon S3 come file system locale. Con Mountpoint, le applicazioni possono accedere agli oggetti archiviati in Amazon S3 tramite operazioni sui file system, come apertura e lettura. Mountpoint converte automaticamente queste operazioni in chiamate API a oggetti S3, offrendo alle applicazioni l'accesso all'archiviazione elastica e alla velocità di trasmissione effettiva di Amazon S3 tramite un'interfaccia di file.

Mountpoint per Amazon S3 è [disponibile per l'uso in produzione su applicazioni ad alta lettura su larga scala](#): data lake, apprendimento per il machine learning, rendering di immagini, simulazione di veicoli autonomi, estrazione, trasformazione e caricamento (ETL) e altro ancora.

Mountpoint supporta le operazioni di base del file system e può leggere file di dimensioni fino a 50 TB. Può elencare e leggere file esistenti e crearne di nuovi. Non può modificare file esistenti o eliminare directory e non supporta collegamenti simbolici o il blocco dei file. Mountpoint è ideale per le applicazioni che non richiedono tutte le funzionalità e le POSIX-style autorizzazioni di un file system condiviso, ma richiedono il throughput elastico di Amazon S3 per leggere e scrivere set di dati S3 di grandi dimensioni. Per i dettagli, consulta [Mountpoint file system behavior](#) su GitHub. Per carichi di lavoro che richiedono il supporto POSIX completo, è consigliabile utilizzare [Amazon FSx per Lustre](#) e il relativo [supporto per il collegamento di bucket Amazon S3](#).

Mountpoint per Amazon S3 è disponibile solo per sistemi operativi Linux. Puoi utilizzare Mountpoint per accedere agli oggetti S3 in tutte le classi di storage tranne S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Archive Access Tier e S3 Deep Archive Access Tier. Intelligent-Tiering

Argomenti

- [Installazione di Mountpoint](#)
- [Configurazione e utilizzo di Mountpoint](#)
- [Risoluzione dei problemi di Mountpoint](#)

Installazione di Mountpoint

Puoi scaricare e installare pacchetti predefiniti di Mountpoint per Amazon S3 utilizzando la riga di comando. Le istruzioni per scaricare e installare Mountpoint variano a seconda del sistema operativo Linux che stai utilizzando.

Argomenti

- [Amazon Linux 2023 \(AL2023\)](#)
- [Altre RPM-based distribuzioni \(Amazon Linux 2, Fedora, CentOS, RHEL\)](#)
- [DEBdistribuzioni basate su \(Debian, Ubuntu\)](#)
- [Altro Linux distribuzioni](#)
- [Verifica della firma del pacchetto Mountpoint per Amazon S3](#)

Amazon Linux 2023 (AL2023)

Mountpoint è disponibile direttamente nel repository Amazon Linux 2023 a partire dalla versione AL2023 2023.9.20251110.

1. Installalo inserendo il seguente comando:

```
sudo dnf install mount-s3
```

2. Verifica che Mountpoint for Amazon S3 sia installato correttamente:

```
mount-s3 --version
```

Verrà visualizzato un output simile al seguente:

```
mount-s3 1.21.0+1.amzn2023
```

Altre RPM-based distribuzioni (Amazon Linux 2, Fedora, CentOS, RHEL)

1. Copia il seguente URL di download per la tua architettura.

x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
```

ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.rpm
```

2. Scarica il pacchetto Mountpoint per Amazon S3. Sostituisci *download-link* con l'URL di download appropriato della fase precedente.

```
wget download-link
```

3. (Facoltativo) Verifica dell'integrità e dell'autenticità dei file scaricati. Per prima cosa, copia l'URL della firma appropriato per la tua architettura.

x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm.asc
```

ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.rpm.asc
```

Quindi, consulta [Verifica della firma del pacchetto Mountpoint per Amazon S3](#).

4. Installa il pacchetto utilizzando il seguente comando:

```
sudo yum install ./mount-s3.rpm
```

5. Verifica che Mountpoint sia installato correttamente inserendo il seguente comando:

```
mount-s3 --version
```

Verrà visualizzato un output simile al seguente:

```
mount-s3 1.21.0
```

DEBdistribuzioni basate su (Debian, Ubuntu)

1. Copia l'URL di download per la tua architettura.

x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.deb
```

ARM64 (Graviton):


```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.deb
```

2. Scarica il pacchetto Mountpoint per Amazon S3. Sostituisci *download-link* con l'URL di download appropriato della fase precedente.

```
wget download-link
```

3. (Facoltativo) Verifica dell'integrità e dell'autenticità dei file scaricati. Innanzitutto, copia l'URL della firma per la tua architettura.

x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.deb.asc
```

ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.deb.asc
```

Quindi, consulta [Verifica della firma del pacchetto Mountpoint per Amazon S3](#).

4. Installa il pacchetto utilizzando il seguente comando:

```
sudo apt-get install ./mount-s3.deb
```

5. Verifica che Mountpoint per Amazon S3 sia installato correttamente eseguendo il seguente comando:

```
mount-s3 --version
```

Verrà visualizzato un output simile al seguente:

```
mount-s3 1.21.0
```

Altro Linux distribuzioni

1. Consulta la documentazione del sistema operativo per installare i pacchetti FUSE e libfuse2, che sono obbligatori.

2. Copia l'URL di download per la tua architettura.

x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.tar.gz
```

ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.tar.gz
```

3. Scarica il pacchetto Mountpoint per Amazon S3. Sostituisci *download-link* con l'URL di download appropriato della fase precedente.

```
wget download-link
```

4. (Facoltativo) Verifica dell'integrità e dell'autenticità dei file scaricati. Innanzitutto, copia l'URL della firma per la tua architettura.

x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.tar.gz.asc
```

ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.tar.gz.asc
```

Quindi, consulta [Verifica della firma del pacchetto Mountpoint per Amazon S3](#).

5. Installa il pacchetto utilizzando il seguente comando:

```
sudo mkdir -p /opt/aws/mountpoint-s3 && sudo tar -C /opt/aws/mountpoint-s3 -xzf ./mount-s3.tar.gz
```

6. Aggiungi il file binario mount-s3 alla variabile di ambiente PATH. Nel file \$HOME/.profile, aggiungi la seguente riga:

```
export PATH=$PATH:/opt/aws/mountpoint-s3/bin
```

Salva il file `.profile` ed esegui il seguente comando:

```
source $HOME/.profile
```

7. Verifica che Mountpoint per Amazon S3 sia installato correttamente eseguendo il seguente comando:

```
mount-s3 --version
```

Verrà visualizzato un output simile al seguente:

```
mount-s3 1.21.0
```

Verifica della firma del pacchetto Mountpoint per Amazon S3

1. Installa GnuPG (il comando `gpg`). È necessario verificare l'autenticità e l'integrità di un pacchetto Mountpoint per Amazon S3 scaricato. GnuPG è installato per impostazione predefinita sulle Amazon Machine Images (AMI) di Amazon Linux. Dopo l'installazione di GnuPG, passa alla fase 2.
2. Scarica la chiave pubblica Mountpoint eseguendo il seguente comando:

```
wget https://s3.amazonaws.com/mountpoint-s3-release/public_keys/KEYS
```

3. Importa la chiave pubblica Mountpoint nel keyring eseguendo il seguente comando:

```
gpg --import KEYS
```

4. Verifica l'impronta digitale della chiave pubblica Mountpoint eseguendo il seguente comando:

```
gpg --fingerprint mountpoint-s3@amazon.com
```

Verificare che la stringa di impronte digitali visualizzata corrisponda a una delle seguenti:

```
8AEF E705 EBE3 29C0 948C 75A6 6F1C 3B3A EF4B 030B  
673F E406 1506 BB46 9A0E F857 BE39 7A52 B086 DA5A (older key)
```

Se la stringa di impronte digitali non corrisponde, non terminare l'installazione di Mountpoint e contatta [Supporto AWS](#).

5. Scarica il file SIGNATURE del pacchetto. Sostituisci *signature-link* con l'apposito link per la firma riportato nelle sezioni precedenti.

```
wget signature-link
```

6. Verifica la firma del pacchetto scaricato eseguendo il seguente comando. Sostituisci *signature-filename* con il nome del file della fase precedente.

```
gpg --verify signature-filename
```

Ad esempio, nelle RPM-based distribuzioni, incluso Amazon Linux, inserisci il seguente comando:

```
gpg --verify mount-s3.rpm.asc
```

7. L'output deve includere la frase Good signature. Se l'output include la frase BAD signature, scarica nuovamente il file del pacchetto Mountpoint e ripeti queste fasi. Se il problema persiste, non terminare l'installazione di Mountpoint e contatta [Supporto AWS](#).

L'output può includere un avviso relativo a una firma attendibile. Ciò non indica un problema. Significa solo che non hai verificato in modo indipendente la chiave pubblica Mountpoint.

Configurazione e utilizzo di Mountpoint

Per utilizzare Mountpoint per Amazon S3, il tuo host ha bisogno di AWS credenziali valide con accesso al bucket o ai bucket Amazon S3 che desideri montare. Per le diverse modalità di autenticazione, consulta Mountpoint [AWS Credentials](#) su GitHub.

Ad esempio, puoi creare un nuovo utente e ruolo AWS Identity and Access Management (IAM) per questo scopo. Assicurati che questo ruolo abbia accesso al bucket o ai bucket che desideri montare. Puoi [passare il ruolo IAM](#) all'istanza Amazon EC2 con un profilo dell'istanza.

Argomenti

- [Utilizzo di Mountpoint per Amazon S3](#)
- [Configurazione della memorizzazione nella cache in Mountpoint](#)

Utilizzo di Mountpoint per Amazon S3

Usa Mountpoint per Amazon S3 per effettuare le seguenti operazioni:

1. Montaggio dei bucket Amazon S3.
 - a. È possibile montare i bucket Amazon S3 manualmente utilizzando il comando `mount-s3`.

Nell'esempio seguente, sostituisci `amzn-s3-demo-bucket` con il nome del bucket S3 e sostituisci `~/mnt` con la directory sull'host in cui desideri che venga montato il bucket S3.

```
mkdir ~/mnt
mount-s3 amzn-s3-demo-bucket ~/mnt
```

Poiché il client Mountpoint viene eseguito in background per impostazione predefinita, la directory `~/mnt` ora fornisce l'accesso agli oggetti nel bucket Amazon S3.

- b. In alternativa, a partire da Mountpoint v1.18, puoi configurare il montaggio automatico dei bucket Amazon S3 all'avvio o al riavvio di un'istanza.

Per le istanze Amazon EC2 esistenti o in esecuzione, trova il file `fstab` nella directory `/etc/fstab` del sistema Linux. Quindi, aggiungi una riga al file `fstab`. Ad esempio, per eseguire il montaggio di `amzn-s3-demo-bucket` utilizzando il prefisso `example-prefix/` nel percorso di sistema `/mnt/mountpoint`, attieniti a quanto segue. Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate.

```
s3://amzn-s3-demo-bucket/example-prefix/ /mnt/mountpoint mount-s3
_netdev,nosuid,nodev,nofail,rw 0 0
```

Consulta la tabella seguente per una spiegazione delle opzioni utilizzate nell'esempio.

Opzione	Description
<code>_netdev</code>	Specifica che il file system richiede una rete per il montaggio.
<code>nosuid</code>	Specifica che il file system non può contenere file con ID utente impostati.

Opzione	Description
nodev	Specifica che il file system non può contenere dispositivi speciali.
nofail	Specifica che il mancato montaggio del file system deve comunque consentire l'avvio del sistema.
rw	Specifica che il punto di montaggio viene creato con autorizzazioni di lettura e scrittura. In alternativa, utilizza ro per la sola lettura.

Per le nuove istanze Amazon EC2, è possibile modificare i dati utente su un modello Amazon EC2 e configurare il file `fstab` come segue. Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate.

```
#!/bin/bash -e
MP_RPM=$(mktemp --suffix=.rpm)
curl https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
  > $MP_RPM
yum install -y $MP_RPM
rm $MP_RPM

MNT_PATH=/mnt/mountpoint
echo "s3://amzn-s3-demo-bucket/ ${MNT_PATH} mount-s3
_netdev,nosuid,nodev,rw,allow-other,nofail" >> /etc/fstab
mkdir $MNT_PATH

systemctl daemon-reload
mount -a
```

2. Accedi agli oggetti nel bucket Amazon S3 tramite Mountpoint.

Dopo aver montato il bucket localmente, puoi utilizzare comandi Linux comuni, come `cat` o `ls`, per lavorare con gli oggetti S3. Mountpoint per Amazon S3 interpreta le chiavi nel bucket Amazon S3 come percorsi di file system suddividendole al carattere barra (/). Ad esempio, se

disponi della chiave oggetto `Data/2023-01-01.csv` nel bucket, nel file system Mountpoint avrai una directory denominata `Data`, con un file denominato `2023-01-01.csv` al suo interno.

Mountpoint per Amazon S3 non implementa intenzionalmente la specifica standard completa [POSIX](#) per i file system. Mountpoint è ottimizzato per carichi di lavoro che richiedono un accesso in lettura e scrittura con elevato throughput ai dati archiviati in Amazon S3 tramite un'interfaccia di file system, ma che per il resto non si basano sulle funzionalità del file system. Per ulteriori informazioni, consulta Mountpoint for Amazon S3 [file system behavior](#) su GitHub. I clienti che necessitano di una semantica dei file system più completa dovrebbero prendere in considerazione altri servizi di file, come [Amazon Elastic AWS File System \(Amazon EFS\)](#) o [Amazon FSx](#). <https://aws.amazon.com/fsx/>

3. Smonta il bucket Amazon S3 utilizzando il comando `umount`. Questo comando smonta il bucket S3 ed esce da Mountpoint.

Per utilizzare il comando di esempio seguente, sostituisci `~/mnt` con la directory sull'host in cui è montato il bucket S3.

```
umount ~/mnt
```

Note

Per ottenere un elenco di opzioni per questo comando, esegui `umount --help`.

Per ulteriori dettagli sulla configurazione di Mountpoint, consulta [Amazon S3 bucket configuration](#) e [File system configuration](#) in GitHub.

Configurazione della memorizzazione nella cache in Mountpoint

Mountpoint per Amazon S3 supporta diversi tipi di cache dei dati. Per accelerare le richieste di lettura ripetute, è possibile scegliere quanto segue:

- **Cache locale** - È possibile utilizzare una cache locale nello storage dell'istanza Amazon EC2 o in un volume Amazon Elastic Block Store. Se si leggono ripetutamente gli stessi dati dalla stessa istanza di calcolo e se si dispone di spazio inutilizzato nello storage dell'istanza locale per il set di dati letto ripetutamente, si dovrebbe optare per una cache locale.

- **Cache condivisa** - È possibile utilizzare una cache condivisa su S3 Express One Zone. Se si leggono ripetutamente oggetti di piccole dimensioni da più istanze di calcolo o se non si conoscono le dimensioni del set di dati letto ripetutamente e si vuole beneficiare dell'elasticità delle dimensioni della cache, si dovrebbe optare per la cache condivisa. Una volta effettuata l'iscrizione, Mountpoint conserva gli oggetti con dimensioni fino a un megabyte in un bucket di directory che utilizza S3 Express One Zone.
- **Cache locale e condivisa combinate** - Se si dispone di spazio inutilizzato nella cache locale, ma si desidera anche una cache condivisa tra più istanze, è possibile optare per una cache locale e una cache condivisa.

La memorizzazione nella cache in Mountpoint è ideale per i casi d'uso in cui si leggono ripetutamente gli stessi dati che non cambiano durante le letture multiple. Ad esempio, puoi utilizzare la memorizzazione nella cache per le attività di training di machine learning che richiedono una lettura ripetuta di un set di dati di training per migliorare l'accuratezza del modello.

Per ulteriori informazioni su come configurare la cache in Mountpoint, consulta gli esempi seguenti.

Argomenti

- [Cache locale](#)
- [Cache condivisa](#)
- [Cache locale e condivisa combinate](#)

Cache locale

È possibile accedere a una cache locale con il flag `--cache` **CACHE_PATH**. Nell'esempio seguente, sostituisci **CACHE_PATH** con il percorso file della directory in cui desideri memorizzare i dati nella cache. Sostituisci **amzn-s3-demo-bucket** con il nome del bucket Amazon S3 e sostituisci **~/mnt** con la directory dell'host in cui desideri che venga montato il bucket S3.

```
mkdir ~/mnt
mount-s3 --cache CACHE_PATH amzn-s3-demo-bucket ~/mnt
```

Quando si opta per la cache locale durante l'installazione di un bucket Amazon S3, Mountpoint crea nella posizione della cache configurata una sottodirectory vuota, se non esiste già. Quando si installa per la prima volta un bucket e quando lo si disinstalla, Mountpoint cancella il contenuto della cache locale.

⚠ Important

Se si abilita la cache locale, Mountpoint mantiene il contenuto degli oggetti non crittografati del bucket Amazon S3 montato nella posizione della cache locale fornita al momento del montaggio. Per proteggere i dati, è necessario limitare l'accesso alla posizione della cache dei dati utilizzando i meccanismi di controllo dell'accesso al file system.

Cache condivisa

Se si leggono ripetutamente oggetti di piccole dimensioni (fino a 1 MB) da più istanze di calcolo o se le dimensioni dei set di dati letti ripetutamente superano spesso le dimensioni della cache locale, è consigliabile utilizzare una cache condivisa in [S3 Express One Zone](#). Quando si leggono ripetutamente gli stessi dati da più istanze, questo approccio migliora la latenza evitando richieste ridondanti al bucket Amazon S3 montato.

Una volta che si opta per la cache condivisa, si paga per i dati memorizzati nella cache del proprio bucket di directory in S3 Express One Zone. Paga anche per le richieste effettuate sui dati nel bucket della directory in S3 Express One Zone. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Mountpoint non cancella mai gli oggetti memorizzati nella cache dai bucket di directory. Per gestire i costi di archiviazione, è necessario impostare una [policy del ciclo di vita sul bucket della directory](#), in modo che Amazon S3 faccia scadere i dati memorizzati nella cache in S3 Express One Zone dopo un periodo di tempo specificato dall'utente. Per ulteriori informazioni, consulta [Configurazione della cache Mountpoint per Amazon S3](#) su GitHub.

Per abilitare la cache in S3 Express One Zone quando si monta un bucket Amazon S3 sull'istanza di calcolo, occorre utilizzare il flag `--cache-xz` e specificare un bucket di directory come posizione della cache. Nel seguente esempio, sostituisci il *user input placeholders*

```
mount-s3 amzn-s3-demo-bucket ~/mnt --cache-xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

Cache locale e condivisa combinate

Se si dispone di spazio inutilizzato nell'istanza ma si desidera anche una cache condivisa tra più istanze, è possibile optare per una cache locale e una cache condivisa. Con questa configurazione della cache, è possibile evitare richieste di lettura ridondanti dalla stessa istanza alla cache condivisa nel bucket della directory quando i dati richiesti sono memorizzati nella cache locale. Questo può ridurre i costi di richiesta e migliorare le prestazioni.

Per abilitare sia la cache locale sia la cache condivisa quando si monta un bucket Amazon S3, si specificano entrambe le posizioni della cache utilizzando i flag `--cache` e `--cache-xz`. Per utilizzare l'esempio seguente per attivare sia una cache locale che condivisa, sostituisci il *user input placeholders*.

```
mount -s3 amzn-s3-demo-bucket ~/mnt --cache /path/to/mountpoint/cache --cache -xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

Per ulteriori informazioni, consulta [Configurazione della cache Mountpoint per Amazon S3](#) su GitHub.

Important

Se si abilita la cache condivisa, Mountpoint copia il contenuto degli oggetti dal bucket Amazon S3 montato nel bucket di directory S3 fornito come posizione della cache condivisa, rendendolo accessibile a qualsiasi chiamante con accesso al bucket di directory S3. Per proteggere i dati memorizzati nella cache, è necessario seguire [Best practice di sicurezza per Amazon S3](#) per assicurarsi che i bucket utilizzino le policy corrette e non siano accessibili pubblicamente. È necessario utilizzare un bucket di directory dedicato alla cache condivisa di Mountpoint e concedere l'accesso solo ai client Mountpoint.

Risoluzione dei problemi di Mountpoint

Mountpoint per Amazon S3 è supportato da. Supporto Se hai bisogno di assistenza, contatta il [Supporto AWS Center](#).

Puoi anche esaminare e inviare [Problemi](#) relativi a Mountpoint su GitHub.

Se scopri un potenziale problema di sicurezza in questo progetto, ti chiediamo di segnalarlo ad AWS Security tramite la [pagina di segnalazione delle vulnerabilità](#). Non creare un problema GitHub pubblico.

Se l'applicazione si comporta in modo imprevisto con Mountpoint, è possibile controllare le informazioni dei log per diagnosticare il problema.

Registrazione di log

Per impostazione predefinita, Mountpoint emette informazioni di log ad elevata gravità per [syslog](#).

Per visualizzare i log sulla maggior parte delle distribuzioni Linux moderne, incluso Amazon Linux, esegui il seguente comando `journalctl`:

```
journalctl -e SYSLOG_IDENTIFIER=mount-s3
```

Su altri sistemi Linux, le voci `syslog` sono probabilmente scritte in un file come `/var/log/syslog`.

Puoi utilizzare questi log per risolvere i problemi dell'applicazione. Ad esempio, se l'applicazione tenta di sovrascrivere un file esistente, l'operazione non riesce e nel log verrà visualizzata una riga simile alla seguente:

```
[WARN] open{req=12 ino=2}: mountpoint_s3::fuse: open failed: inode error: inode 2 (full key "README.md") is not writable
```

Per ulteriori informazioni, consulta Mountpoint for Amazon S3 [Logging](#) su GitHub.

Operazioni con Storage Browser per Amazon S3

[Storage Browser per S3](#) è un componente open source che si può aggiungere alla propria applicazione web per fornire agli utenti finali una semplice interfaccia grafica per i dati memorizzati in Amazon S3. Con Storage Browser per S3, è possibile fornire agli utenti finali autorizzati l'accesso a sfogliare, scaricare, caricare, copiare ed eliminare dati in S3 direttamente dalle proprie applicazioni.

Storage Browser per S3 supporta le seguenti operazioni per i file: LIST, GET, PUT, COPY, UPLOAD e DELETE. Per garantire un elevato throughput di trasferimento dei dati, Storage Browser per S3 visualizza solo i dati a cui gli utenti finali sono autorizzati ad accedere e ottimizza le richieste di upload. Storage Browser ottimizza inoltre le prestazioni per velocizzare i tempi di caricamento, calcola le checksum dei dati caricati dagli utenti finali e accetta gli oggetti dopo aver confermato che l'integrità dei dati è stata mantenuta (in transito) su Internet pubblica. Puoi controllare l'accesso ai tuoi dati in base all'identità dell'utente finale utilizzando i servizi AWS di sicurezza e identità o i tuoi servizi gestiti. È inoltre possibile personalizzare Storage Browser per adattarlo al design e al marchio dell'applicazione esistente.

Storage Browser per S3 è disponibile solo per applicazioni web e intranet sul framework React. Puoi utilizzare Storage Browser per accedere agli oggetti Amazon S3 in tutte le classi di storage tranne S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Archive Access tier e S3 Deep Intelligent-Tiering Archive Access tier. Intelligent-Tiering

Storage Browser per S3 è disponibile per essere utilizzato con le applicazioni web nella libreria [AWS Amplify React](#). Per ulteriori informazioni su Storage Browser, consulta [Storage Browser per S3](#).

Argomenti

- [Utilizzo di Storage Browser per S3](#)
- [Installazione di Storage Browser per S3](#)
- [Impostazione di Storage Browser per S3](#)
- [Configurazione di Storage Browser per S3](#)
- [Risoluzione dei problemi di Storage Browser per S3](#)

Utilizzo di Storage Browser per S3

In Storage Browser per S3, una posizione è un prefisso o un bucket per uso generico S3 a cui hanno accesso gli utenti finali tramite [S3 Access Grants](#), policy IAM o il proprio servizio di autorizzazione gestito. Dopo aver autorizzato gli utenti finali ad accedere a una posizione specifica, possono lavorare con tutti i dati presenti in quella posizione.

L'interfaccia utente di Storage Browser per S3 presenta quattro viste principali:

- Home page: la home page elenca le posizioni S3 a cui gli utenti possono accedere e le autorizzazioni per ciascuna di esse. Questa è la visualizzazione iniziale per gli utenti che mostra le risorse S3 di livello root a cui hanno accesso gli utenti finali e le autorizzazioni () per ogni sede S3. READ/WRITE/READWRITE
- Dettagli sulla posizione: questa vista consente agli utenti di sfogliare i file e le cartelle in S3 e di caricare o scaricare i file (si noti che in Storage Browser per S3 gli oggetti sono noti come file, mentre i prefissi e i bucket sono noti come cartelle).
- Azione sulla posizione: dopo che l'utente sceglie un'azione (come Carica) in Storage Browser, si apre un'altra vista della posizione del file.
- Puntini di sospensione in verticale: l'icona dei puntini di sospensione in verticale apre l'elenco a discesa delle azioni.

Quando si utilizza Storage Browser per S3, tieni presente le seguenti limitazioni:

- Le cartelle che iniziano o terminano con punti (.) non sono supportate.
- Non sono supportati S3 Access Grants con autorizzazione solo WRITE.

- Storage Browser per S3 supporta l'operazione PUT per file di dimensioni fino a 160 GB.
- Storage Browser per S3 supporta l'operazione COPY solo per i file di dimensioni inferiori a 5 GB. Se le dimensioni del file superano i 5 GB, Storage Browser rifiuta la richiesta.

Installazione di Storage Browser per S3

Il modo più veloce per iniziare a usare Storage Browser è clonare uno dei progetti di esempio su GitHub. Questi progetti di esempio possono aiutarti a implementare app Web pronte per la produzione per Storage Browser con integrazioni di AWS servizi preimpostate per AWS Identity and Access Management connettere rapidamente gli utenti finali autorizzati ai dati in S3.

Per ulteriori informazioni, consultare [Quick start](#) in Amplify Dev Center.

Installazione di Storage Browser per S3 da GitHub

In alternativa, puoi installare Storage Browser per S3 dalla versione più recente `aws-amplify/ui-react-storage` e dai `aws-amplify` pacchetti presenti nel [aws-amplify](#) GitHub repository per iniziare a integrare Storage Browser nell'applicazione esistente. Quando si installa Storage Browser per S3, assicurati di aggiungere le seguenti dipendenze al file `package.json`:

```
"dependencies": {  
  "aws-amplify/ui-react-storage": "latest",  
  "aws-amplify": "latest",  
}
```

In alternativa, è possibile aggiungere le dipendenze utilizzando Node Package Manager (NPM):

```
npm i --save @aws-amplify/ui-react-storage aws-amplify
```

Impostazione di Storage Browser per S3

Per collegare gli utenti finali alle posizioni Amazon S3, è necessario prima impostare un metodo di autenticazione e autorizzazione. Esistono tre metodi per impostare un metodo di autenticazione e autorizzazione con Storage Browser:

- [Metodo 1: Gestione dell'accesso ai dati per i clienti e partner terzi](#)
- [Metodo 2: gestione dell'accesso ai dati per i tuoi presidi IAM per conto tuo AWS account](#)
- [Metodo 3: Gestione dell'accesso ai dati su larga scala](#)

Metodo 1: Gestione dell'accesso ai dati per i clienti e partner terzi

Con questo metodo, è possibile utilizzare [AWS Amplify Auth](#) per gestire il controllo degli accessi e la sicurezza dei file. Questo metodo è ideale quando si desidera collegare i clienti o i partner di terze parti con i dati presenti in S3. Con questa opzione, i clienti possono autenticarsi utilizzando gestori dell'identità sociali o aziendali.

Fornisci le credenziali IAM ai tuoi utenti finali e ai partner terzi utilizzando AWS Amplify Auth con un bucket S3 configurato per utilizzare Amplify Storage. AWS Amplify Auth è basato su [Amazon Cognito](#), un servizio di gestione delle identità e degli accessi dei clienti completamente gestito in cui è possibile autenticare e autorizzare gli utenti da una directory utente o da una directory aziendale integrata o da provider di identità di consumo. Il modello di autorizzazione di Amplify definisce a quali prefissi può accedere l'utente attualmente autenticato. Per ulteriori informazioni su come impostare l'autorizzazione per AWS Amplify, consulta [Impostazione dell'archiviazione](#).

Per inizializzare il componente con i metodi di autenticazione e archiviazione di Amplify, aggiungere il seguente frammento di codice all'applicazione web:

```
import {
  createAmplifyAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

import config from './amplify_outputs.json';

Amplify.configure(config);

export const { StorageBrowser } = createStorageBrowser({
  config: createAmplifyAuthAdapter(),
});
```

Metodo 2: gestione dell'accesso ai dati per i tuoi presidi IAM per conto tuo AWS account

Se desideri gestire l'accesso per i tuoi principali IAM o Account AWS direttamente, puoi creare un ruolo IAM con le autorizzazioni per richiamare l'operazione dell'[GetDataAccess](#) API S3. Per configurarlo, è necessario creare un'istanza S3 Access Grants per mappare le autorizzazioni per i prefissi e i bucket per uso generico S3 alle identità IAM specificate. Il componente Storage Browser (che deve essere chiamato sul lato client dopo aver ottenuto le credenziali IAM) invoca

quindi l'operazione API [ListCallerAccessGrants](#) S3 per recuperare le concessioni disponibili per il richiedente dell'identità e popolarne le posizioni nel componente. Dopo aver ottenuto l'autorizzazione `s3:GetDataAccess`, le credenziali vengono utilizzate dal componente Storage Browser per richiedere l'accesso ai dati a S3.

```
import {
  createManagedAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

export const { StorageBrowser } = createStorageBrowser({
  config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
          sessionToken: 'my-session-token',
          expiration: new Date()
        },
      },
    },
  },
  // AWS `region` and `accountId`
  region: '',
  accountId: '',
  // call `onAuthStateChange` when end user auth state changes
  // to clear sensitive data from the `StorageBrowser` state
  registerAuthListener: (onAuthStateChange) => {},
});
```

Metodo 3: Gestione dell'accesso ai dati su larga scala

Se si desidera associare un'istanza di [S3 Access Grants](#) al proprio Centro identità IAM per una soluzione più scalabile (ad esempio per fornire l'accesso ai dati a tutta l'azienda), è possibile richiedere i dati da Amazon S3 per conto dell'utente corrente autenticato. Ad esempio, è possibile concedere ai gruppi di utenti della directory aziendale l'accesso ai dati in S3. Questo approccio consente di gestire centralmente le autorizzazioni di S3 Access Grants per i vostri utenti e gruppi, compresi quelli ospitati da fornitori esterni come Microsoft Entra, Okta e altri.

Quando si utilizza questo metodo, l'[integrazione con il Centro identità IAM](#) consente di utilizzare le directory utenti esistenti. Un altro vantaggio della propagazione dell'identità attendibile del Centro identità IAM è che ogni [evento di dati AWS CloudTrail per Amazon S3](#) contiene un riferimento diretto all'identità dell'utente finale che ha avuto accesso ai dati S3.

Se disponi di un'applicazione che supporta OAuth 2.0 e i tuoi utenti devono accedere da queste applicazioni ai AWS servizi, ti consigliamo di utilizzare una propagazione affidabile delle identità. Grazie alla propagazione affidabile dell'identità, un utente può accedere a un'applicazione e tale applicazione può trasmettere l'identità dell'utente in qualsiasi richiesta che acceda ai dati nei servizi. AWS Questa applicazione interagisce con il Centro identità IAM per conto degli utenti autenticati. Per ulteriori informazioni, consulta [Utilizzo della propagazione dell'identità attendibile con le applicazioni gestite dai clienti](#).

[La propagazione affidabile delle identità](#) è una Centro identità AWS IAM funzionalità che gli amministratori di connected Servizi AWS possono utilizzare per concedere e controllare l'accesso ai dati del servizio. L'accesso a questi dati si basa su attributi utente come le associazioni di gruppo. L'impostazione di una propagazione affidabile delle identità richiede la collaborazione tra gli amministratori di connected Servizi AWS e gli amministratori dello IAM Identity Center. Per ulteriori informazioni, consulta [Prerequisites and considerations](#).

Configurazione

Per configurare l'autenticazione di Storage Browser Console di gestione AWS utilizzando [S3 Access Grants](#) e [IAM Identity Center trusted Propagation](#), le applicazioni devono richiedere dati ad Amazon S3 per conto dell'utente autenticato corrente. Con questo approccio, è possibile dare agli utenti o ai gruppi di utenti della directory aziendale l'accesso diretto ai bucket, ai prefissi o agli oggetti S3. Ciò significa che l'applicazione non dovrà mappare alcun utente a un principale IAM.

Il seguente flusso di lavoro illustra le fasi di impostazione di Storage Browser per S3, utilizzando il Centro identità IAM e S3 Access Grants:

Fasi	Description
1	Abilita IAM Identity Center per il tuo AWS Organizations
2	Configura AWS Identity and Access Management federazione di Identity Center
3	Aggiungi un emittente di token affidabile nel AWS Identity and Access Management Console Identity Center

Fasi	Description
	L'emittente di token attendibile rappresenta il gestore dell'identità digitale esterno nel Centro identità IAM, consentendo il riconoscimento dei token di identità per gli utenti autenticati dell'applicazione.
4	Crea un ruolo IAM per l'applicazione bootstrap e il portatore di identità
5	Creazione e configurazione dell'applicazione nel Centro identità IAM Questa applicazione interagisce con il Centro identità IAM per conto degli utenti autenticati.
6	Aggiunta di S3 Access Grants come applicazione attendibile per la propagazione dell'identità Questo passaggio collega l'applicazione a S3 Access Grants, in modo che possa effettuare richieste a S3 Access Grants per conto di utenti autenticati.
7	Creazione di una concessione a un utente o un gruppo Questo passaggio sincronizza gli utenti da AWS Identity and Access Management Identity Center con il System for Cross-domain Identity Management (SCIM). SCIM mantiene le identità del Centro identità IAM sincronizzate con quelle del gestore dell'identità digitale.
8	Creazione del componente Storage Browser per S3

Abilita IAM Identity Center per il tuo AWS Organizations

Per abilitare IAM Identity Center per te AWS Organizations, procedi nel seguente modo:

1. Accedi a Console di gestione AWS, utilizzando uno di questi metodi:

1. Nuovo a AWS (utente root): accedi come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.
 2. Già in uso AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.
2. Apri la [console Centro identità IAM](#).
 3. In Abilita il Centro identità IAM, scegli Abilita.

 Note

IAM Identity Center richiede la configurazione di AWS Organizations. Se non hai configurato un'organizzazione, puoi scegliere di AWS crearne una per te. Scegli [Crea AWS organizzazione](#) per completare questo processo.

4. Scegli Abilita con AWS Organizations.
5. Scegli Continua.
6. (Facoltativo) Aggiungi eventuali tag da associare a questa istanza dell'organizzazione.
7. (Facoltativo) Configura l'amministrazione delegata.

 Note

Se si utilizza un ambiente con più account, si consiglia di configurare l'amministrazione delegata. Con l'amministrazione delegata, è possibile limitare il numero di persone che richiedono l'accesso all'account di gestione in AWS Organizations. Per ulteriori informazioni, consulta [Amministrazione delegata](#).

8. Selezionare Salva.

AWS Organizations invia automaticamente un'email di verifica all'indirizzo associato al tuo account di gestione. Potrebbe verificarsi un ritardo prima di ricevere l'e-mail di verifica. Assicurati di verificare l'indirizzo e-mail entro 24 ore, prima che l'e-mail di verifica scada.

Configura AWS Identity and Access Management federazione di Identity Center

Per utilizzare Storage Browser per S3 con gli utenti della directory aziendale, è necessario configurare il Centro identità IAM per utilizzare un gestore dell'identità digitale esterno. È possibile utilizzare il gestore dell'identità digitale preferito di propria scelta. Tuttavia, occorre tenere presente

che ogni gestore dell'identità digitale utilizza impostazioni di configurazione diverse. Per le esercitazioni sull'uso di diversi gestori dell'identità digitale esterni, consulta i [tutorial sulle origini per il Centro identità IAM](#).

Note

Assicurati di registrare l'URL dell'emittente e gli attributi dei destinatari del gestore dell'identità digitale configurato, perché sarà necessario farvi riferimento nelle fasi successive. Se non si dispone dell'accesso o delle autorizzazioni necessarie per configurare un gestore dell'identità digitale, potrebbe essere necessario contattare l'amministratore del gestore dell'identità digitale esterno per ottenerli.

Aggiungi un emittente di token affidabile nel AWS Identity and Access Management Console Identity Center

L'emittente di token attendibile rappresenta il gestore dell'identità digitale esterno nel Centro identità AWS Identity and Access Management, consentendo il riconoscimento dei token di identità per gli utenti autenticati dell'applicazione. Il proprietario dell'account dell'istanza IAM Identity Center nella tua AWS Organizations deve eseguire questi passaggi. Questi passaggi possono essere eseguiti nella console Centro identità IAM o in modo programmatico.

Per aggiungere un emittente di token attendibile nella console di AWS Identity and Access Management Identity Center, procedi nel seguente modo:

1. Apri la [console Centro identità IAM](#).
2. Seleziona Impostazioni.
3. Scegli la scheda Autenticazione.
4. Vai alla sezione Emittenti di token attendibili e compila i seguenti dati:
 1. In URL dell'emittente, inserisci l'URL del gestore dell'identità digitale esterno che funge da emittente di token attendibile. Potrebbe essere necessario contattare l'amministratore del gestore dell'identità digitale esterno per ottenere queste informazioni. Per ulteriori informazioni, vedere [Utilizzo di applicazioni con un emittente di token attendibili](#).
 2. In Nome dell'emittente di token attendibili, inserisci un nome per l'emittente di token attendibili. Questo nome apparirà nell'elenco degli emittenti di token attendibili che è possibile selezionare nella Fase 8, quando una risorsa applicativa è configurata per la propagazione dell'identità.

5. Aggiorna gli attributi di mappatura all'attributo dell'applicazione preferita, dove ogni attributo del gestore dell'identità digitale è mappato a un attributo del Centro identità IAM. Ad esempio, si potrebbe voler [mappare l'attributo dell'applicazione email](#) all'attributo dell'utente del Centro identità IAM email. Per visualizzare l'elenco degli attributi utente consentiti in IAM Identity Center, consulta la tabella in Mappature [degli attributi per la directory AWS gestita di Microsoft AD](#).
6. (Facoltativo) Se desideri aggiungere un tag di risorsa, inserire la coppia chiave e valore. Per aggiungere più tag di risorse, scegli Aggiungi nuovo tag per generare una nuova voce e inserire le coppie di chiavi e valori.
7. Scegli Crea emittente di token attendibili.
8. Una volta terminata la creazione dell'emittente di token attendibili, contatta l'amministratore dell'applicazione per comunicargli il nome dell'emittente di token attendibili, in modo che possa confermare che l'emittente di token attendibili è visibile nella console applicabile.
9. Assicurati che l'amministratore dell'applicazione selezioni questo emittente di token attendibili nella console applicabile per consentire l'accesso degli utenti all'applicazione dalle applicazioni configurate per la propagazione delle identità attendibili.

Crea un ruolo IAM per l'**applicazione** bootstrap e il portatore di identità

Per garantire che l'applicazione bootstrap e gli utenti identity bearer possano lavorare correttamente tra loro, assicurati di [creare due ruoli IAM](#). Un ruolo IAM è necessario per l'applicazione bootstrap e l'altro ruolo IAM deve essere utilizzato per il portatore di identità, ovvero gli utenti finali che accedono all'applicazione web e che richiedono l'accesso tramite S3 Access Grants. L'applicazione bootstrap riceve il token rilasciato dal gestore dell'identità digitale e invoca l'API CreateTokenWithIAM, scambiando questo token con quello rilasciato dal Centro identità.

Crea un ruolo IAM, ad esempio bootstrap-role, con autorizzazioni come le seguenti. Il seguente esempio di policy IAM fornisce le autorizzazioni a bootstrap-role per eseguire lo scambio di token:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "sso-oauth:CreateTokenWithIAM",
    ],
    "Resource": "arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}",
  ]
}
```

```

    "Effect": "Allow"
  },
  {
    "Action": [
      "sts:AssumeRole",
      "sts:SetContext"
    ],
    "Resource": "arn:aws:iam::${AccountId}:role/identity-bearer-role",
    "Effect": "Allow"
  }
]
}

```

Quindi, crea un secondo ruolo IAM (come *identity-bearer-role*), che il gestore di identità utilizza per generare le credenziali IAM. Le credenziali IAM restituite dal gestore di identità all'applicazione web vengono utilizzate dal componente Storage Browser per S3 per consentire l'accesso ai dati S3:

```

{
  "Action": [
    "s3:GetDataAccess",
    "s3:ListCallerAccessGrants",
  ],
  "Resource": "arn:${Partition}:s3:${Region}:${Account}:access-grants/default",
  "Effect": "Allow"
}

```

Questo ruolo IAM (*identity-bearer-role*) deve utilizzare una policy attendibile con la seguente istruzione:

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}"
  },
  "Action": [
    "sts:AssumeRole",
    "sts:SetContext"
  ]
}

```

Creazione e configurazione dell'applicazione nel Centro identità IAM

Note

Prima di iniziare, assicurati di aver creato i ruoli IAM richiesti nel passaggio precedente. In questo passaggio è necessario specificare uno di questi ruoli IAM.

Per creare e configurare un'applicazione gestita dal cliente in AWS IAM Identity Center, procedi nel seguente modo:

1. Apri la [console Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestione clienti.
4. Scegli Aggiungi applicazione.
5. Nella pagina Seleziona tipo di applicazione, alla voce Preferenze di impostazione, scegli Applicazione da configurare presente.
6. In Tipo di applicazione, scegli OAuth 2.0.
7. Scegli Avanti. Viene visualizzata la pagina Specifica applicazione.
8. Nella sezione Nome e descrizione dell'applicazione, inserisci un Nome di visualizzazione per l'applicazione, ad esempio **storage-browser-oauth**.
9. Inserisci una Description (Descrizione). La descrizione dell'applicazione viene visualizzata nella console di IAM Identity Center e nelle richieste API, ma non nel portale di AWS accesso.
10. In Metodo di assegnazione degli utenti e dei gruppi, scegli Non richiedere assegnazioni. Questa opzione consente a tutti gli utenti e gruppi autorizzati del Centro identità IAM di accedere a questa applicazione.
11. Nel Portale di accesso AWS , inserisci un URL dell'applicazione, dove gli utenti possono accedere all'applicazione.
12. (Facoltativo) Se desideri aggiungere un tag di risorsa, inserire la coppia chiave e valore. Per aggiungere più tag di risorse, scegli Aggiungi nuovo tag per generare una nuova voce e inserire le coppie di chiavi e valori.
13. Scegli Avanti. Viene visualizzata la pagina Specifica autenticazione.
14. In Autenticazione con emittente di token attendibili, utilizza la casella di controllo per selezionare l'emittente di token attendibili che hai creato in precedenza.

15. In Configura emittenti di token attendibili selezionati, inserisci [aud claim](#). claim aud identifica i destinatari del JSON Web Token (JWT) ed è il nome con cui l'emittente di token attendibile identifica questa applicazione.

 Note

Potrebbe essere necessario contattare l'amministratore del gestore dell'identità digitale esterno per ottenere queste informazioni.

16. Scegli Avanti. Viene visualizzata la pagina Specifica credenziali di autenticazione.
17. In Metodo di configurazione, scegli Inserisci uno o più ruoli IAM.
18. In Inserisci ruoli IAM, aggiungi il [ruolo IAM](#) o il nome della risorsa Amazon (ARN) per il token portatore di identità. È necessario inserire il ruolo IAM creato nel passaggio precedente per l'applicazione del gestore di identità (ad esempio, **bootstrap-role**).
19. Scegli Avanti.
20. Nella pagina Revisione e configurazione, rivedi i dettagli della configurazione dell'applicazione. Se è necessario modificare una qualsiasi impostazione, scegli Modifica per la sezione che si desidera modificare e apporta le modifiche.
21. Seleziona Invia. Viene visualizzata la pagina dei dettagli dell'applicazione appena aggiunta.

Dopo aver configurato le applicazioni, gli utenti possono accedere alle applicazioni dall'interno del loro portale di AWS accesso in base ai set di [autorizzazioni che hai creato](#) e all'accesso [utente che hai assegnato](#).

Aggiunta di S3 Access Grants come applicazione attendibile per la propagazione dell'identità

Dopo aver configurato l'applicazione gestita dal cliente, è necessario specificare S3 Access Grants per la propagazione delle identità. S3 Access Grant fornisce agli utenti le credenziali per accedere ai dati di Amazon S3. Quando si accede all'applicazione gestita dal cliente, S3 Access Grants trasmette l'identità dell'utente all'applicazione attendibile.

Prerequisito: assicurati di aver configurato S3 Access Grants (ad esempio [creando un'istanza S3 Access Grants](#) e [registrando una posizione](#)) prima di seguire questi passaggi. Per ulteriori informazioni, consulta [Introduzione a S3 Access Grants](#).

Per aggiungere S3 Access Grants per la propagazione dell'identità all'applicazione gestita dal cliente, esegui le seguenti operazioni:

1. Apri la [console Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestione clienti.
4. Nell'elenco Applicazioni gestite dal cliente, seleziona l'applicazione OAuth 2.0 per la quale desideri avviare le richieste di accesso. Questa è l'applicazione a cui gli utenti accederanno.
5. Nella pagina Dettagli, in Applicazioni attendibili per la propagazione dell'identità, scegli Specifica applicazioni attendibili.
6. In Tipo di impostazione, seleziona Applicazioni individuali e specifica l'accesso, quindi scegli Avanti.
7. Nella pagina Seleziona servizio, scegli S3 Access Grants. S3 Access Grants dispone di applicazioni che possono essere utilizzate per definire la propria applicazione web per la propagazione di identità affidabili.
8. Scegli Avanti. La selezione delle applicazioni avverrà nella fase successiva.
9. Nella pagina Seleziona applicazioni, scegli Applicazioni individuali, seleziona la casella di controllo per ogni applicazione che può ricevere richieste di accesso e scegli Avanti.
10. Nella pagina Configura accesso, alla voce Metodo di configurazione, scegli una delle seguenti opzioni:
 - Seleziona accesso per applicazione - Seleziona questa opzione per configurare livelli di accesso diversi per ciascuna applicazione. Scegli l'applicazione per la quale desideri configurare il livello di accesso, quindi scegli Modifica accesso. In Livello di accesso da applicare, modifica i livelli di accesso secondo necessità, quindi scegli Salva modifiche.
 - Applica lo stesso livello di accesso a tutte le applicazioni - Seleziona questa opzione se non è necessario configurare i livelli di accesso per ogni applicazione.
11. Scegli Avanti.
12. Nella pagina Rivedi configurazione, rivedi le scelte effettuate.

 Note

È necessario assicurarsi che le autorizzazioni `s3:access_grants:read_write` siano concesse agli utenti. Questa autorizzazione consente agli utenti di recuperare le credenziali di accesso ad Amazon S3. Assicurati di utilizzare la policy IAM creata in precedenza o S3 Access Grants per limitare l'accesso alle operazioni di scrittura.

13. Per apportare modifiche, scegli Modifica per la sezione di configurazione da modificare. Quindi, apporta le modifiche richieste e scegli Salva modifiche.
14. Scegli Applicazioni attendibili per aggiungere l'applicazione attendibile per la propagazione dell'identità.

Creazione di una concessione a un utente o un gruppo

In questa fase, si utilizza il Centro identità IAM per effettuare il provisioning degli utenti. È possibile utilizzare SCIM per il [provisioning automatico o manuale di utenti e gruppi](#). SCIM mantiene le identità del Centro identità IAM sincronizzate con quelle del gestore dell'identità digitale. Ciò include il provisioning, gli aggiornamenti e il deprovisioning degli utenti tra il gestore dell'identità digitale e il Centro identità IAM.

Note

Questo passaggio è necessario perché, quando S3 Access Grants viene utilizzato con il Centro identità IAM, gli utenti locali del Centro identità IAM non vengono utilizzati. Gli utenti devono invece essere sincronizzati dal gestore dell'identità digitale con il Centro identità IAM.

Per sincronizzare gli utenti del gestore dell'identità digitale con il Centro identità IAM, esegui le seguenti operazioni:

1. [Attiva il provisioning automatico](#).
2. [Genera un token di accesso](#).

Per esempi su come impostare il gestore dell'identità digitale con il Centro identità IAM per il caso d'uso specifico, consulta i [tutorial sulle origini per il Centro identità IAM](#).

Creazione del componente Storage Browser per S3

Dopo aver configurato l'istanza Centro identità IAM e creato concessioni in S3 Access Grants, apri l'applicazione React. Nell'applicazione React, utilizza `createManagedAuthAdapter` per impostare le regole di autorizzazione. È necessario specificare un fornitore di credenziali per restituire le credenziali acquisite dal Centro identità IAM. È quindi possibile chiamare `createStorageBrowser` per inizializzare il componente Storage Browser per S3:

```
import {
```

```
    createManagedAuthAdapter,  
    createStorageBrowser,  
  } from '@aws-amplify/ui-react-storage/browser';  
import '@aws-amplify/ui-react-storage/styles.css';  
  
export const { StorageBrowser } = createStorageBrowser({  
  config: createManagedAuthAdapter({  
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {  
      // return your credentials object  
      return {  
        credentials: {  
          accessKeyId: 'my-access-key-id',  
          secretAccessKey: 'my-secret-access-key',  
          sessionToken: 'my-session-token',  
          expiration: new Date(),  
        },  
      },  
    },  
  },  
  // AWS `region` and `accountId` of the S3 Access Grants Instance.  
  region: '',  
  accountId: '',  
  // call `onAuthStateChange` when end user auth state changes  
  // to clear sensitive data from the `StorageBrowser` state  
  registerAuthListener: (onAuthStateChange) => {},  
});
```

Quindi, crea un meccanismo per scambiare i JSON Web Token (JWT) dell'applicazione web con le credenziali IAM del Centro identità IAM. Per ulteriori informazioni su come scambiare JWT, consulta le seguenti risorse:

- Post [How to develop a user-facing data application with IAM Identity Center and S3 Access Grants](#) in AWS Storage Blog
- Post [Ridimensionamento dell'accesso ai dati con S3 Access Grants](#) in AWS Storage Blog
- [Workshop S3 Access Grants](#) su AWS workshop studio
- [Workshop S3 Access Grants su](#) GitHub

Quindi, imposta un endpoint API per gestire le richieste di recupero delle credenziali. Per convalidare lo scambio di JSON Web Token (JWT), esegui le seguenti operazioni:

1. Recupera il JSON Web Token dall'intestazione di autorizzazione per le richieste in entrata.
2. Convalida il token utilizzando le chiavi pubbliche dall'URL JWKS (JSON Web Key Set) specificato.
3. Verifica la scadenza, l'emittente, l'oggetto e le istruzioni dei destinatari pubblico del token.

Per scambiare il token web JSON del provider di identità con le credenziali AWS IAM, procedi nel seguente modo:

 Tip

Assicurati di evitare di registrare qualsiasi informazione sensibile. Si consiglia di utilizzare controlli di gestione degli errori per le autorizzazioni mancanti, i token scaduti e altre eccezioni. Per ulteriori informazioni, consulta il [post](#) Implementazione dei modelli AWS Lambda di gestione degli errori in AWS Compute Blog.

1. Verifica che i parametri Autorizzazione e Ambito siano forniti nella richiesta.
2. Utilizza l'API [CreateTokenWithIAM](#) per scambiare il JSON Web Token con un token del Centro identità IAM.

 Note

Il JSON Web Token del gestore dell'identità digitale non può essere utilizzato più volte. È necessario utilizzare un nuovo token per lo scambio con il Centro identità IAM.

3. Usa l'operazione [AssumeRole](#) API per assumere un ruolo temporaneo utilizzando il token IAM Identity Center. Assicurati di utilizzare il ruolo di portatore di identità, noto anche come ruolo che trasporta il contesto di identità (ad esempio, **identity-bearer-role**) per richiedere le credenziali.
4. Restituisci le credenziali IAM all'applicazione web.

 Note

Assicurati di aver impostato un meccanismo di registrazione adeguato. Le risposte vengono restituite in un formato JSON standardizzato con un codice di stato HTTP appropriato.

Configurazione di Storage Browser per S3

Per consentire a Storage Browser per S3 di accedere ai bucket S3, il componente Storage Browser effettua le chiamate REST API ad Amazon S3. Per impostazione predefinita, la [condivisione incrociata delle risorse \(CORS\)](#) non è abilitata sui bucket S3. Di conseguenza, è necessario abilitare CORS per ogni bucket S3 da cui Storage Browser accede ai dati.

Ad esempio, per abilitare CORS sul bucket S3, si può aggiornare la policy CORS in questo modo:

```
[
  {
    "ID": "S3CORSRuleId1",
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "HEAD",
      "PUT",
      "POST",
      "DELETE"
    ],
    "AllowedOrigins": [
      "*"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-type",
      "content-length",
      "etag",
      "x-amz-version-id",
      "x-amz-request-id",
      "x-amz-id-2",
      "x-amz-cf-id",
      "x-amz-storage-class",
      "date",
      "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

Risoluzione dei problemi di Storage Browser per S3

Se riscontri problemi con Storage Browser per S3, verifica i seguenti suggerimenti per la risoluzione dei problemi:

- Evita di provare a usare lo stesso token (`idToken` o `accessToken`) per più richieste. I token non possono essere riutilizzati. Ciò potrebbe determinare un errore di richiesta.
- Assicurati che le credenziali IAM fornite al componente Storage Browser includano le autorizzazioni per invocare l'operazione `s3:GetDataAccess`. In caso contrario, gli utenti finali non potranno accedere ai dati.

In alternativa, è possibile consultare le seguenti risorse:

- Storage Browser per S3 è supportato dal supporto. AWS Se hai bisogno di assistenza, contatta il [Centro di assistenza AWS](#).
- Se hai problemi con Storage Browser per S3 o desideri inviare un feedback, visita la pagina [GitHub Amplify](#).
- Se si scopre un potenziale problema di sicurezza in questo progetto, è possibile segnalarlo a AWS Security attraverso la pagina di [Segnalazione delle vulnerabilità di AWS](#).

Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration

Accelerazione del trasferimento Amazon S3 è una funzionalità a livello di bucket che permette il trasferimento rapido, semplice e sicuro di file su lunga distanza tra un client e un bucket per uso generico S3. Accelerazione del trasferimento è progettato per ottimizzare la velocità di trasferimento da tutto il mondo verso i bucket per uso generico S3. Transfer Acceleration sfrutta le edge location distribuite a livello globale in Amazon. CloudFront Quando arrivano in una edge location, i dati vengono instradati ad Amazon S3 su un percorso di rete ottimizzato.

Quando si utilizza Transfer Acceleration, potrebbero essere applicati costi aggiuntivi per il trasferimento dei dati. Per ulteriori informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Perché utilizzare Transfer Acceleration?

L'utilizzo di Accelerazione del trasferimento in un bucket per uso generico è consigliabile in diversi casi:

- Clienti che effettuano il caricamento in un bucket per uso generico centralizzato da ogni parte del mondo.
- Trasferimento regolare da qualche gigabyte a diversi terabyte di dati tra vari continenti.
- Durante il caricamento su Amazon S3 non è possibile utilizzare tutta la larghezza di banda disponibile su Internet.

Per maggiori informazioni sui casi in cui utilizzare Transfer Acceleration, consulta le [Domande frequenti su Amazon S3](#).

Requisiti per l'utilizzo di Transfer Acceleration

Di seguito sono riportati i requisiti per l'utilizzo di Transfer Acceleration in un bucket S3:

- Transfer Acceleration è supportato solo in caso di richieste in stile hosting virtuale. Per ulteriori informazioni sulle richieste di tipo virtual-hosted, consulta [Making requests using the REST API](#) nella documentazione di riferimento delle API di Amazon S3.
- Il nome del bucket utilizzato per Transfer Acceleration deve essere DNS-compliant e non deve contenere punti («.»).
- Transfer Acceleration deve essere abilitato nel bucket. Per ulteriori informazioni, consulta [Abilitazione e utilizzo di S3 Transfer Acceleration](#).

Dopo avere abilitato Transfer Acceleration in un bucket, la velocità di trasferimento dei dati verso il bucket aumenta nel giro di 20 minuti.

Note

La funzionalità Accelerazione del trasferimento attualmente non è supportata per i bucket situati nelle seguenti regioni:

- Asia Pacifico (Tokyo) (ap-northeast-1)
- Asia Pacifico (Seoul) (ap-northeast-2)
- Asia Pacifico (Mumbai) (ap-south-1)
- Asia Pacifico (Singapore) (ap-southeast-1)
- Asia Pacifico (Sydney) (ap-southeast-2)
- Canada (Centrale) (ca-central-1)
- Europa (Francoforte) (eu-central-1)

- Europa (Irlanda) (eu-west-1)
- Europa (Londra) (eu-west-2)
- Europa (Parigi) (eu-west-3)
- Sud America (San Paolo) (sa-east-1)
- Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Stati Uniti orientali (Ohio) (us-east-2)
- Stati Uniti occidentali (California settentrionale) (us-west-1)
- Stati Uniti occidentali (Oregon) (us-west-2)

- Per accedere al bucket abilitato per Transfer Acceleration, è necessario utilizzare l'endpoint `bucket-name.s3-accelerate.amazonaws.com`. In alternativa, puoi utilizzare l'endpoint dual-stack `bucket-name.s3-accelerate.dualstack.amazonaws.com` per connetterti al bucket abilitato su IPv6. Puoi continuare a utilizzare gli endpoint normali per il trasferimento di dati standard.
- Per impostare lo stato di Transfer Acceleration, è necessario essere il proprietario del bucket. Il proprietario del bucket può assegnare autorizzazioni ad altri utenti in modo che possano impostare lo stato di accelerazione nel bucket. L'autorizzazione `s3:PutAccelerateConfiguration` consente agli utenti di attivare o disattivare Transfer Acceleration in un bucket. L'autorizzazione `s3:GetAccelerateConfiguration` consente agli utenti di restituire lo stato di Transfer Acceleration di un bucket, che è `Enabled` o `Suspended`.

Le sezioni seguenti descrivono come iniziare e utilizzare Amazon S3 Transfer Acceleration per il trasferimento dei dati.

Argomenti

- [Nozioni di base su Amazon S3 Transfer Acceleration](#)
- [Abilitazione e utilizzo di S3 Transfer Acceleration](#)
- [Utilizzo dello strumento Speed Comparison di Amazon S3 Transfer Acceleration](#)

Nozioni di base su Amazon S3 Transfer Acceleration

È possibile utilizzare Amazon S3 Transfer Acceleration per il trasferimento rapido, semplice e sicuro di file su lunga distanza tra un client e un bucket S3. Transfer Acceleration utilizza le edge location

distribuite a livello globale in Amazon. CloudFront. Quando arrivano in una posizione edge, i dati vengono instradati ad Amazon S3 su un percorso di rete ottimizzato.

Per iniziare a utilizzare Amazon S3 Transfer Acceleration, eseguire le fasi descritte di seguito:

1. Attivazione di Transfer Acceleration su un bucket

È possibile abilitare Transfer Acceleration in un bucket in uno dei seguenti modi:

- Utilizzare la console di Amazon S3
- Utilizzare l'operazione REST API [PutBucketAccelerateConfiguration](#).
- Usa gli AWS SDK AWS CLI e. Per ulteriori informazioni, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Per ulteriori informazioni, consulta [Abilitazione e utilizzo di S3 Transfer Acceleration](#).

Note

Affinché il bucket funzioni con l'accelerazione di trasferimento, il nome del bucket deve essere conforme ai requisiti di denominazione DNS e non deve contenere punti (.).

2. Trasferimento dei dati da e verso il bucket abilitato per l'accelerazione

Utilizza uno dei seguenti nomi di dominio endpoint `s3-accelerate`:

- Per accedere a un bucket abilitato per l'accelerazione, utilizza `bucket-name.s3-accelerate.amazonaws.com`.
- Per accedere a un bucket abilitato per l'accelerazione su IPv6, utilizza `bucket-name.s3-accelerate.dualstack.amazonaws.com`.

Gli endpoint dual-stack Amazon S3; supportano le richieste ai bucket S3 su IPv6 e IPv4.

L'endpoint dual-stack Transfer Acceleration utilizza solo il tipo di nome di endpoint in stile hosting virtuale. Per ulteriori informazioni, consulta [Esecuzione di richieste ad Amazon S3 su IPv6](#) nella documentazione di riferimento delle API di Amazon S3 e [Utilizzo di endpoint Amazon S3 dual-stack](#) nella documentazione di riferimento delle API di Amazon S3.

Note

L'applicazione di trasferimento dei dati deve utilizzare uno dei due tipi di endpoint seguenti per accedere al bucket per il trasferimento dati rapido: `.s3-`

`accelerate.amazonaws.com` o `.s3-accelerate.dualstack.amazonaws.com` per l'endpoint dual-stack. Se desideri utilizzare il trasferimento di dati standard, puoi continuare a utilizzare gli endpoint normali.

È possibile indirizzare le richieste PUT object e GET object di Amazon S3 sul nome di dominio endpoint `s3-accelerate` dopo avere abilitato Accelerazione del trasferimento. Ad esempio, supponi di disporre di un'applicazione REST API che utilizza [PutObject](#) con il nome host `amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com` nella richiesta PUT. Per accelerare PUT, si modifica il nome host nella richiesta in `amzn-s3-demo-bucket.s3-accelerate.amazonaws.com`. Per tornare a utilizzare la velocità di caricamento standard, modifica nuovamente il nome in `amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com`.

Una volta abilitato Transfer Acceleration, sarà possibile riscontrare miglioramenti delle prestazioni nel giro di 20 minuti. Tuttavia, l'endpoint di accelerazione sarà disponibile non appena viene abilitato Transfer Acceleration.

Puoi utilizzare l'endpoint accelerate negli AWS SDK e in altri strumenti che trasferiscono dati da e verso Amazon S3. AWS CLI Se utilizzi gli AWS SDK, alcune delle lingue supportate utilizzano un flag di configurazione del client Accelerate Endpoint, quindi non è necessario impostare esplicitamente l'endpoint per Transfer Acceleration su `bucket-name.s3-accelerate.amazonaws.com`. Per gli esempi su come utilizzare un flag di configurazione del client per l'endpoint di accelerazione, consulta [Abilitazione e utilizzo di S3 Transfer Acceleration](#).

Puoi utilizzare tutte le operazioni di Amazon S3 negli endpoint di accelerazione del trasferimento, ad eccezione di quanto segue:

- [ListBuckets](#)
- [CreateBucket](#)
- [DeleteBucket](#)

Inoltre, Accelerazione del trasferimento Amazon S3 non supporta le copie multi-Regione mediante l'utilizzo di [CopyObject](#).

Abilitazione e utilizzo di S3 Transfer Acceleration

È possibile utilizzare Accelerazione del trasferimento Amazon S3 per trasferire file in modo rapido e sicuro su lunghe distanze tra il client e un bucket per uso generico S3. Puoi abilitare Transfer Acceleration utilizzando la console S3, AWS Command Line Interface (AWS CLI), l'API o gli SDK. AWS

In questa sezione vengono forniti alcuni esempi di come abilitare Amazon S3 Transfer Acceleration in un bucket e utilizzare l'endpoint di accelerazione per il bucket abilitato.

Per ulteriori informazioni sui requisiti di Transfer Acceleration, consulta [Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#).

Utilizzo della console S3

Note

Se desideri confrontare le velocità di caricamento accelerate e non accelerate, apri lo [strumento Speed Comparison di Amazon S3 Transfer Acceleration](#).

Lo strumento Speed Comparison utilizza il caricamento in più parti per trasferire un file dal tuo browser a diversi browser Regioni AWS con e senza l'accelerazione di trasferimento di Amazon S3. Puoi confrontare la velocità di caricamento per i caricamenti diretti e trasferire i caricamenti accelerati per Regione.

Come abilitare Accelerazione del trasferimento per un bucket per uso generico S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco Bucket per uso generico, scegli il nome del bucket per il quale desideri abilitare Accelerazione del trasferimento.
4. Scegli Properties (Proprietà).
5. In Transfer acceleration (Accelerazione trasferimento), scegliere Edit (Modifica).
6. Scegliere Enable (Abilita) e quindi Save changes (Salva modifiche).

Per accedere a trasferimenti di dati accelerati

1. Dopo che Amazon S3 ha attivato Transfer Acceleration per il bucket, consulta la scheda Proprietà del bucket.
2. In Transfer acceleration, Endpoint accelerated (Accelerated endpoint) visualizza l'endpoint Transfer acceleration per il bucket. Utilizza questo endpoint per accedere ai trasferimenti accelerati di dati da e verso il bucket.

Sospendendo Transfer Acceleration, l'endpoint dell'accelerazione non funziona più.

Utilizzo di AWS CLI

Di seguito sono riportati alcuni esempi di AWS CLI comandi utilizzati per Transfer Acceleration. Per istruzioni sulla configurazione di AWS CLI, consulta [Developing with Amazon S3 using the AWS CLI](#) in the Amazon S3 API Reference.

Attivazione di Transfer Acceleration su un bucket

Usa il AWS CLI [put-bucket-accelerate-configuration](#) comando per abilitare o sospendere l'accelerazione di trasferimento su un bucket.

L'esempio seguente imposta Status=Enabled per abilitare Accelerazione del trasferimento in un bucket denominato *amzn-s3-demo-bucket*. Utilizza Status=Suspended per sospendere Accelerazione del trasferimento.

Example

```
$ aws s3api put-bucket-accelerate-configuration --bucket amzn-s3-demo-bucket --  
accelerate-configuration Status=Enabled
```

Utilizzo di Transfer Acceleration

Puoi indirizzare tutte le richieste s3 e i s3api AWS CLI comandi di Amazon S3 effettuati da Amazon S3 all'endpoint di accelerazione: *s3-accelerate.amazonaws.com*. Per fare ciò, imposta il valore di configurazione su *use_accelerate_endpoint true* in un profilo nel tuo AWS Config file. Per utilizzare l'endpoint di accelerazione, è necessario che Transfer Acceleration sia abilitato nel bucket.

Tutte le richieste vengono inviate tramite il modello di indirizzamento virtuale del bucket: *amzn-s3-demo-bucket.s3-accelerate.amazonaws.com*. Qualsiasi richiesta *ListBuckets*,

CreateBucket e DeleteBucket non verrà inviata all'endpoint di accelerazione in quanto tale endpoint non supporta queste operazioni.

Per ulteriori informazioni su use_accelerate_endpoint, consulta [Configurazione di AWS CLI S3](#) in Guida di riferimento dei comandi AWS CLI .

Nell'esempio che segue, use_accelerate_endpoint viene impostato su true nel profilo di default.

Example

```
$ aws configure set default.s3.use_accelerate_endpoint true
```

Se desideri utilizzare l'endpoint accelerate per alcuni AWS CLI comandi ma non per altri, puoi utilizzare uno dei due metodi seguenti:

- È possibile utilizzare l'endpoint di accelerazione per qualsiasi comando s3 o s3api impostando il parametro --endpoint-url su <https://s3-accelerate.amazonaws.com>.
- Configura profili separati nel tuo AWS Config file. Ad esempio, si può creare un profilo che imposta use_accelerate_endpoint su true e un profilo che non imposta use_accelerate_endpoint. Quando si esegue un comando, specifica il profilo da usare, a seconda dell'intenzione di utilizzare o meno l'endpoint di accelerazione.

Caricamento di un oggetto in un bucket abilitato per Transfer Acceleration

L'esempio seguente carica un file in un bucket denominato *amzn-s3-demo-bucket* che è stato abilitato per Accelerazione del trasferimento mediante il profilo predefinito configurato per l'utilizzo dell'endpoint di accelerazione.

Example

```
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region
```

Nell'esempio che segue viene caricato un file in un bucket abilitato per Transfer Acceleration mediante il parametro --endpoint-url per specificare l'endpoint di accelerazione.

Example

```
$ aws configure set s3.addressing_style virtual
```

```
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region --endpoint-url https://s3-accelerate.amazonaws.com
```

Utilizzo di AWS SDK

Di seguito sono riportati alcuni esempi di utilizzo di Transfer Acceleration per caricare oggetti su Amazon S3 utilizzando l' AWS SDK. Alcuni dei linguaggi supportati dall' AWS SDK (ad esempio, Java e .NET) utilizzano un flag di configurazione del client Accelerate Endpoint, quindi non è necessario impostare esplicitamente l'endpoint per Transfer Acceleration su. *bucket-name*.s3-accelerate.amazonaws.com

Java

Per utilizzare un endpoint di accelerazione per caricare un oggetto su Amazon S3 con l'SDK per Java, puoi: AWS

- Creare un S3Client configurato per utilizzare endpoint di accelerazione. Tutti i bucket cui accede il client devono avere Transfer Acceleration abilitato.
- Abilitare Accelerazione del trasferimento in un bucket specificato. Questa fase è necessaria solo se sul bucket specificato non è ancora abilitato Transfer Acceleration.
- Verificare se Accelerazione del trasferimento è abilitato per il bucket specificato.
- Caricare un nuovo oggetto nel bucket specificato utilizzando l'endpoint di accelerazione del bucket.

Per ulteriori informazioni sull'uso di Transfer Acceleration, consulta [Nozioni di base su Amazon S3 Transfer Acceleration](#).

Il seguente esempio di codice mostra come configurare Transfer Acceleration con l' AWS SDK per Java.

```
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.BucketAccelerateStatus;
import
    software.amazon.awssdk.services.s3.model.GetBucketAccelerateConfigurationRequest;
import
    software.amazon.awssdk.services.s3.model.PutBucketAccelerateConfigurationRequest;
import software.amazon.awssdk.services.s3.model.PutObjectRequest;
```

```
import software.amazon.awssdk.services.s3.model.AccelerateConfiguration;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.core.exception.SdkClientException;

public class TransferAcceleration {
    public static void main(String[] args) {
        Region clientRegion = Region.US_EAST_1;
        String bucketName = "**** Provide bucket name ****";
        String keyName = "**** Provide key name ****";

        try {
            // Create an Amazon S3 client that is configured to use the accelerate
            endpoint.
            S3Client s3Client = S3Client.builder()
                .region(clientRegion)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .accelerate(true)
                .build();

            // Enable Transfer Acceleration for the specified bucket.
            s3Client.putBucketAccelerateConfiguration(
                PutBucketAccelerateConfigurationRequest.builder()
                    .bucket(bucketName)

                .accelerateConfiguration(AccelerateConfiguration.builder()
                    .status(BucketAccelerateStatus.ENABLED)
                    .build())
                .build());

            // Verify that transfer acceleration is enabled for the bucket.
            String accelerateStatus = s3Client.getBucketAccelerateConfiguration(
                GetBucketAccelerateConfigurationRequest.builder()
                    .bucket(bucketName)
                    .build()
                .status().toString());
            System.out.println("Bucket accelerate status: " + accelerateStatus);

            // Upload a new object using the accelerate endpoint.
            s3Client.putObject(PutObjectRequest.builder()
                .bucket(bucketName)
                .key(keyName)
                .build(),
                RequestBody.fromString("Test object for transfer
                acceleration"));
```

```

        System.out.println("Object \"" + keyName + "\" uploaded with transfer
acceleration.");
    } catch (S3Exception e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
}
}

```

.NET

L'esempio seguente mostra come utilizzare per abilitare Transfer Acceleration su un bucket. AWS SDK per .NET Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Nozioni di base su AWS SDK per .NET](#) nella Guida per gli sviluppatori di AWS SDK per .NET .

Example

```

using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TransferAccelerationTest
    {
        private const string bucketName = "**** bucket name ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
        RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            EnableAccelerationAsync().Wait();
        }
    }
}

```

```

static async Task EnableAccelerationAsync()
{
    try
    {
        var putRequest = new PutBucketAccelerateConfigurationRequest
        {
            BucketName = bucketName,
            AccelerateConfiguration = new AccelerateConfiguration
            {
                Status = BucketAccelerateStatus.Enabled
            }
        };
        await
s3Client.PutBucketAccelerateConfigurationAsync(putRequest);

        var getRequest = new GetBucketAccelerateConfigurationRequest
        {
            BucketName = bucketName
        };
        var response = await
s3Client.GetBucketAccelerateConfigurationAsync(getRequest);

        Console.WriteLine("Acceleration state = '{0}' ",
response.Status);
    }
    catch (AmazonS3Exception amazonS3Exception)
    {
        Console.WriteLine(
            "Error occurred. Message:'{0}' when setting transfer
acceleration",
            amazonS3Exception.Message);
    }
}
}
}

```

Durante il caricamento di un oggetto in un bucket con Transfer Acceleration abilitato, specifica l'utilizzo dell'endpoint di accelerazione durante la creazione di un client.

```

var client = new AmazonS3Client(new AmazonS3Config
{
    RegionEndpoint = TestRegionEndpoint,

```



```
        UseAccelerateEndpoint = true
    }
```

JavaScript

Per un esempio di attivazione dell'accelerazione del trasferimento utilizzando il [PutBucketAccelerateConfiguration comando AWS SDK per JavaScript](#), vedi nell'API Reference. AWS SDK per JavaScript

Python (Boto)

Per un esempio di abilitazione di Accelerazione del trasferimento utilizzando SDK per Python, consulta [put_bucket_accelerate_configuration](#) nella Guida di riferimento delle API AWS SDK per Python (Boto3).

Other

Per informazioni sull'utilizzo di altri AWS SDK, consulta Codice e [librerie di esempio](#).

Utilizzo della REST API

Utilizza l'operazione REST API PutBucketAccelerateConfiguration per abilitare la configurazione accelerata su un bucket esistente.

Per ulteriori informazioni, consulta [PutBucketAccelerateConfiguration](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo dello strumento Speed Comparison di Amazon S3 Transfer Acceleration

Puoi utilizzare lo [strumento Speed Comparison di Amazon S3 Transfer Acceleration](#) per confrontare le velocità di caricamento accelerate e non accelerate tra regioni Amazon S3. Lo strumento Speed Comparison usa carichi in più parti per trasferire un file dal browser a diverse regioni Amazon S3 con o senza l'utilizzo di Transfer Acceleration.

È possibile accedere allo Strumento di confronto delle velocità utilizzando uno dei metodi riportati di seguito:

- Copia il seguente URL nella finestra del browser, sostituendolo *region* con Regione AWS quello che stai utilizzando (ad esempio *us-west-2*) e *amzn-s3-demo-bucket* con il nome del bucket che desideri valutare:

`https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html?region=region&origBucketName=amzn-s3-demo-bucket`

Per un elenco delle regioni supportate da Amazon S3, consultare la sezione relativa a [endpoint e quote di Amazon S3](#) nella Riferimenti generali di AWS.

- Utilizzare la console di Amazon S3

Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati

In generale, i proprietari dei bucket pagano tutti i costi di storage e trasferimento dei dati Amazon S3 associati al loro bucket. Tuttavia, è possibile configurare un bucket per uso generico come bucket con pagamento a carico del richiedente. Nel caso di bucket con Pagamento a carico del richiedente, il costo della richiesta e del download dei dati dal bucket viene pagato dal richiedente anziché dal proprietario del bucket. Il proprietario del bucket paga sempre il costo di archiviazione dei dati.

Generalmente, si configurano bucket Requester Pays quando si desidera condividere dati senza incorrere nei costi associati all'accesso ai dati da parte di altre persone. Ad esempio, puoi utilizzare bucket con pagamento a carico del richiedente se desideri rendere disponibili grandi set di dati, come directory di codici postali, dati di riferimento, informazioni geospaziali o dati di Web crawling.

Important

Se si abilita il Pagamento a carico del richiedente su un bucket per uso generico, l'accesso anonimo al bucket non è consentito.

È necessario autenticare tutte le richieste che riguardano i bucket con Pagamento a carico del richiedente. L'autenticazione delle richieste consente ad Amazon S3 di identificare il richiedente e addebitargli l'utilizzo del bucket con Pagamento a carico del richiedente.

Quando il richiedente assume un ruolo AWS Identity and Access Management (IAM) prima di effettuare la richiesta, l'account a cui appartiene il ruolo viene addebitato per la richiesta. Per ulteriori informazioni sui ruoli IAM, consultare [Ruoli IAM](#) nella Guida per l'utente di IAM.

Dopo aver configurato un bucket come bucket con pagamento a carico del richiedente, questi deve dimostrare di aver compreso che verrà addebitato il costo della richiesta e del download dei dati. Per dimostrare di accettare gli addebiti, i richiedenti devono includere `x-amz-request-payer` come intestazione nella loro richiesta API per le richieste DELETE, GET, HEAD, POST e PUT, oppure aggiungere il parametro `RequestPayer` nella loro richiesta REST. Per le richieste CLI, i richiedenti possono utilizzare il parametro `--request-payer`.

Example- Utilizzo di pagamenti a carico del richiedente per l'eliminazione di un oggetto

Per utilizzare la seguente [API DeleteObjectVersion](#) di esempio, sostituire *user input placeholders* con le proprie informazioni.

```
DELETE /Key+?versionId=VersionId HTTP/1.1
Host: Bucket.s3.amazonaws.com
x-amz-mfa: MFA
x-amz-request-payer: RequestPayer
x-amz-bypass-governance-retention: BypassGovernanceRetention
x-amz-expected-bucket-owner: ExpectedBucketOwner
```

Se il richiedente ripristina gli oggetti utilizzando l'API [RestoreObject](#), il pagamento a carico del richiedente è supportato finché l'intestazione `x-amz-request-payer` o il parametro `RequestPayer` sono presenti nella richiesta; tuttavia, il richiedente paga solo il costo della richiesta. Il proprietario del bucket paga le spese di recupero.

I bucket con pagamento a carico del richiedente non supportano quanto riportato di seguito.

- Richieste anonime
- Richieste SOAP
- L'uso di un bucket con pagamento a carico del richiedente come bucket di destinazione per la registrazione degli utenti finali o viceversa. Tuttavia, è possibile attivare la registrazione degli utenti finale su un bucket con pagamento a carico del richiedente in cui il bucket di destinazione non è un bucket di questo genere.

Come funzionano i pagamenti a carico del richiedente

L'addebito delle richieste di pagamento a carico del richiedente che hanno esito positivo è diretto: il richiedente paga il trasferimento dei dati e la richiesta; il proprietario del bucket paga lo storage dei dati. Tuttavia, il proprietario del bucket riceve l'addebito della richiesta nei casi seguenti:

- La richiesta restituisce un errore AccessDenied (HTTP403 Forbidden) e la richiesta viene avviata all'interno dell'account o dell'organizzazione individuale AWS del proprietario del bucket. AWS
- La richiesta è una richiesta SOAP.

Per ulteriori informazioni sui pagamenti a carico del richiedente, consulta gli argomenti riportati di seguito.

Argomenti

- [Configurazione di pagamenti a carico del richiedente su un bucket](#)
- [Recupero della configurazione requestPayment tramite REST API](#)
- [Download di oggetti dai bucket con pagamento a carico del richiedente](#)

Configurazione di pagamenti a carico del richiedente su un bucket

Puoi configurare un bucket Amazon S3 in modo che sia un bucket con pagamento a carico del richiedente in modo che il richiedente paghi il costo della richiesta e il download dei dati al posto del proprietario del bucket.

In questa sezione sono riportati esempi di come configurare i pagamenti a carico del richiedente per un bucket Amazon S3 utilizzando la console e REST API.

Utilizzo della console S3

Come abilitare il Pagamento a carico del richiedente per un bucket per uso generico S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco Bucket per uso generico scegli il nome del bucket per il quale desideri abilitare il Pagamento a carico del richiedente.
4. Scegliere Properties (Proprietà).
5. In Requester pays (Pagamento a carico del richiedente), scegliere Edit (Modifica).
6. Scegliere Enable (Abilita) e quindi Save changes (Salva modifiche).

Amazon S3 abilita il Pagamento a carico del richiedente per il bucket e visualizza la panoramica del bucket. In Pagamento a carico del richiedente si può notare che è Abilitato.

Utilizzo dell'API REST

Solo il proprietario del bucket può impostare il valore di configurazione

`RequestPaymentConfiguration.payer` di un bucket su `BucketOwner`, impostazione predefinita, o su `Requester`. La configurazione della risorsa `requestPayment` è facoltativa. Per impostazione predefinita, il bucket non è un bucket con Pagamento a carico del richiedente.

Per riportare il bucket con Pagamento a carico del richiedente a un bucket normale, si utilizza il valore `BucketOwner`. Generalmente, si utilizza `BucketOwner` quando si caricano dati nel bucket Amazon S3 e successivamente si imposta il valore su `Requester` prima di pubblicare gli oggetti nel bucket.

Per configurare `requestPayment`

- Utilizzare una richiesta PUT per impostare il valore `Payer` su `Requester` in un bucket specificato.

```
PUT ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
Content-Length: 173
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]

<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

Se la richiesta ha esito positivo, Amazon S3 restituisce una risposta simile a quella riportata di seguito.

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Length: 0
Connection: close
Server: AmazonS3
x-amz-request-charged:requester
```

Puoi impostare il pagamento a carico del richiedente solo a livello di bucket. Non è possibile impostare il pagamento a carico del richiedente per oggetti specifici all'interno del bucket.

È possibile configurare un bucket come `BucketOwner` o `Requester` in qualsiasi momento. Tuttavia, potrebbero essere necessari alcuni minuti prima che il nuovo valore di configurazione abbia effetto.

Note

I proprietari dei bucket che utilizzano URL prefirmati dovrebbero riflettere bene prima di configurare un bucket come bucket con pagamento a carico del richiedente, soprattutto se l'URL ha una durata di vita molto lunga. Il proprietario del bucket riceve l'addebito ogni volta che il richiedente utilizza un URL prefirmato associato alle credenziali del proprietario del bucket.

Recupero della configurazione `requestPayment` tramite REST API

È possibile determinare il valore `Payer` impostato in un bucket richiedendo la risorsa `requestPayment`.

Per ottenere la risorsa `requestPayment`

- Utilizzare una richiesta GET per ottenere la risorsa `requestPayment`, come mostrato nella richiesta seguente.

```
GET ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

Se la richiesta ha esito positivo, Amazon S3 restituisce una risposta simile a quella riportata di seguito.

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Type: [type]
Content-Length: [length]
Connection: close
```

```
Server: AmazonS3
```

```
<?xml version="1.0" encoding="UTF-8"?>
<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

Questa risposta mostra che il valore `payer` è impostato su `Requester`.

Download di oggetti dai bucket con pagamento a carico del richiedente

Poiché i richiedenti ricevono l'addebito del download dei dati dai bucket con pagamento a carico del richiedente, le richieste devono contenere un parametro speciale, `x-amz-request-payer`, che conferma che il richiedente sa che riceverà l'addebito del download. Per accedere agli oggetti nei bucket con Pagamento a carico del richiedente, le richieste devono includere uno degli elementi seguenti.

- Per le richieste DELETE, GET, HEAD, POST e PUT, includere `x-amz-request-payer : requester` nell'intestazione
- Per gli URL firmati, includere `x-amz-request-payer=requester` nella richiesta

Se la richiesta ha esito positivo e il richiedente riceve l'addebito, la risposta include l'intestazione `x-amz-request-charged:requester`. Se la richiesta non contiene `x-amz-request-payer`, Amazon S3 restituisce un errore 403 e addebita la richiesta al proprietario del bucket.

Note

I proprietari dei bucket non devono aggiungere `x-amz-request-payer` alle loro richieste. Assicurarsi di aver incluso `x-amz-request-payer` e il suo valore nel calcolo della firma. Per ulteriori informazioni, consulta [Utilizzo di un'intestazione di autorizzazione](#) nella documentazione di riferimento delle API di Amazon S3.

Utilizzo di REST API

Per scaricare oggetti da un bucket con Pagamento a carico del richiedente

- Utilizzare una richiesta GET per scaricare un oggetto da un bucket con Pagamento a carico del richiedente, come mostrato nella richiesta seguente.

```
GET / [destinationObject] HTTP/1.1
Host: [BucketName].s3.amazonaws.com
x-amz-request-payer : requester
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

Se la richiesta GET ha esito positivo e il richiedente riceve l'addebito, la risposta include `x-amz-request-charged:requester`.

Amazon S3 può restituire un errore `Access Denied` per le richieste di recupero di oggetti da un bucket con Pagamento a carico del richiedente. Per ulteriori informazioni, consulta [Risposte agli errori](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di AWS CLI

Per scaricare oggetti da un bucket `Requester Pays` utilizzando il AWS CLI, lo specifichi `--request-payer requester` come parte della richiesta. `get-object` Per ulteriori informazioni, consulta [get-object](#) nella Documentazione di riferimento della AWS CLI .

Utilizzo degli oggetti in Amazon S3

Per memorizzare i tuoi dati in Amazon S3, lavori con risorse denominate bucket e oggetti. Un bucket è un container per oggetti o file. Un oggetto è un file e tutti i metadati che descrivono tale file.

Per memorizzare un oggetto in Amazon S3, crei un bucket e quindi carichi l'oggetto in un bucket. Quando l'oggetto si trova nel bucket, è possibile aprirlo, scaricarlo e copiarlo. Quando non hai più bisogno di un oggetto o di un bucket, puoi ripulire queste risorse.

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Important

Nella console di Amazon S3, quando scegli Open (Apri) o Download As (Scarica come) per un oggetto, queste operazioni creano URL prefirmati. L'oggetto sarà accessibile a chiunque abbia accesso a questi URL prefirmati per cinque minuti. Per ulteriori informazioni sugli URL prefirmati, consulta la sezione relativa all'[utilizzo di URL prefirmati](#).

Con Amazon S3 paghi solo per le risorse utilizzate. Per ulteriori informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Amazon S3](#). Se sei un nuovo cliente Amazon S3, puoi iniziare a utilizzare Amazon S3 gratuitamente. Per ulteriori informazioni, consulta [Piano gratuito AWS](#).

Argomenti

- [Panoramica degli oggetti di Amazon S3](#)
- [Denominazione di oggetti Amazon S3](#)
- [Utilizzo dei metadati degli oggetti](#)
- [Caricamento degli oggetti](#)
- [Aggiunta di precondizioni alle operazioni S3 con richieste condizionali](#)
- [Copia, spostamento e denominazione di oggetti](#)
- [Download di oggetti](#)

- [Verifica dell'integrità degli oggetti in Amazon S3](#)
- [Eliminazione di oggetti Amazon S3](#)
- [Organizzare, elencare e utilizzare gli oggetti](#)
- [Download e caricamento di oggetti con URL predefiniti](#)
- [Trasformazione di oggetti con S3 Object Lambda](#)
- [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch](#)
- [Interrogazione dei dati in loco con Amazon S3 Select](#)

Panoramica degli oggetti di Amazon S3

Amazon S3 è un object store che utilizza valori chiave univoci per archiviare tutti gli oggetti desiderati. Archivi questi oggetti in uno o più bucket e ogni oggetto può avere una dimensione massima di 50 TB. Un oggetto è costituito dai seguenti elementi:

Chiave

Il nome assegnato a un oggetto. La chiave dell'oggetto viene utilizzata per recuperare l'oggetto. Per ulteriori informazioni, consulta [Utilizzo dei metadati degli oggetti](#).

ID versione

All'interno di un bucket, una chiave e l'ID versione identificano in modo univoco un oggetto. L'ID versione è una stringa generata da Amazon S3 quando aggiungi un oggetto a un bucket. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Valore

Il contenuto che stai archiviando.

Il valore di un oggetto può essere costituito da qualsiasi sequenza di byte. Le dimensioni degli oggetti possono variare da zero a 50 TB. Per ulteriori informazioni, consulta [Caricamento degli oggetti](#).

Note

Sebbene la documentazione di Amazon S3 faccia comunemente riferimento a un limite di dimensione degli oggetti di 50 TB, la dimensione massima effettiva degli oggetti è 53,7 TB

(48,8 TiB). Questo limite è determinato dai vincoli di caricamento in più parti: 10.000 parti massime x 5 GiB per parte = 50.000 GiB (53,7 TB)

Metadati

Un set di coppie nome-valore con le quali è possibile archiviare le informazioni relative all'oggetto. È possibile assegnare metadati, denominati metadati definiti dall'utente, agli oggetti disponibili in Amazon S3. Inoltre, Amazon S3 assegna a questi oggetti metadati di sistema che utilizza per gestire gli oggetti. Per ulteriori informazioni, consulta [Utilizzo dei metadati degli oggetti](#).

Risorse secondarie

Amazon S3 utilizza il meccanismo delle risorse secondarie per archiviare ulteriori informazioni specifiche dell'oggetto. Poiché le risorse secondarie sono subordinate agli oggetti, sono sempre associate a un'altra entità, ad esempio un oggetto o un bucket. Per ulteriori informazioni, consulta [Risorse secondarie degli oggetti](#).

Informazioni sul controllo degli accessi

È possibile controllare l'accesso agli oggetti archiviati in Amazon S3. Amazon S3 supporta sia il controllo degli accessi basato sulle risorse, ad esempio una lista di controllo degli accessi (ACL) e le policy dei bucket, oltre al controllo degli accessi basato sugli utenti. Per ulteriori informazioni sul controllo degli accessi, consulta:

- [Controllo degli accessi in Amazon S3](#)
- [Identity and Access Management per Amazon S3](#)
- [Configurazione delle ACL](#)

Le risorse di Amazon S3 (ad esempio, bucket e oggetti) sono private per default. È necessario concedere l'autorizzazione in modo esplicito affinché altri utenti possano accedere alle risorse. Per ulteriori informazioni sulla condivisione degli oggetti, consulta [Condivisione di oggetti mediante URL prefirmati](#).

Tag

È possibile utilizzare i tag per classificare gli oggetti archiviati, per il controllo degli accessi o l'allocazione dei costi. Per ulteriori informazioni, consulta [Etichettare i tuoi oggetti](#).

Risorse secondarie degli oggetti

Amazon S3 definisce un set di risorse secondarie associate ai bucket e agli oggetti. Le risorse secondarie sono subordinate agli oggetti. Ciò significa che le risorse secondarie non esistono da sole. Sono sempre associate a qualche altra entità, ad esempio un oggetto o un bucket.

Nella tabella seguente sono elencate le risorse secondarie associate agli oggetti di Amazon S3.

Risorsa secondaria	Descrizione
acl	Contiene un elenco delle assegnazioni, che identificano gli assegnatari e le autorizzazioni concesse. Quando si crea un oggetto, la risorsa secondaria <code>acl</code> identifica il proprietario dell'oggetto assegnandogli il controllo completo sull'oggetto. È possibile recuperare un'ACL dell'oggetto o sostituirla con un elenco aggiornato delle assegnazioni. Qualsiasi aggiornamento apportato a un'ACL richiede la sostituzione dell'ACL esistente. Per ulteriori informazioni sulle ACL, consulta Panoramica delle liste di controllo accessi (ACL) .

Denominazione di oggetti Amazon S3

La chiave oggetto (o nome di chiave) identifica l'oggetto in modo univoco in un bucket Amazon S3. Quando si crea un oggetto, si specifica il nome della chiave. Ad esempio, nella [console Amazon S3](#), quando si seleziona un bucket, viene visualizzato un elenco di oggetti presenti nel bucket. Questi nomi sono le chiavi degli oggetti.

Il nome della chiave dell'oggetto è costituito da una sequenza di caratteri Unicode codificati in UTF-8, con una lunghezza massima di 1.024 byte o circa 1.024 caratteri latini. In alcune lingue, un singolo carattere può richiedere 2 byte per la codifica. Quando si assegna un nome agli oggetti, occorre tenere presente quanto segue:

- I nomi delle chiavi degli oggetti fanno distinzione tra maiuscole e minuscole.
- I nomi delle chiavi dell'oggetto includono i prefissi (denominati come cartelle nella console). Ad esempio, `Development/Projects.xls` è il nome completo della chiave dell'oggetto `Projects.xls` che si trova all'interno del prefisso (o cartella) `Development`. Il prefisso, il delimitatore (`/`) e il nome dell'oggetto sono inclusi nel limite di 1.024 byte per il nome della chiave

dell'oggetto. Per ulteriori informazioni su prefissi e cartelle, consultare [the section called “Scelta dei nomi delle chiavi di oggetti”](#).

- Alcuni caratteri potrebbero richiedere una gestione speciale quando vengono utilizzati nei nomi delle chiavi degli oggetti. Per ulteriori informazioni, consulta [the section called “Linee guida per la denominazione delle chiavi degli oggetti”](#).

Note

I nomi delle chiavi dell'oggetto con il valore "soap" non sono supportati per le [richieste virtual-hosted-style](#). Per i valori dei nomi delle chiavi dell'oggetto in cui viene utilizzato "soap", è necessario utilizzare un [URL in stile percorso](#).

Scelta dei nomi delle chiavi di oggetti

Il modello di dati di Amazon S3 è una struttura flat: crei un bucket e il bucket archivia gli oggetti. Non c'è nessuna gerarchia di bucket secondari o sottocartelle. Tuttavia, è possibile applicare una gerarchia logica utilizzando delimitatori e prefissi di nomi di chiavi come avviene nella console di Amazon S3. La console di Amazon S3 supporta il concetto di cartella. Per ulteriori informazioni su come modificare i metadati dalla console di Amazon S3, consulta [Modifica dei metadati degli oggetti nella console di Amazon S3](#).

Supponiamo che il bucket (admin-created) contenga quattro oggetti con le seguenti chiavi:

Development/Projects.xls

Finance/statement1.pdf

Private/taxdocument.pdf

s3-dg.pdf

La console utilizza i prefissi dei nomi di chiavi (Development/, Finance/ e Private/) e il delimitatore (/) per visualizzare una struttura di cartelle. Poiché la chiave s3-dg.pdf non include un prefisso delimitato da barra, i relativi oggetti vengono visualizzati direttamente a livello root del bucket. Se si apre la cartella Development/, viene visualizzato l'oggetto Projects.xlsx in essa contenuto.

- Amazon S3 supporta i bucket e gli oggetti e non sono presenti gerarchie. Tuttavia, utilizzando prefissi e delimitatori nel nome della chiave di un oggetto, la console Amazon S3 e gli SDK possono dedurre la gerarchia e introdurre il AWS concetto di cartelle.
- La console di Amazon S3 implementa la creazione di oggetti cartella creando un oggetto a byte zero con il prefisso di cartella e il valore di delimitatore come chiave. Questi oggetti cartella non vengono visualizzati nella console. Altrimenti si comportano come qualsiasi altro oggetto e possono essere visualizzati e manipolati tramite l'API REST, la CLI e gli SDK. AWS AWS

Linee guida per la denominazione delle chiavi degli oggetti

È possibile utilizzare qualsiasi UTF-8 carattere nel nome della chiave di un oggetto. Tuttavia, utilizzare alcuni caratteri nei nomi delle chiavi può causare problematiche con alcuni protocolli e applicazioni. Le seguenti linee guida garantiscono la massima conformità con DNS, i caratteri sicuri per il Web, i parser XML e altre interfacce API.

Caratteri sicuri

I seguenti set di caratteri possono essere utilizzati con la massima sicurezza nei nomi delle chiavi:

Caratteri alfanumerici

- 0-9
- a-z
- A-Z

Caratteri speciali

- Punto esclamativo (!)
- Trattino (-)
- Carattere di sottolineatura (_)
- Punto (.)
- Asterisco (*)
- Virgoletta singola (')
- Parentesi aperta ((
- Parentesi chiusa ())

Di seguito sono riportati esempi di nomi di chiavi validi per gli oggetti:

- 4my-organization

- `my.great_photos-2014/jan/myvacation.jpg`
- `videos/2014/birthday/video1.wmv`

Note

Se utilizzi la console di Amazon S3 per scaricare un oggetto il cui nome della chiave termina con un punto (.), il punto viene rimosso dal nome della chiave dell'oggetto scaricato. Per conservare i punti alla fine dei nomi delle chiavi negli oggetti scaricati, devi utilizzare AWS Command Line Interface (AWS CLI), AWS SDK o l'API REST di Amazon S3.

Inoltre, tieni a mente le seguenti limitazioni sui prefissi:

- Gli oggetti con il prefisso di `./` devono essere caricati o scaricati con gli AWS SDK o AWS CLI l'API REST. Non è possibile utilizzare la console Amazon S3 per caricare questi oggetti.
- Le chiavi dell'oggetto contenenti elementi di percorso relativo (ad esempio, `../`) sono valide se, quando analizzate da sinistra a destra, il numero cumulativo dei segmenti di percorso relativo non supera il numero di elementi di percorso non relativo rilevati. Questa regola si applica a tutte le richieste effettuate utilizzando la console Amazon S3, l'API REST di Amazon S3 e gli SDK. AWS CLI AWS

Ad esempio:

- `videos/2014/../../video1.wmv` è valido.
- `videos/../../video1.wmv` non è valido.
- `videos/../../2014/video1.wmv` non è valido.

Period-only segmenti di percorso

Le chiavi dell'oggetto contenenti segmenti di percorso con solo punto (. `o ..`) possono causare un comportamento imprevisto se elaborate da applicazioni, SDK o strumenti che li interpretano come riferimenti di percorsi relativi.

I seguenti modelli possono causare problemi:

- `folder/./file.txt`: contiene il riferimento alla directory corrente
- `folder/../file.txt`: contiene il riferimento alla directory principale
- `./file.txt`: inizia con il riferimento alla directory corrente

- `../file.txt`: inizia con il riferimento alla directory principale

I seguenti modelli funzionano normalmente:

- `folder/.hidden/file.txt`: il punto fa parte del nome del file, non è standalone
- `folder/..backup/file.txt` i punti fanno parte del nome del file, non sono standalone

Quando le applicazioni elaborano le chiavi degli oggetti con segmenti con solo punto, possono verificarsi i seguenti impatti sul comportamento:

- Normalizzazione del percorso: molti sistemi risolvono i riferimenti `.` e `..` automaticamente, modificando potenzialmente il percorso effettivo (ad esempio `folder./file.txt` diventa `folder/file.txt`).
- Problemi di accesso: le applicazioni potrebbero non riuscire a individuare gli oggetti a causa delle differenze di risoluzione dei percorsi.
- Comportamento incoerente: strumenti e SDK diversi potrebbero gestire questi modelli in modo diverso.

Important

Per evitare questi problemi, è consigliabile non utilizzare segmenti di percorso con solo punto nei nomi delle chiavi dell'oggetto. È possibile utilizzare convenzioni di denominazione alternative per scopi organizzativi.

Caratteri che potrebbero richiedere una gestione speciale

I seguenti caratteri in un nome di chiave potrebbero richiedere ulteriori operazioni di gestione del codice e molto probabilmente dovranno essere codificati tramite URL o vi si dovrà fare riferimento come HEX. Alcuni di essi sono caratteri non stampabili ed è possibile che non vengano gestiti dal browser in uso; per tale motivo, richiedono una gestione speciale:

- E commerciale (`&`)
- Simbolo del dollaro (`$`)
- I caratteri ASCII sono compresi tra 00-1F hex (0-31 decimale) e 7F (127 decimale)
- Simbolo at (`@`)

- Segno uguale (=)
- Punto e virgola (,) ;
- Barra obliqua (/)
- Due punti (:) :
- Segno più (+)
- Spazio - È possibile che in alcuni casi vadano perse sequenze significative di spazi (in particolare, gli spazi multipli)
- Virgola (,)
- Punto interrogativo (?)

Caratteri da evitare

È consigliabile non utilizzare i seguenti caratteri nel nome di una chiave a causa della gestione significativa dei caratteri speciali, che non è coerente in tutte le applicazioni:

- Barra rovesciata (\)
- Parentesi graffa di sinistra ({)
- Non-printable Caratteri ASCII (128—255 caratteri decimali)
- Accento circonflesso (^)
- Parentesi graffa di destra (})
- Carattere percentuale (%)
- Accento grave o apice inverso (`)
- Parentesi quadra di destra (])
- Virgolette (")
- Segno maggiore di (>)
- Parentesi quadra di sinistra ([)
- Tilde (~)
- Segno minore di (<)
- Simbolo di numero (#)
- Barra verticale (|)

XML-related vincoli chiave dell'oggetto

Come specificato dallo [standard XML sulla gestione di fine riga](#), tutto il testo XML viene normalizzato in modo tale che i ritorni a capo singoli (codice ASCII 13) e i ritorni a capo immediatamente seguiti da un avanzamento riga (codice ASCII 10), noti anche come caratteri di nuova riga, vengano sostituiti da un singolo carattere di avanzamento riga. Per garantire l'analisi corretta delle chiavi degli oggetti nelle richieste XML, i ritorni a capo e [altri caratteri speciali devono essere sostituiti con il codice di entità XML equivalente](#) quando vengono inseriti all'interno dei tag XML.

Di seguito è riportato un elenco di tali caratteri speciali e dei loro codici di entità XML equivalenti:

- L'apostrofo (') deve essere sostituito con &apos ;
- Le virgolette (") devono essere sostituite con &quot ;
- La e commerciale (&) deve essere sostituita con &amp ;
- Il segno minore di (<) deve essere sostituito con &lt ;
- Il segno maggiore di (>) deve essere sostituito con &gt ;
- Il ritorno a capo (\r) deve essere sostituito con &#13 ; o &#x0D ;
- Il carattere di nuova riga (\n) deve essere sostituito con &#10 ; o &#x0A ;

Example

Nell'esempio seguente viene illustrato l'utilizzo di un codice di entità XML come sostituzione di un ritorno a capo. Questa richiesta DeleteObjects elimina un oggetto con il parametro key /some/prefix/objectwith\r\n (dove \r è il ritorno a capo).

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Object>
    <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
  </Object>
</Delete>
```

Ordinamento delle chiavi degli oggetti

Amazon S3 ordina le chiavi degli oggetti, inclusi i prefissi, lessicograficamente in base ai relativi valori di byte codificati. UTF-8

I caratteri ASCII vengono disposti nel seguente ordine:

- Caratteri speciali (ad esempio !, /)
- Lettere maiuscole (A–Z)
- Lettere minuscole (a–z)

Non-ASCII i caratteri (ad esempio, é,) sono codificati come UTF-8 sequenze a più byte e in genere vengono ordinati in base ai caratteri ASCII a causa dei loro valori di byte più alti (ad esempio, per é, per). 0xC3 0xE4

Ad esempio, i prefissi apple/, Apple/, éclair/, # #/ vengono ordinati come segue:

1. Apple/ (inizia con 0x41)
2. apple/ (inizia con 0x61)
3. éclair/ (inizia con 0xC3 0xA9)
4. # #/ (inizia con 0xE4 0xB8 0xAD 0xE6 0x96 0x87)

Utilizzo dei metadati degli oggetti

Amazon S3 offre diversi modi per allegare metadati ai tuoi oggetti. Le annotazioni consentono di allegare ricchi payload di dati fino a 1 MB agli oggetti utilizzando operazioni API dedicate. I tag degli oggetti sono coppie chiave-valore per la categorizzazione e il controllo dell'accesso agli oggetti. Puoi anche impostare metadati definiti dall'utente al momento del caricamento e Amazon S3 mantiene automaticamente i metadati definiti dal sistema. Per ulteriori informazioni, vedere [the section called “Metadati degli oggetti personalizzati”](#), [the section called “Annotazione di oggetti”](#), [the section called “Etichettare gli oggetti”](#), [the section called “User-defined metadati”](#) e [the section called “System-defined metadati degli oggetti”](#).

Quando si crea un oggetto, si specifica la chiave dell'oggetto (o nome della chiave), che identifica in modo univoco l'oggetto in un bucket Amazon S3. Per ulteriori informazioni, consulta [Denominazione di oggetti Amazon S3](#). È anche possibile impostare [metadati definiti dall'utente](#) in Amazon S3 al momento del caricamento dell'oggetto.

Dopo aver caricato l'oggetto, non è possibile modificare i metadati definiti dall'utente. L'unico modo per modificare questi metadati è fare una copia dell'oggetto e impostare i metadati. Per ulteriori informazioni sulla modifica dei metadati tramite la console Amazon S3, consulta [Modifica dei metadati degli oggetti nella console di Amazon S3](#).

Metadati degli oggetti personalizzati

I metadati degli oggetti personalizzati sono metadati controllati dall'utente. È possibile utilizzare i metadati degli oggetti personalizzati per archiviare informazioni sugli oggetti che sono significative per le applicazioni. Amazon S3 supporta tre tipi di metadati personalizzati degli oggetti: annotazioni, tag di oggetti e metadati definiti dall'utente.

Annotazioni

Le annotazioni sono payload di dati denominati che puoi allegare a qualsiasi oggetto Amazon S3 dopo il caricamento. Ogni annotazione può memorizzare fino a 1 MB di UTF-8 testo, ad esempio AI-generated output, risultati di classificazione o record di elaborazione. È possibile creare, recuperare, elencare ed eliminare le annotazioni senza modificare l'oggetto stesso. Per ulteriori informazioni, consulta [the section called “Annotazione di oggetti”](#).

Tag dell'oggetto

I tag degli oggetti sono coppie chiave-valore che è possibile utilizzare per classificare, organizzare e controllare l'accesso agli oggetti. Ogni oggetto può avere fino a 10 tag. Puoi utilizzare i tag nelle policy IAM e bucket, nelle regole del ciclo di vita di S3 e nei report di allocazione dei costi. Per ulteriori informazioni, consulta [the section called “Etichettare gli oggetti”](#).

User-defined metadati

Quando si carica un oggetto, è anche possibile assegnare metadata a esso. Queste informazioni facoltative vengono fornite come coppia nome-valore (chiave-valore) quando si invia una richiesta PUT o POST per creare l'oggetto. Quando si caricano gli oggetti utilizzando la REST API, i nomi facoltativi dei metadati definiti dall'utente devono iniziare con x-amz-meta- per distinguerli dalle altre intestazioni HTTP. Quando si recupera l'oggetto utilizzando REST API, questo prefisso viene restituito. Quando si caricano gli oggetti utilizzando l'API SOAP, il prefisso non è necessario. Quando si recupera l'oggetto mediante l'API SOAP, il prefisso viene rimosso, indipendentemente dall'API utilizzata per caricare l'oggetto.

Note

Le API SOAP per Amazon S3 non sono disponibili per i nuovi clienti, con la fine del ciclo di vita prevista per il 31 agosto 2025. Ti consigliamo di utilizzare l'API REST o gli AWS SDK.

Quando i metadati vengono recuperati tramite REST API, Amazon S3 riunisce le intestazioni con lo stesso nome (senza distinzione tra maiuscole e minuscole) in un elenco delimitato da virgole. I metadata contenenti caratteri non stampabili non vengono restituiti. Al contrario, viene restituita l'intestazione `x-amz-missing-meta` con il numero di voci di metadata non stampabili come valore. L'operazione `HeadObject` richiama i metadati da un oggetto senza restituire l'oggetto stesso. Questa operazione è utile se sei interessato solo ai metadati di un oggetto. Per utilizzare `HEAD` è necessario disporre dell'accesso `READ` all'oggetto. Per ulteriori informazioni, consulta [HeadObject Amazon Simple Storage Service API Reference](#).

User-defined i metadati sono un insieme di coppie chiave-valore. Amazon S3 archivia le chiavi dei metadati definiti dall'utente in caratteri minuscoli.

Amazon S3 consente caratteri Unicode arbitrari nei valori dei metadati.

Per evitare problemi legati alla presentazione di questi valori di metadati, è necessario conformarsi all'uso dei US-ASCII caratteri quando si utilizza REST e UTF-8 quando si utilizzano SOAP o caricamenti basati su browser tramite. POST

Quando si utilizzano US-ASCII caratteri non presenti nei valori dei metadati, la stringa Unicode fornita viene esaminata per individuare eventuali caratteri non presenti. US-ASCII I caratteri dei valori di tali header sono decodificati come da [RFC 2047](#) prima di memorizzarli e codificarli come da [RFC 2047](#) per renderli sicuri per la posta elettronica prima di restituirli. Se la stringa contiene solo US-ASCII caratteri, viene presentata così com'è.

Di seguito è riportato un esempio di :

```
PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: ÄMÄZÖÑ S3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: =?UTF-8?B?w4PChE3Dg8KEWsODwpXDg8KRIFMz?=

PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-ascii: AMAZONS3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
```

```
x-amz-meta-ascii: AMAZONS3
```

Note

L'intestazione della richiesta PUT è limitata a una dimensione di 8 KB. Nell'intestazione della richiesta PUT, la dimensione dei metadata definiti dall'utente è limitata a 2 KB. La dimensione dei metadata definiti dall'utente viene misurata sommando il numero di byte nella UTF-8 codifica di ogni chiave e valore.

Per informazioni sulla modifica dei metadata dell'oggetto dopo il caricamento mediante la creazione di una copia dell'oggetto, la modifica e la sostituzione dell'oggetto precedente o la creazione di una nuova versione, consulta [Modifica dei metadata degli oggetti nella console di Amazon S3](#).

Interroga i metadata e accelera la scoperta dei dati con S3 Metadata

Per trovare, memorizzare e interrogare facilmente i metadata degli oggetti S3, è possibile utilizzare S3 Metadata. Con S3 Metadata, puoi preparare rapidamente i dati da utilizzare nell'analisi aziendale, nel recupero dei contenuti, nell'intelligenza artificiale e nella formazione sui modelli di machine learning () e altro ancora. AI/ML

S3 Metadata accelera il reperimento dei dati acquisendo automaticamente i metadata per gli oggetti nei bucket per uso generico e memorizzandoli in tabelle Apache Iceberg di sola lettura e completamente gestite che possono essere interrogate. Queste tabelle di sola lettura sono chiamate tabelle di metadata. Quando gli oggetti vengono aggiunti, aggiornati e rimossi dai bucket per uso generico, S3 Metadata aggiorna automaticamente le tabelle di metadata corrispondenti per riflettere le ultime modifiche.

Per impostazione predefinita, S3 Metadata fornisce metadata sugli oggetti [definiti dal sistema, come l'ora di creazione e la classe di archiviazione di un oggetto](#), e metadata personalizzati, come tag, metadata definiti dall'utente e annotazioni. [???](#) S3 Metadata fornisce anche metadata sugli eventi, come ad esempio quando un oggetto viene aggiornato o eliminato e Account AWS che ha effettuato la richiesta.

Le tabelle di metadata sono archiviate in bucket di tabelle S3, che forniscono uno storage ottimizzato per i dati tabellari. Per interrogare i metadata, puoi integrare il tuo table bucket con servizi di analisi, come Amazon Athena, Amazon Redshift e Amazon Quick. AWS

Per ulteriori informazioni su S3 Metadata, consulta [the section called “Individuazione dei dati con le tabelle di S3 Metadata”](#).

System-defined metadati degli oggetti

Per ogni oggetto archiviato in un bucket, Amazon S3 mantiene un set di metadati di sistema. Questi metadati vengono elaborati da Amazon S3 in base alle necessità. Ad esempio, Amazon S3 conserva i metadati relativi alla data di creazione e alla dimensione degli oggetti, utilizzando queste informazioni come parte della gestione degli oggetti.

Esistono due categorie di metadata di sistema:

- Controllati dal sistema - Metadati come la data di creazione dell'oggetto sono controllati dal sistema, il che significa che solo Amazon S3 può modificare il valore della data.
- Controllati dall'utente: altri metadata di sistema, come la classe di storage configurata per l'oggetto e se la crittografia lato server è abilitata per l'oggetto, sono esempi di metadata di sistema, il cui valore viene controllato dall'utente. Se il bucket è configurato come un sito web, a volte si potrebbe voler reindirizzare una richiesta di pagina a un'altra pagina o a un URL esterno. In questo caso, la pagina Web è un oggetto nel bucket. Amazon S3 memorizza il valore di reindirizzamento della pagina come metadati di sistema, che è possibile controllare.

Quando si creano oggetti, è possibile configurare i valori di questi metadata di sistema o aggiornarli in base alle esigenze. Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

Amazon S3 utilizza AWS KMS le chiavi per crittografare i tuoi oggetti Amazon S3. AWS KMS crittografa solo i dati dell'oggetto. Il checksum e l'algoritmo specificato sono memorizzati come parte dei metadati dell'oggetto. Se la crittografia lato server viene richiesta per l'oggetto, il checksum viene archiviato in formato crittografato. Per ulteriori informazioni sulla crittografia lato server, consulta [Protezione dei dati con la crittografia](#).

Note

L'intestazione della richiesta PUT è limitata a una dimensione di 8 KB. Nell'intestazione della richiesta PUT, la dimensione dei metadati definiti dal sistema è limitata a 2 KB. La dimensione dei metadati definiti dal sistema viene misurata sommando il numero di byte nella US-ASCII codifica di ogni chiave e valore.

Nella tabella riportata di seguito viene fornito un elenco dei metadata definiti dal sistema e viene indicato se è possibile modificarli.

Nome	Descrizione	L'utente può modificare il valore?
Date	Data e ora correnti.	No
Cache-Control	Un campo di intestazione generico utilizzato per specificare i criteri di memorizzazione nella cache.	Sì
Content-Disposition	Informazioni relative alla modalità di presentazione dell'oggetto.	Sì
Content-Encoding	Le codifiche del contenuto (come la compressione) che sono state applicate ai dati dell'oggetto.	Sì
Content-Length	Dimensioni dell'oggetto in byte.	No
Content-Type	Il tipo di oggetto.	Sì
Last-Modified	Data di creazione dell'oggetto o data dell'ultima modifica, scegliendo la più recente delle due. Per i caricamenti in più parti, la data di creazione dell'oggetto è la data di inizio del caricamento in più parti.	No
ETag	Tag di entità (ETag) che rappresenta la versione specifica di un oggetto. Per gli oggetti che non vengono caricati come caricamento in più parti e sono non crittografati o crittografati tramite crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3), l'ETag è un digest MD5 dei dati.	No
x-amz-server-side-encryption	Un'intestazione che indica se la crittografia lato server è abilitata per l'oggetto e se tale crittografia utilizza le chiavi () o le chiavi di crittografia gestite di Amazon AWS KMS S3 AWS Key Management Service (SSE-KMS). SSE-S3	Sì

Nome	Descrizione	L'utente può modificare il valore?
Per ulteriori informazioni, consulta Protezione dei dati con la crittografia lato server .		
x-amz-checksum-crc64nvme , x-amz-checksum-crc32 , x-amz-checksum-crc32c , x-amz-checksum-sha1 , x-amz-checksum-sha256	Intestazioni che contengono il checksum o il digest dell'oggetto. Viene impostata al massimo una intestazione alla volta, a seconda dell'algoritmo di checksum che Amazon S3 deve utilizzare. Per ulteriori informazioni sulla scelta dell'algoritmo di checksum, consulta Verifica dell'integrità degli oggetti in Amazon S3 .	No
x-amz-checksum-type	Il tipo di checksum, che determina il modo in cui i checksum a livello di parte vengono combinati per creare un checksum a livello di oggetto per gli oggetti multiparte.	Sì
x-amz-version-id	Versione dell'oggetto. Quando abiliti il controllo delle versioni in un bucket, Amazon S3 assegna un ID versione agli oggetti aggiunti al bucket. Per ulteriori informazioni, consulta Conservazione di più versioni degli oggetti con Controllo delle versioni S3 .	No
x-amz-delete-marker	Contrassegno booleano che indica se l'oggetto è un contrassegno di eliminazione. Questo contrassegno viene utilizzato solo nei bucket in cui è abilitato il controllo delle versioni.	No
x-amz-storage-class	Classe di archiviazione utilizzata per l'archiviazione dell'oggetto. Per ulteriori informazioni, consulta Comprensione e gestione delle classi di storage Amazon S3 .	Sì

Nome	Descrizione	L'utente può modificare il valore?
<code>x-amz-website-redirect-location</code>	Intestazione che reindirizza le richieste per l'oggetto associato a un altro oggetto nello stesso bucket o a un URL esterno. Per ulteriori informazioni, consulta (Facoltativo) Configurazione del reindirizzamento di una pagina Web .	Sì
<code>x-amz-server-side-encryption-aws-kms-key-id</code>	Un'intestazione che indica l'ID della chiave KMS di crittografia AWS KMS simmetrica utilizzata per crittografare l'oggetto. Questa intestazione viene utilizzata solo quando è presente l'intestazione <code>x-amz-server-side-encryption</code> e ha il valore <code>aws:kms</code> .	Sì
<code>x-amz-server-side-encryption-customer-algorithm</code>	Un'intestazione che indica se la crittografia lato server con chiavi di crittografia fornite dal cliente () è abilitata. SSE-C Per ulteriori informazioni, consulta Utilizzo della crittografia lato server con chiavi fornite dal cliente () SSE-C .	Sì
<code>x-amz-tagging</code>	Il set di tag per l'oggetto. Il set di tag deve essere codificato sotto forma di parametri della URL Query.	Sì

Annotazione degli oggetti

Usa le annotazioni per allegare payload di dati denominati ai tuoi oggetti Amazon S3. Ogni annotazione è un payload di metadati personalizzato di dimensioni comprese tra 1 byte e 1 MiB che puoi creare, recuperare, elencare ed eliminare senza modificare l'oggetto stesso.

È possibile associare fino a 1.000 annotazioni a una versione dell'oggetto. Ogni annotazione ha un nome univoco e può memorizzare dati strutturati come AI-generated etichette, contesto del documento, risultati di elaborazione o record di conformità.

I casi d'uso più comuni includono l'archiviazione dei risultati di inferenza tramite machine learning, gli AI-generated incorporamenti, le etichette di moderazione dei contenuti, l'output della classificazione dei documenti, la derivazione dei dati e gli audit trail, le etichette di conformità come i contrassegni PII

o le politiche di conservazione, i metadati di immagini medicali, le informazioni sui diritti degli asset digitali e lo stato della pipeline ETL insieme all'oggetto di origine.

Le annotazioni vengono gestite utilizzando operazioni API dedicate, quindi non è necessario caricare nuovamente l'oggetto per aggiungere o aggiornare i metadati.

Puoi abilitare una tabella di annotazioni come parte della configurazione dei metadati di S3 per interrogare i dati delle annotazioni su larga scala utilizzando Athena e altri servizi di analisi. S3 Metadata archivia i dati delle annotazioni in tabelle completamente gestite Apache Iceberg che Amazon S3 mantiene automaticamente aggiornate. Per ulteriori informazioni, consulta [the section called “Individuazione dei dati con le tabelle di S3 Metadata”](#).

Le annotazioni sono disponibili in tutte le AWS regioni commerciali e in Cina (Pechino e Ningxia). Le annotazioni non sono disponibili nelle regioni Medio Oriente (Emirati Arabi Uniti) e Medio Oriente (Bahrain). Le tabelle di annotazione dei metadati S3 sono disponibili in tutte le regioni in cui sono disponibili i metadati S3.

Quando utilizzare le annotazioni rispetto ai tag degli oggetti

Utilizzate il confronto seguente per determinare se le annotazioni o i tag degli oggetti sono la soluzione migliore per il vostro caso d'uso.

Caratteristica	Tag dell'oggetto	Annotazioni
Numero massimo per oggetto	10 per versione dell'oggetto	1.000 per versione dell'oggetto
Dimensione massima	128 caratteri (chiave) + 256 caratteri (valore)	512 byte (nome) + 1 MiB (payload)
Formato dei dati	Key-value coppie di stringhe	Qualsiasi UTF-8 testo (JSON, XML, YAML, ecc.)
Mutabilità	Sì (PutObjectTagging)	Sì (PutObjectAnnotation)
Impostato durante il caricamento	Sì (PutObject, POST)	No (PutObjectAnnotation solo dopo il caricamento)

Scegli le annotazioni quando devi archiviare dati strutturati (come JSON o XML), payload con più di 256 caratteri o più di 10 voci di metadati per oggetto. Scegli i tag degli oggetti quando hai bisogno

dell'integrazione delle policy IAM, del filtro delle regole del ciclo di vita di Amazon S3 o dei report sull'allocazione dei costi.

Operazioni API per le annotazioni

Amazon S3 supporta le seguenti operazioni API per lavorare con le annotazioni:

- **PutObjectAnnotation**— Crea o sovrascrive un'annotazione su un oggetto. Si specificano il nome e il payload dell'annotazione nella richiesta.
- **GetObjectAnnotation**— Restituisce il payload di un'annotazione specifica per nome.
- **ListObjectAnnotations**— Restituisce l'elenco delle annotazioni su un oggetto. La risposta include il nome, la dimensione, l'ETag e la data dell'ultima modifica di ogni annotazione.
- **DeleteObjectAnnotation**— Rimuove un'annotazione specifica per nome.

Amazon S3 supporta anche le annotazioni nelle seguenti operazioni API:

- **CopyObject**— Copia le annotazioni dall'oggetto sorgente per impostazione predefinita. È possibile specificare l'`x-amz-annotation-directive` in testata per controllare se le annotazioni vengono copiate (COPY) o escluse (). EXCLUDE
- **UpdateBucketMetadataAnnotationTableConfiguration**— Abilita o disabilita la tabella delle annotazioni nella configurazione dei metadati S3.
- **CreateBucketMetadataConfiguration**— Accetta un nuovo `AnnotationTableConfiguration` parametro per abilitare le tabelle di annotazione quando si crea una configurazione di metadati S3.
- **GetBucketMetadataConfiguration**— Restituisce `AnnotationTableConfigurationResult` la risposta, che indica lo stato corrente della tabella di annotazione.

Limiti di annotazione

Ogni versione dell'oggetto supporta fino a 1.000 annotazioni. Le annotazioni associate a una versione dell'oggetto devono avere nomi di annotazione univoci. Si applicano i seguenti limiti:

- Il nome di un'annotazione può avere una lunghezza massima di 512 byte (UTF-8), in base alle regole di denominazione riportate di seguito.
- Una dimensione del payload di annotazioni deve essere compresa tra 1 byte e 1 MiB.
- La memoria totale delle annotazioni per oggetto può essere fino a 1 GiB (1.000 annotazioni da 1 MiB ciascuna).

- Algoritmi di checksum supportati: CRC32, CRC32C, CRC64NVME, SHA1, SHA256, SHA512, XXHASH64, XXHASH3, XXHASH128.

Regole di denominazione delle annotazioni

I nomi delle annotazioni devono soddisfare i seguenti requisiti:

- La lunghezza deve essere compresa tra 1 e 512 byte.
- Può contenere solo i seguenti caratteri: lettere (qualsiasi lingua), cifre (0-9), trattino basso (`_`), punto (`.`) e trattino (`-`).
- Non può iniziare con `aws` o `s3` (senza distinzione tra maiuscole e minuscole). Ad esempio,, `aws AWSs3`, e `S3` sono tutti prefissi riservati.
- Non deve essere vuoto o essere composto solo da spazi bianchi.

Encryption (Crittografia)

Le annotazioni vengono crittografate automaticamente quando sono inattive utilizzando la stessa configurazione di crittografia dell'oggetto principale. Il tipo di crittografia viene ereditato dall'oggetto padre, non dall'impostazione predefinita del bucket.

- SSE-S3— Se l'oggetto principale utilizza la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3), le annotazioni vengono crittografate con. SSE-S3 Se l'oggetto principale non ha una crittografia lato server configurata, per impostazione predefinita le annotazioni vengono crittografate con. SSE-S3
- SSE-KMS— Se l'oggetto principale utilizza la crittografia lato server con AWS KMS keys (SSE-KMS), le annotazioni vengono crittografate con la stessa chiave KMS. Questo vale sia per le chiavi gestite dal cliente che per le chiavi gestite. AWS Le chiavi S3 Bucket sono supportate.
- DSSE-KMS— Se l'oggetto principale utilizza la crittografia lato server a doppio livello con AWS KMS keys (DSSE-KMS), le annotazioni vengono crittografate utilizzando la stessa chiave. DSSE-KMS
- SSE-C— Server-side la crittografia con chiavi fornite dal cliente () SSE-C non è supportata per le annotazioni. Se si tenta di aggiungere un'annotazione a un oggetto crittografato con SSE-C, Amazon S3 restituisce un errore.

Checksum

Quando carichi un'annotazione utilizzando `PutObjectAnnotation`, puoi fornire un checksum per verificare l'integrità dei dati. L'algoritmo di checksum per un'annotazione è indipendente dall'algoritmo di checksum dell'oggetto principale.

Quando si copia un oggetto utilizzando `CopyObject`, Amazon S3 conserva i valori di checksum delle annotazioni dall'origine. Se si specifica un algoritmo di checksum diverso nella richiesta di copia, il nuovo algoritmo si applica sia all'oggetto che alle relative annotazioni.

Algoritmi supportati: CRC32, CRC32C, CRC64NVME, SHA1, SHA256, SHA512, XXHASH64, XXHASH3, XXHASH128.

Se l'annotazione non ha un algoritmo di checksum o un valore di checksum specificato, Amazon S3 utilizza l'algoritmo per calcolare il valore di checksum per l'annotazione. CRC-64/NVME

Comportamento del controllo delle versioni

Le annotazioni sono allegate a una versione specifica dell'oggetto.

Le annotazioni di una versione dell'oggetto sono indipendenti dalle annotazioni su altre versioni dello stesso oggetto. La creazione di una nuova versione non copia le annotazioni dalla versione precedente. L'eliminazione o l'aggiunta di un'annotazione su una versione non influisce sulle annotazioni sulle altre versioni. La sovrascrittura di un oggetto sostituisce le relative annotazioni con le annotazioni presenti nella nuova versione (se nessuna, le elimina effettivamente).

L'aggiunta, l'aggiornamento o la rimozione di un'annotazione non modifica l'ETag dell'oggetto principale.

In un bucket senza versione, se elimini o sovrascrivi l'oggetto, le annotazioni vengono eliminate con esso.

In un bucket con versione, si applica il seguente comportamento:

- Una semplice richiesta DELETE (senza specificare un ID di versione) crea un indicatore di eliminazione ma conserva le annotazioni sulla versione sottostante.
- L'eliminazione di un ID di versione specifico comporta l'eliminazione di tale versione e di tutte le annotazioni associate.
- Le annotazioni non hanno una versione indipendente. Quando sovrascrivi un'annotazione con lo stesso nome, Amazon S3 sostituisce il valore precedente senza creare una nuova versione dell'oggetto.

Important

L'eliminazione delle annotazioni è permanente e irreversibile, anche in un bucket con diverse versioni. A differenza degli oggetti nei bucket con versioni, le annotazioni non hanno indicatori di eliminazione o cronologia delle versioni. Una volta eliminata, un'annotazione non può essere recuperata.

Comportamento e coerenza della copia

Quando copi un oggetto utilizzando l'`CopyObjectAPI` (per oggetti di dimensioni inferiori a 5 GiB), Amazon S3 copia le annotazioni insieme all'oggetto in un'unica operazione.

Quando si copiano oggetti utilizzando il caricamento in più parti (ad esempio, quando gli AWS SDK AWS CLI o gli SDK utilizzano Transfer Manager per oggetti di dimensioni superiori a circa 8 MB), le annotazioni non vengono copiate per impostazione predefinita. Per includere le annotazioni, specificate nella AWS CLI o `--copy-props all` nella configurazione SDK equivalente. Con questo opt-in, l'SDK legge le annotazioni di origine, completa il caricamento in più parti e quindi scrive ogni annotazione nella destinazione. Tra il completamento del caricamento e l'ultima scrittura dell'annotazione, l'oggetto di destinazione esiste senza tutte le sue annotazioni.

Considerazioni

- Non è possibile aggiungere annotazioni come parte di una richiesta di caricamento `PutObject` o di più parti. Per aggiungere annotazioni a un oggetto, chiama `PutObjectAnnotation` dopo che l'oggetto è stato caricato. Per copiare un oggetto esistente con le relative annotazioni in una nuova posizione, utilizzatelo `CopyObject` con la direttiva di annotazione predefinita.
- Per aggiungere o aggiornare le annotazioni su molti oggetti in blocco, usa Batch Operations per richiamare una funzione Lambda che richiama ogni oggetto. `PutObjectAnnotation` Per ulteriori informazioni, consulta [the section called “Invoca funzione AWS Lambda”](#).
- Le annotazioni non sono supportate dalle seguenti funzionalità: S3 Inventory Reports, API Gateway, S3 Storage Lens, Amazon S3 File Gateway, Amazon FSx, S3 on Outposts, S3 Express One Zone (bucket di directory) e Amazon S3 Files.
- Per assicurarti di scrivere annotazioni nella versione corrente di un oggetto e non in una versione sovrascritta, utilizza l'intestazione condizionale con o. `x-amz-object-if-match` `PutObjectAnnotation DeleteObjectAnnotation` Questa intestazione convalida l'ETag

dell'oggetto padre per confermare che l'oggetto non è stato sovrascritto dall'ultima volta che il chiamante lo ha letto. L'aggiunta di tag o annotazioni non modifica l'ETag.

- Non è possibile aggiungere un'annotazione condizionatamente alla presenza o all'assenza di un'altra annotazione. L'`x-amz-object-if-match` intestazione convalida solo l'ETag dell'oggetto padre, non lo stato dell'annotazione.
- I payload delle annotazioni devono essere testo codificato valido. UTF-8 Per archiviare dati binari, codificate i dati con Base64 prima di scrivere l'annotazione.
- È possibile chiamare le operazioni API di annotazione (`PutObjectAnnotation`, `GetObjectAnnotation`, `ListObjectAnnotations`, `DeleteObjectAnnotation`) su oggetti di qualsiasi classe di archiviazione, inclusi S3 Glacier e S3 Glacier Deep Archive, senza prima ripristinare l'oggetto.

Configurazioni aggiuntive

Questa sezione spiega in che modo le annotazioni si relazionano ad altre configurazioni.

Replica

Se hai configurato S3 Replication sul tuo bucket, Amazon S3 replica automaticamente le annotazioni. Ogni annotazione viene replicata indipendentemente. Per ulteriori informazioni, consulta [the section called “Cosa viene replicato?”](#).

Per replicare le annotazioni, aggiungi `s3:GetObjectVersionAnnotationForReplication` al bucket di origine le autorizzazioni nel tuo ruolo IAM di replica. Per ulteriori informazioni, consulta [the section called “Impostazione delle autorizzazioni”](#).

Per impedire la replica delle annotazioni pur consentendo la replica degli oggetti, aggiungi un'istruzione `deny for` nella policy del ruolo di replica. `s3:ReplicateObjectAnnotation` La replica degli oggetti continua ad avere successo; viene bloccata solo la replica delle annotazioni.

Notifiche degli eventi

Amazon S3 può inviare notifiche di eventi quando le annotazioni vengono create, aggiornate o eliminate. Puoi configurare i seguenti tipi di eventi:

- `s3:ObjectAnnotation:Put`— Inviato quando viene creata o aggiornata un'annotazione.
- `s3:ObjectAnnotation:Delete`— Inviato quando un'annotazione viene eliminata.

Per ulteriori informazioni, consulta [the section called “Tipi di notifiche e destinazioni”](#).

Gestione delle annotazioni

Puoi aggiungere, recuperare ed eliminare annotazioni sui tuoi oggetti Amazon S3 utilizzando gli SDK,, o. Console di gestione AWS AWS CLI AWS Le seguenti sezioni descrivono come eseguire ciascuna operazione.

Aggiungere o aggiornare un'annotazione

È possibile aggiungere una nuova annotazione a un oggetto o aggiornare un'annotazione esistente sostituendone il payload.

Utilizzo della console S3

Per aggiungere un'annotazione a un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti, scegli il nome dell'oggetto che desideri annotare.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Annotazioni e scegli Aggiungi annotazione.
6. Per Nome, inserite un nome per l'annotazione (ad esempio,). ml . sentiment I nomi devono contenere da 1 a 512 byte e possono contenere lettere Unicode, cifre, caratteri di sottolineatura, punti e trattini. I aws nomi non possono iniziare con o. s3
7. Scegli Scegli file per caricare il contenuto dell'annotazione. Il file deve essere UTF-8 codificabile e avere una dimensione massima di 1 MB.

Per completare l'annotazione

1. (Facoltativo) In Checksum, scegli un algoritmo di checksum.
2. Scegli Aggiungi annotazione.

 Note

Per visualizzare il contenuto di un'annotazione dopo la sua creazione, è necessario scaricarla. La console S3 non visualizza il contenuto delle annotazioni in linea.

Utilizzo di AWS CLI

Per aggiungere o aggiornare un'annotazione su un oggetto, usa il comando `put-object-annotation`. Il `--annotation-payload` parametro accetta un percorso di file.

```
aws s3api put-object-annotation \
  --bucket amzn-s3-demo-bucket \
  --key myDocument.pdf \
  --annotation-name "ml.sentiment" \
  --annotation-payload /tmp/sentiment.json
```

Per scrivere l'annotazione solo se l'oggetto non è stato sovrascritto dall'ultima volta che l'avete letto, specificate il `--object-if-match` parametro con l'ETag corrente dell'oggetto.

```
aws s3api put-object-annotation \
  --bucket amzn-s3-demo-bucket \
  --key myDocument.pdf \
  --annotation-name "ml.sentiment" \
  --annotation-payload /tmp/sentiment.json \
  --object-if-match "\"d6eb32081c822ed572b70567826d9d9d\""
```

Utilizzo di AWS SDK

L'esempio seguente utilizza l' AWS SDK per Python (Boto3) per aggiungere un'annotazione a un oggetto.

```
import boto3
import json

s3 = boto3.client('s3')

s3.put_object_annotation(
    Bucket='amzn-s3-demo-bucket',
    Key='myDocument.pdf',
```

```
AnnotationName='ml.sentiment',  
AnnotationPayload=json.dumps({  
    'score': 0.95,  
    'label': 'positive',  
    'model': 'sentiment-v3'  
}).encode('utf-8')  
)
```

Recupero delle annotazioni

È possibile recuperare un'annotazione specifica o elencare tutte le annotazioni su un oggetto.

Utilizzo della console S3

Per recuperare un'annotazione

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti scegliere il nome dell'oggetto.
4. Scegli la scheda Proprietà e scorri fino alla sezione Annotazioni.
5. Per visualizzare il contenuto delle annotazioni, scegli Scarica accanto al nome dell'annotazione.

Utilizzo di AWS CLI

Per recuperare un'annotazione specifica, utilizzate il comando. `get-object-annotation`

```
aws s3api get-object-annotation \  
    --bucket amzn-s3-demo-bucket \  
    --key myDocument.pdf \  
    --annotation-name "ml.sentiment" \  
    output.json
```

Per elencare tutte le annotazioni su un oggetto, usate il comando. `list-object-annotations`

```
aws s3api list-object-annotations \  
    --bucket amzn-s3-demo-bucket \  
    --key myDocument.pdf
```

Utilizzo di AWS SDK

L'esempio seguente utilizza l' AWS SDK per Python (Boto3) per recuperare ed elencare le annotazioni.

```
import boto3
import json

s3 = boto3.client('s3')

# Retrieve a specific annotation
response = s3.get_object_annotation(
    Bucket='amzn-s3-demo-bucket',
    Key='myDocument.pdf',
    AnnotationName='ml.sentiment'
)
content = json.loads(response['AnnotationPayload'].read())

# List all annotations on an object
response = s3.list_object_annotations(
    Bucket='amzn-s3-demo-bucket',
    Key='myDocument.pdf'
)
for annotation in response['Annotations']:
    print(f"{annotation['AnnotationName']} - {annotation['Size']} bytes")
```

Eliminazione delle annotazioni

È possibile eliminare un'annotazione specifica da un oggetto. L'eliminazione delle annotazioni è permanente e non può essere annullata.

Utilizzo della console S3

Per eliminare un'annotazione

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti scegliere il nome dell'oggetto.
4. Scegli la scheda Proprietà e scorri fino alla sezione Annotazioni.
5. Seleziona l'annotazione che desideri eliminare.

6. Scegli Elimina, quindi conferma l'eliminazione.

Utilizzo di AWS CLI

Per eliminare un'annotazione specifica, utilizzate il `delete-object-annotation` comando.

```
aws s3api delete-object-annotation \  
  --bucket amzn-s3-demo-bucket \  
  --key myDocument.pdf \  
  --annotation-name "ml.sentiment"
```

Utilizzo di AWS SDK

L'esempio seguente utilizza l' AWS SDK per Python (Boto3) per eliminare un'annotazione.

```
import boto3  
  
s3 = boto3.client('s3')  
  
s3.delete_object_annotation(  
    Bucket='amzn-s3-demo-bucket',  
    Key='myDocument.pdf',  
    AnnotationName='ml.sentiment'  
)
```

Etichettare i tuoi oggetti

Utilizza il tagging degli oggetti per catalogare lo storage. Ogni tag è una coppia chiave-valore.

Se devi archiviare dati strutturati con più di 256 caratteri per valore, associare più di 10 voci di metadati a un oggetto o allegare contenuti complessi come risultati o AI-generated etichette di inferenza con apprendimento automatico, consulta. [Annotazione degli oggetti](#)

È possibile aggiungere tag ai nuovi oggetti durante il caricamento oppure è possibile aggiungerli agli oggetti esistenti.

- È possibile associare fino a un massimo di 10 tag a ciascun oggetto. I tag associati a un oggetto devono avere chiavi di tag univoche.
- Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori dei tag possono contenere fino a 256 caratteri Unicode. I tag degli oggetti Amazon S3 sono rappresentati internamente in UTF-16. Nota che in UTF-16, i caratteri occupano 1 o 2 posizioni di caratteri.

- La chiave e i valori fanno distinzione tra maiuscole e minuscole.
- Per ulteriori informazioni sulle restrizioni relative ai tag, consulta le restrizioni relative ai [User-defined tag](#) nella Guida per l'utente di AWS Billing and Cost Management. Per le restrizioni di base dei tag, consulta [Restrizioni dei tag](#) nella Guida all'utente di Amazon EC2.

Esempi

Considerare i seguenti esempi di tagging:

Example Informazioni PHI

Supponiamo che un oggetto contenga dati sanitari protetti (PHI). È possibile assegnare un tag all'oggetto utilizzando la seguente coppia chiave-valore.

```
PHI=True
```

oppure

```
Classification=PHI
```

Example File di progetto

Supponiamo di archiviare i file di progetto nel bucket S3. È possibile assegnare un tag a questi oggetti mediante una chiave denominata `Project` e un valore, come illustrato di seguito.

```
Project=Blue
```

Example Tag multipli

È possibile aggiungere più tag a un oggetto, come illustrato di seguito.

```
Project=x  
Classification=confidential
```

Prefissi e tag dei nomi delle chiavi

I prefissi dei nomi di una chiave dell'oggetto ti permettono anche di categorizzare lo storage. Tuttavia, la categorizzazione basata sui prefissi è monodimensionale. Consideriamo i seguenti nomi delle chiavi degli oggetti:

```
photos/photo1.jpg  
project/projectx/document.pdf  
project/projecty/document2.pdf
```

Questi nomi di chiavi hanno il prefisso `photos/`, `project/projectx/` e `project/projecty/`. Questi prefissi consentono la categorizzazione monodimensionale, ossia: tutti gli elementi sotto un prefisso costituiscono una categoria. Ad esempio, il prefisso `project/projectx` identifica tutti i documenti relativi al progetto x.

Il tagging rende disponibile un'altra dimensione. Se si desidera che `photo1` sia nella categoria `project x`, è possibile assegnare un tag all'oggetto di conseguenza.

Altri vantaggi

Oltre alla classificazione dei dati, il tagging offre vantaggi quali i seguenti:

- I tag degli oggetti consentono un controllo degli accessi granulare per le autorizzazioni. Ad esempio, è possibile concedere a un utente le autorizzazioni per leggere esclusivamente gli oggetti con tag specifici.
- I tag degli oggetti consentono una gestione granulare del ciclo di vita dell'oggetto, in cui è possibile specificare filtri basati su tag, oltre a prefissi del nome della chiave, in una regola del ciclo di vita.
- L'utilizzo dell'analisi Amazon S3 consente di configurare filtri per raggruppare gli oggetti per l'analisi in base ai tag dell'oggetto, al prefisso del nome della chiave di accesso o in base sia al prefisso che ai tag.
- Puoi anche personalizzare le CloudWatch metriche di Amazon per visualizzare le informazioni tramite filtri di tag specifici. Nelle seguenti sezioni sono fornite maggiori informazioni.

Important

Si possono utilizzare tag per etichettare oggetti contenenti informazioni riservate (ad esempio le informazioni personali (PII) o i dati sanitari protetti (PHI)). Tuttavia, i tag non devono contenere informazioni confidenziali.

Aggiunta di serie di tag oggetto a più oggetti Amazon S3 con una singola richiesta

Per aggiungere set di tag a più di un oggetto Amazon S3 con una sola richiesta, puoi utilizzare le operazioni in batch S3. Fornisci alle operazioni in batch S3 un elenco di oggetti su cui operare. Le

operazioni in batch S3 richiamano la rispettiva API per eseguire l'operazione specificata. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti contenenti esabyte di dati.

La funzionalità Operazioni in batch S3 tiene traccia dei progressi, invia notifiche e memorizza un report dettagliato sul completamento di tutte le azioni, offrendo un'esperienza serverless completamente gestita e verificabile. Puoi utilizzare S3 Batch Operations tramite la console Amazon S3, AWS CLI, gli AWS SDK o l'API REST. Per ulteriori informazioni, consulta [the section called “Nozioni di base sulle operazioni in batch”](#).

Per ulteriori informazioni sui tag degli oggetti, consulta [Gestione di tag degli oggetti](#).

Operazioni API correlate al tagging oggetti

Amazon S3 supporta le seguenti operazioni API, specifiche per il tagging oggetti:

Operazioni delle API sugli oggetti

- [PUT Object tagging](#) – Sostituisce i tag su un oggetto. È possibile specificare i tag nel corpo della richiesta. La gestione di tag degli oggetti mediante queste API prevede due scenari distinti.
 - L'oggetto non ha tag – Mediante questa API, è possibile aggiungere un set di tag a un oggetto (l'oggetto non ha tag precedenti).
 - L'oggetto ha un set tag esistenti – Per modificare il set di tag esistenti, è necessario prima recuperarlo, modificarlo sul lato client, quindi utilizzare questa API per sostituire il set di tag.

Note

Se si invia questa richiesta con un set di tag vuoto, Amazon S3 elimina il set di tag esistenti sull'oggetto. Se si usa questo metodo, verrà addebitata una richiesta Tier 1 (PUT). Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

La richiesta [DELETE Object tagging](#) è preferibile perché fornisce lo stesso risultato senza nessun addebito.

- [GET Object tagging](#) – Restituisce il set di tag associato a un oggetto. Amazon S3 restituisce i tag degli oggetti nel corpo della risposta.
- [DELETE Object tagging](#) – Elimina il set di tag associato a un oggetto.

Altre operazioni API che supportano il tagging

- [PUT Object](#) e [Initiate Multipart Upload](#) – È possibile specificare i tag quando si creano oggetti. I tag possono essere specificati utilizzando l'intestazione di richiesta `x-amz-tagging`.
- [GET Object](#) – Anziché restituire il set di tag, Amazon S3 restituisce il conteggio dei tag degli oggetti nell'intestazione di `x-amz-tag-count` (solo se il richiedente dispone delle autorizzazioni per leggere i tag) poiché le dimensioni della risposta nell'intestazione sono limitate a 8 K di byte. Se si desidera visualizzare i tag, fare un'altra richiesta di operazione API [GET Object tagging](#).
- [POST Object](#) – È possibile specificare tag nella richiesta POST.

È possibile utilizzare l'API `PUT Object` per creare oggetti con tag, purché i tag della richiesta non superino le dimensioni massime dell'intestazione della richiesta HTTP di 8 Kbyte. Se i tag specificati superano le dimensioni massime dell'intestazione, è possibile utilizzare questo metodo POST che consiste nell'includere i tag nel corpo.

[PUT Object - Copy](#) – È possibile specificare `x-amz-tagging-directive` nella richiesta per indicare ad Amazon S3 di copiare (comportamento di default) i tag o sostituirli mediante un nuovo set di tag fornito nella richiesta.

Tieni presente quanto segue:

- Il tagging degli oggetti S3 è molto coerente. Per ulteriori informazioni, consulta [Modello di consistenza dati Amazon S3](#).

Configurazioni aggiuntive

In questa sezione viene descritto in che modo il tagging oggetti è correlato alle altre configurazioni.

Tagging oggetti e gestione del ciclo di vita

In una configurazione del ciclo di vita del bucket, è possibile specificare un filtro per selezionare un sottoinsieme di oggetti a cui si applica la regola. È possibile specificare un filtro in base ai prefissi dei nomi delle chiavi, ai tag degli oggetti o entrambi.

Supponiamo di archiviare foto (in formato raw e in formato finito) nel bucket Amazon S3. A questi oggetti possono essere assegnati tag nel modo seguente.

```
phototype=raw  
or  
phototype=finished
```

È possibile archiviare le foto non elaborate in Amazon Glacier poco dopo la creazione. È possibile configurare una regola del ciclo di vita con un filtro che identifica il sottoinsieme di oggetti con prefisso del nome della chiave (photos/) aventi un tag specifico (phototype=raw).

Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#).

Tagging degli oggetti e replica

Se è stata configurata la replica nel bucket, Amazon S3 replica i tag, purché ad Amazon S3 siano assegnate le autorizzazioni per leggerli. Per ulteriori informazioni, consulta [Panoramica della configurazione della replica in tempo reale](#).

Notifiche eventi di assegnazione tag su oggetti

Puoi configurare una notifica eventi Amazon S3 per ricevere una notifica quando viene aggiunto o eliminato un tag oggetto da un oggetto. Il tipo di evento `s3:ObjectTagging:Put` ti avvisa quando un tag viene INSERITO su un oggetto o quando viene aggiornato un tag esistente. Il tipo di evento `s3:ObjectTagging:Delete` ti avvisa quando un tag viene rimosso da un oggetto. Per ulteriori informazioni, consulta [Abilitazione notifiche eventi](#).

Per ulteriori informazioni sul tagging degli oggetti, consulta i seguenti argomenti:

Argomenti

- [Tagging e policy di controllo degli accessi](#)
- [Gestione di tag degli oggetti](#)

Tagging e policy di controllo degli accessi

Le policy di autorizzazione (policy bucket e policy utente) possono essere utilizzate per gestire le autorizzazioni relative al tagging oggetti. Per le operazioni delle policy, consulta i seguenti argomenti:

- [Operazioni con gli oggetti](#)
- [Operazioni relative ai bucket](#)

I tag degli oggetti consentono un controllo degli accessi granulare per la gestione delle autorizzazioni. È possibile concedere autorizzazioni condizionali in base ai tag degli oggetti. Amazon S3 supporta le seguenti chiavi di condizione che è possibile utilizzare per concedere autorizzazioni condizionali basate sui tag degli oggetti.

- `s3:ExistingObjectTag/<tag-key>` – Utilizzare questa chiave di condizione per verificare che un tag degli oggetti esistente abbia una chiave e un valore di tag specifici.

Note

Quando si concedono autorizzazioni per le operazioni `PUT Object` e `DELETE Object`, questa chiave di condizione non è supportata. Ciò significa che non è possibile creare una policy per concedere o rifiutare le autorizzazioni utente che consentono di eliminare o sovrascrivere un oggetto in base ai relativi tag esistenti.

- `s3:RequestObjectTagKeys` – Utilizzare questa chiave di condizione per limitare le chiavi di tag che si desidera consentire sugli oggetti. Ciò è utile quando si aggiungono tag agli oggetti utilizzando le richieste di oggetti `PutObjectTagging` and `PutObject` e `POST`.
- `s3:RequestObjectTag/<tag-key>` – Utilizzare questa chiave di condizione per limitare i valori e le chiavi di tag che si desidera consentire sugli oggetti. Ciò è utile quando si aggiungono tag agli oggetti utilizzando le richieste `PutObjectTagging` and `PutObject` e `POST Bucket`.

Per un elenco completo delle chiavi di condizione specifiche per il servizio Amazon S3, consulta [Esempi di policy per i bucket che utilizzano le chiavi di condizione](#). Le seguenti policy di autorizzazione illustrano il modo in cui il tagging oggetti consente una gestione granulare delle autorizzazioni di accesso.

Example 1: concedere a un utente autorizzazioni di sola lettura per gli oggetti con un valore di tag o chiave specifico

La seguente policy di autorizzazione limita l'utente a leggere solo gli oggetti che hanno il tag chiave e il valore `environment: production`. Questa policy utilizza la chiave di condizione `s3:ExistingObjectTag` per specificare la chiave e il valore del tag.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:role/JohnDoe"
        ]
      }
    }
  ]
}
```

```

    ]
  },
  "Effect": "Allow",
  "Action": ["s3:GetObject", "s3:GetObjectVersion"],
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "StringEquals": {
      "s3:ExistingObjectTag/environment": "production"
    }
  }
}
]
}

```

Example 2: limitare le chiavi di tag dell'oggetto che gli utenti possono aggiungere

La seguente policy di autorizzazione concede a un utente le autorizzazioni per eseguire l'operazione `s3:PutObjectTagging`, che permette di aggiungere tag a un oggetto esistente. La condizione utilizza la chiave di condizione `s3:RequestObjectTagKeys` per specificare le chiavi di tag consentite, ad esempio `Owner` o `CreationDate`. Per ulteriori informazioni, consulta la sezione [Creazione di una condizione con più chiavi o valori](#) nella Guida per l'utente IAM.

La policy garantisce che ogni chiave di tag specificata nella richiesta sia una chiave di tag autorizzata. Il qualificatore `ForAnyValue` nella condizione garantisce che almeno una delle chiavi specificate sia presente nella richiesta.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:role/JohnDoe"
        ]
      },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}

```

```

    "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
        "Owner",
        "CreationDate"
    ]}
  }
}

```

Example 3: richiedere una chiave e un valore di tag specifici per consentire agli utenti di aggiungere tag di oggetti

Il seguente esempio di policy concede a un utente l'autorizzazione a eseguire l'azione `s3:PutObjectTagging`, che consente di aggiungere tag a un oggetto esistente. La condizione prevede che l'utente includa una chiave di tag specifica (ad esempio, *Project*) con valore impostato su *X*.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {"AWS": [
        "arn:aws:iam::111122223333:user/JohnDoe"
      ]},
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"}
    }
  ]
}

```

Gestione di tag degli oggetti

Questa sezione spiega come gestire i tag degli oggetti utilizzando gli AWS SDK per Java e .NET o la console Amazon S3.

Il tagging degli oggetti consente di classificare l'archiviazione in bucket per uso generico. Ciascun tag è una coppia chiave-valore che aderisce alle seguenti regole:

- Puoi associare fino a 10 tag a un oggetto. I tag associati a un oggetto devono avere chiavi di tag univoche.
- Una chiave tag può contenere fino a 128 caratteri Unicode e i valori dei tag possono avere una lunghezza massima di 256 caratteri Unicode. I tag degli oggetti Amazon S3 sono rappresentati internamente in UTF-16. Nota che in UTF-16, i caratteri occupano 1 o 2 posizioni di caratteri.
- La chiave e i valori fanno distinzione tra maiuscole e minuscole.

Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#). Per ulteriori informazioni sulle restrizioni relative ai tag, consulta [Restrizioni relative ai User-Defined tag](#) nella Guida per Gestione costi e fatturazione AWS l'utente.

Utilizzo della console S3

Per aggiungere tag a un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket contenente l'oggetto.
4. Seleziona la casella di controllo a sinistra dei nomi degli oggetti da modificare.
5. Dal menu Operazioni, seleziona Modifica tag.
6. Esamina gli oggetti elencati e seleziona Aggiungi tag.
7. Ogni tag oggetto è una coppia chiave-valore. Immettere una chiave e un valore. Per aggiungere un altro tag, scegliere Add Tag (Aggiungi tag).

È possibile immettere fino a un massimo di 10 tag per ciascun oggetto.

8. Seleziona Salva modifiche.

Amazon S3 aggiungerà i tag agli oggetti specificati.

Per ulteriori informazioni, vedi anche [Visualizzazione delle proprietà di un oggetto nella console di Amazon S3](#) e [Caricamento degli oggetti](#) in questa guida.

Utilizzo di AWS SDK

Java

Per gestire i tag degli oggetti utilizzando l' AWS SDK per Java, puoi impostare i tag per un nuovo oggetto e recuperare o sostituire i tag per un oggetto esistente. Per ulteriori informazioni sul tagging dell'oggetto, consulta [Etichettare i tuoi oggetti](#).

Caricare un oggetto in un bucket e impostare tag mediante un'interfaccia S3Client. Per esempi, consulta [Caricamento di un oggetto in un bucket](#) nella Guida di riferimento delle API di Amazon S3.

.NET

L'esempio seguente mostra come utilizzare il AWS SDK per .NET per impostare i tag per un nuovo oggetto e recuperare o sostituire i tag per un oggetto esistente. Per ulteriori informazioni sul tagging dell'oggetto, consulta [Etichettare i tuoi oggetti](#).

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    public class ObjectTagsTest
    {
        private const string bucketName = "**** bucket name ****";
        private const string keyName = "**** key name for the new object ****";
        private const string filePath = @"**** file path ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
            RegionEndpoint.USWest2;
        private static IAmazonS3 client;
```

```
public static void Main()
{
    client = new AmazonS3Client(bucketRegion);
    PutObjectWithTagsTestAsync().Wait();
}

static async Task PutObjectWithTagsTestAsync()
{
    try
    {
        // 1. Put an object with tags.
        var putRequest = new PutObjectRequest
        {
            BucketName = bucketName,
            Key = keyName,
            FilePath = filePath,
            TagSet = new List<Tag>{
                new Tag { Key = "Keyx1", Value = "Value1"},
                new Tag { Key = "Keyx2", Value = "Value2" }
            }
        };

        PutObjectResponse response = await
client.PutObjectAsync(putRequest);
        // 2. Retrieve the object's tags.
        GetObjectTaggingRequest getTagsRequest = new GetObjectTaggingRequest
        {
            BucketName = bucketName,
            Key = keyName
        };

        GetObjectTaggingResponse objectTags = await
client.GetObjectTaggingAsync(getTagsRequest);
        for (int i = 0; i < objectTags.Tagging.Count; i++)
            Console.WriteLine("Key: {0}, Value: {1}",
objectTags.Tagging[i].Key, objectTags.Tagging[i].Value);

        // 3. Replace the tagset.

        Tagging newTagSet = new Tagging();
        newTagSet.TagSet = new List<Tag>{
            new Tag { Key = "Key3", Value = "Value3"},
            new Tag { Key = "Key4", Value = "Value4" }
        }
    }
}
```



```
};

        PutObjectTaggingRequest putObjTagsRequest = new
PutObjectTaggingRequest()
        {
            BucketName = bucketName,
            Key = keyName,
            Tagging = newTagSet
        };
        PutObjectTaggingResponse response2 = await
client.PutObjectTaggingAsync(putObjTagsRequest);

        // 4. Retrieve the object's tags.
        GetObjectTaggingRequest getTagsRequest2 = new
GetObjectTaggingRequest();
        getTagsRequest2.BucketName = bucketName;
        getTagsRequest2.Key = keyName;
        GetObjectTaggingResponse objectTags2 = await
client.GetObjectTaggingAsync(getTagsRequest2);
        for (int i = 0; i < objectTags2.Tagging.Count; i++)
            Console.WriteLine("Key: {0}, Value: {1}",
objectTags2.Tagging[i].Key, objectTags2.Tagging[i].Value);

    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine(
            "Error encountered ***. Message:'{0}' when writing an
object"
            , e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine(
            "Encountered an error. Message:'{0}' when writing an object"
            , e.Message);
    }
}
}
```

Modifica dei metadati degli oggetti nella console di Amazon S3

È possibile utilizzare la console Amazon S3 per modificare i metadati degli oggetti S3 esistenti utilizzando l'azione Copia. Per modificare i metadati, si copiano gli oggetti nella stessa destinazione e si specificano i nuovi metadati da applicare, che sostituiscono i vecchi metadati dell'oggetto. Alcuni metadati vengono impostati da Amazon S3 quando carichi l'oggetto. Ad esempio, Content-Length e Last-Modified sono campi di metadati degli oggetti definiti dal sistema che non possono essere modificati da un utente.

È inoltre possibile impostare metadati definiti dall'utente al momento del caricamento dell'oggetto e sostituirli in base alle proprie esigenze. Ad esempio, è possibile che tu disponga di un insieme di oggetti che inizialmente hai memorizzato nella classe di storage STANDARD. Nel tempo, potrebbe non essere più necessario che questi dati siano altamente disponibili. Quindi, si può cambiare la classe di storage in GLACIER sostituendo il valore della chiave `x-amz-storage-class` da STANDARD a GLACIER.

Note

Quando sostituite i metadati degli oggetti definiti dal sistema o definiti dall'utente utilizzando l'azione Copia, tenete presente quanto segue:

- È necessario specificare i metadati esistenti che si desidera conservare, i metadati che si desidera aggiungere e i metadati che si desidera modificare.
- Se l'oggetto è inferiore a 5 GB, è possibile utilizzare l'azione Copia nella console S3 per sostituire i metadati dell'oggetto. Se l'oggetto è superiore a 5 GB, è possibile sostituire i metadati dell'oggetto quando si copia un oggetto con caricamento multiparte utilizzando gli SDK [AWS CLI](#) o [AWS SDK](#). Per ulteriori informazioni, consulta [Copia di un oggetto utilizzando il caricamento in più parti](#).
- Per un elenco di autorizzazioni aggiuntive necessarie per sostituire i metadati, consulta [the section called “Autorizzazioni necessarie per le operazioni API S3”](#). Per esempi di policy che concedono questa autorizzazione, consulta [the section called “Identity-based esempi di policy”](#).
- Questa operazione crea una copia dell'oggetto con le impostazioni aggiornate e la data dell'ultima modifica. Se è abilitata la funzione Versioni multiple di S3, viene creata una nuova versione dell'oggetto e l'oggetto esistente diventa una versione precedente. Se il controllo delle versioni S3 non è abilitato, una nuova copia dell'oggetto sostituisce l'oggetto

originale. L' Account AWS associato al ruolo IAM che modifica la proprietà diventa anche il proprietario del nuovo oggetto o (versione dell'oggetto).

- La modifica dei metadati sostituisce i valori dei nomi delle chiavi esistenti.
- Gli oggetti crittografati con le chiavi di crittografia fornite dal cliente (SSE-C) non possono essere copiati utilizzando la console. È necessario utilizzare l' AWS SDK o AWS CLI l'API REST di Amazon S3.
- Quando si copia un oggetto tramite la console Amazon S3, è possibile ricevere il messaggio di errore “Copied metadata can’t be verified”. La console utilizza le intestazioni per recuperare e impostare i metadati per l’oggetto. Se la configurazione della rete o del browser modifica le richieste di rete, questo comportamento potrebbe causare la scrittura non intenzionale di metadati (come intestazioni `Cache-Control` modificate) nell’oggetto copiato. Amazon S3 non può verificare questi metadati non intenzionali.

Per risolvere questo problema, controlla la configurazione della rete e del browser per assicurarti che non modifichino le intestazioni, ad esempio `Cache-Control`. Per ulteriori informazioni, consulta [Il modello di responsabilità condivisa](#).

Warning

Quando si sostituiscono i metadati per le cartelle, attendere il termine dell'azione di copia prima di aggiungere nuovi oggetti alla cartella. In caso contrario, potrebbero essere modificati anche i nuovi oggetti.

I seguenti argomenti descrivono come sostituire i metadati di un oggetto utilizzando l'azione Copia nella console Amazon S3.

Note

Per aggiungere, visualizzare o eliminare annotazioni su un oggetto, utilizza la sezione Annotazioni nella scheda Proprietà dell'oggetto. Per ulteriori informazioni, consulta [Gestione delle annotazioni](#).

Sostituzione dei metadati definiti dal sistema

È possibile sostituire alcuni metadati definiti dal sistema per un oggetto S3. Per un elenco dei metadati e dei valori definiti dal sistema che è possibile modificare, consulta [System-defined metadati degli oggetti](#).

Per sostituire i metadati di un oggetto definiti dal sistema

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.
3. Nell'elenco dei bucket scegli il nome del bucket che contiene gli oggetti che desideri modificare.
4. Seleziona la casella di controllo degli oggetti da modificare.
5. Nel menu Azioni, scegli Copia dall'elenco delle opzioni visualizzate.
6. Per specificare il percorso di destinazione, scegli Sfoglia S3, naviga nella stessa destinazione degli oggetti di origine e seleziona la casella di controllo di destinazione. Scegliere Choose destination (Scegli destinazione).

In alternativa, immettere il percorso di destinazione.

7. Se non è abilitato il controllo delle versioni del bucket, viene visualizzato un avviso che consiglia di abilitarlo per evitare la sovrascrittura o l'eliminazione involontaria di oggetti. Se si desidera mantenere tutte le versioni degli oggetti in questo bucket, seleziona Abilita versioni multiple per il bucket. È inoltre possibile visualizzare le proprietà di crittografia e Object Lock predefinite in Dettagli destinazione.
8. In Impostazioni di copia aggiuntive, scegli Specifica impostazioni per specificare le impostazioni dei Metadati.
9. Spostati nella sezione Metadati e scegli Sostituisci tutti i metadati.
10. Seleziona Add metadata (Aggiungi metadati).
11. Per Tipo di metadati, seleziona. System-defined
12. Specificare una Key (Chiave) univoca e il Value (Valore) dei metadati.
13. Per modificare metadati aggiuntivi, scegliere Add metadata (Aggiungi metadati). Puoi anche scegliere Rimuovi per rimuovere un insieme di valori-chiave-tipo.
14. Scegli Copia. Amazon S3 salva le modifiche ai metadati.

Sostituzione di metadati definiti dall'utente

È possibile sostituire i metadati definiti dall'utente di un oggetto combinando il prefisso dei metadati, `x-amz-meta-` e un nome scelto dall'utente per creare una chiave personalizzata. Ad esempio, se si aggiunge il nome personalizzato `alt-name`, la chiave dei metadati sarà `x-amz-meta-alt-name`.

User-defined i metadati possono avere una dimensione totale di 2 KB. Per calcolare la dimensione totale dei metadati definiti dall'utente, sommate il numero di byte nella UTF-8 codifica per ogni chiave e valore. Entrambe le chiavi e i relativi valori devono essere conformi agli standard. US-ASCII Per ulteriori informazioni, consulta [User-defined metadati](#).

Per sostituire i metadati di un oggetto definiti dall'utente

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione, scegli Bucket, quindi scegli la scheda Bucket per uso generico o Bucket di directory. Naviga al bucket o alla cartella Amazon S3 che contiene gli oggetti da modificare.
3. Seleziona la casella di controllo degli oggetti da modificare.
4. Nel menu Azioni, scegli Copia dall'elenco delle opzioni visualizzate.
5. Per specificare il percorso di destinazione, scegli Sfoglia S3, naviga nella stessa destinazione degli oggetti di origine e seleziona la casella di controllo di destinazione. Scegliere Choose destination (Scegli destinazione).

In alternativa, immettere il percorso di destinazione.

6. Se non è abilitato il controllo delle versioni del bucket, viene visualizzato un avviso che consiglia di abilitarlo per evitare la sovrascrittura o l'eliminazione involontaria di oggetti. Se si desidera mantenere tutte le versioni degli oggetti in questo bucket, seleziona Abilita versioni multiple per il bucket. È inoltre possibile visualizzare le proprietà di crittografia e Object Lock predefinite in Dettagli destinazione.
7. In Impostazioni di copia aggiuntive, scegli Specifica impostazioni per specificare le impostazioni dei Metadati.
8. Spostati nella sezione Metadati e scegli Sostituisci tutti i metadati.
9. Seleziona Add metadata (Aggiungi metadati).
10. Per Tipo di metadati, scegli. User-defined

11. Immetti una Chiave univoca e personalizzata dopo `x-amz-meta-`. Immettere anche un Value (Valore) metadati.
12. Per aggiungere metadati, scegliere Add metadata (Aggiungi metadati). Puoi anche scegliere Rimuovi per rimuovere un insieme di valori-chiave-tipo.
13. Scegli Copia. Amazon S3 salva le modifiche ai metadati.

Individuazione dei dati con le tabelle di S3 Metadata

Amazon S3 Metadata accelera l'individuazione dei dati acquisendo automaticamente i metadati per gli oggetti nei bucket per uso generico e memorizzandoli in tabelle Apache Iceberg di sola lettura e completamente gestite su cui è possibile eseguire query. Queste tabelle di sola lettura sono chiamate tabelle di metadati. Quando gli oggetti vengono aggiunti, aggiornati o rimossi dai bucket per uso generico, S3 Metadata aggiorna automaticamente le tabelle di metadati corrispondenti per riflettere le ultime modifiche.

Per impostazione predefinita, S3 Metadata fornisce tre tipi di metadati:

- [System-defined metadati](#), come l'ora di creazione di un oggetto e la classe di archiviazione
- Metadati degli oggetti personalizzati, come tag, annotazioni e [metadati](#) definiti dall'utente inclusi durante il caricamento degli oggetti
- Metadati degli eventi, ad esempio quando un oggetto viene aggiornato o eliminato e chi ha effettuato la richiesta Account AWS

Con S3 Metadata, puoi trovare, archiviare e interrogare facilmente i metadati per i tuoi oggetti S3, in modo da preparare rapidamente i dati da utilizzare nell'analisi aziendale, nel recupero dei contenuti, nella formazione sui modelli di intelligenza artificiale e machine learning () e altro ancora. AI/ML

Per ogni bucket generico, puoi creare una configurazione di tabella di metadati che contiene fino a tre tabelle di metadati:

- Tabella del diario: per impostazione predefinita, la configurazione della tabella dei metadati contiene una tabella del diario, che acquisisce gli eventi che si verificano per gli oggetti nel bucket. La tabella del diario registra le modifiche apportate ai dati pressoché in tempo reale, aiutando a individuare i nuovi dati caricati nel bucket, a tenere traccia degli oggetti eliminati di recente, a monitorare le transizioni del ciclo di vita e altro ancora. La tabella del diario registra i nuovi oggetti e gli aggiornamenti degli oggetti e dei relativi metadati (gli aggiornamenti che richiedono un'operazione PUT o un'operazione DELETE).

La tabella del diario acquisisce i metadati solo per gli eventi di modifica (come caricamenti, aggiornamenti ed eliminazioni) che si verificano dopo la creazione della configurazione della tabella dei metadati. Poiché questa tabella è sottoponibile a query, è possibile controllare le modifiche al bucket tramite semplici query SQL.

La tabella del diario è obbligatoria per ogni configurazione della tabella dei metadati. Nella versione iniziale di S3 Metadata, la tabella del diario era denominata “tabella dei metadati”.

Per ulteriori informazioni sui dati archiviati nelle tabelle del diario, consulta [the section called “Schema delle tabelle del diario”](#).

Per ridurre al minimo i costi di archiviazione, è possibile scegliere la scadenza dei record della tabella del diario. Per ulteriori informazioni, consulta [the section called “Scadenza dei record della tabella del diario”](#).

- Tabella di inventario in tempo reale: facoltativamente, è possibile aggiungere una tabella di inventario in tempo reale alla configurazione della tabella dei metadati. La tabella di inventario in tempo reale fornisce un inventario semplice e sottoponibile a query di tutti gli oggetti e delle relative versioni presenti nel bucket in modo da poter determinare lo stato più recente dei dati.

È possibile utilizzare la tabella di inventario in tempo reale per semplificare e velocizzare i flussi di lavoro aziendali e i processi relativi ai big data individuando gli oggetti che si desidera elaborare per vari carichi di lavoro. Ad esempio, puoi interrogare la tabella di inventario attiva per trovare tutti gli oggetti archiviati in una particolare classe di archiviazione, tutti gli oggetti con determinati tag, tutti gli oggetti che non sono crittografati con la crittografia lato server tramite AWS Key Management Service (AWS KMS) keys () e altro ancora. SSE-KMS

Se si abilita la tabella di inventario in tempo reale per la configurazione della tabella dei metadati, la tabella viene sottoposta a un processo noto come riempimento, durante il quale Amazon S3 analizza il bucket per uso generico per recuperare i metadati iniziali per tutti gli oggetti presenti nel bucket. A seconda del numero di oggetti nel bucket, questo processo può richiedere da minuti (minimo 15 minuti) a ore. Al termine del processo di riempimento, lo stato della tabella di inventario in tempo reale passa da Riempimento in corso ad Attivo. Una volta completato il riempimento, gli aggiornamenti degli oggetti si riflettono in genere nella tabella di inventario in tempo reale entro un'ora.

Il riempimento della tabella di inventario viene addebitato. Se il bucket per uso generico contiene più di un miliardo di oggetti, verrà addebitata anche una tariffa mensile per la tabella di inventario in tempo reale. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Per ulteriori informazioni sui dati memorizzati nelle tabelle di inventario in tempo reale, consulta [the section called “Schema delle tabelle di inventario in tempo reale”](#).

- Tabella delle annotazioni: facoltativamente, puoi aggiungere una tabella delle annotazioni alla configurazione della tabella dei metadati. La tabella delle annotazioni tiene traccia delle annotazioni più recenti sugli oggetti nel bucket e rende il contenuto delle annotazioni direttamente interrogabile. Ogni riga rappresenta un'annotazione su una versione specifica dell'oggetto.

È possibile utilizzare la tabella delle annotazioni per scoprire e recuperare oggetti in base ai valori delle annotazioni. Ad esempio, è possibile interrogare la tabella delle annotazioni per trovare tutti gli oggetti con una chiave di annotazione specifica, recuperare il contenuto delle annotazioni che corrisponde a un predicato in base alla dimensione dell'oggetto o al prefisso della chiave o correlare le annotazioni tra oggetti.

Per ulteriori informazioni sulla configurazione della tabella di annotazione, vedere [the section called “Attivazione o disabilitazione delle tabelle di annotazione”](#). Per ulteriori informazioni sullo schema della tabella di annotazione, vedere [the section called “Schema della tabella di annotazione”](#).

Le tabelle di metadati sono archiviate in un bucket di tabelle S3 AWS gestito, che fornisce uno storage ottimizzato per i dati tabulari. Per interrogare i metadati, puoi integrare il tuo table bucket con Amazon Lakehouse. SageMaker Questa integrazione, che utilizza AWS Glue Data Catalog and AWS Lake Formation, consente ai servizi di AWS analisi di scoprire e accedere automaticamente ai dati delle tabelle.

Dopo aver integrato il table bucket con AWS Glue Data Catalog, puoi interrogare direttamente le tabelle di metadati con servizi di AWS analisi come Amazon Athena, Amazon EMR e Amazon Redshift. Puoi anche creare dashboard interattive con i dati delle tue query utilizzando Amazon Quick. Per ulteriori informazioni sull'integrazione del bucket di tabelle S3 AWS gestito con Amazon SageMaker Lakehouse, consulta [the section called “Integrazione delle tabelle S3 con AWS i servizi di analisi”](#).

Puoi anche interrogare le tue tabelle di metadati con e qualsiasi altra applicazione che supporti il Apache Iceberg formato utilizzando l'endpoint REST Apache SparkApache Trino, l'endpoint AWS Glue Iceberg REST di Amazon S3 Tables o il catalogo Amazon S3 Tables Iceberg Catalog for client. Apache Iceberg Per ulteriori informazioni sull'accesso alle tabelle dei metadati, consulta [the section called “Accesso alle tabelle”](#).

Per i prezzi di S3 Metadata, consulta [Prezzi di Amazon S3](#).

Come funzionano le tabelle di metadati

Le tabelle dei metadati sono gestite da Amazon S3 e non possono essere modificate da alcun principale IAM al di fuori di Amazon S3 stesso (è tuttavia possibile eliminare le tabelle dei metadati). Di conseguenza, le tabelle dei metadati sono di sola lettura, per garantire che riflettano correttamente il contenuto del bucket per uso generico.

Per generare e archiviare i metadati degli oggetti in tabelle di metadati AWS gestite, crei una configurazione della tabella di metadati per il tuo bucket generico. Amazon S3 è progettato per aggiornare continuamente la tabella dei metadati e riflettere le ultime modifiche ai dati, purché la configurazione sia attiva nel bucket per uso generico.

Per creare una configurazione di tabelle dei metadati, è necessario disporre delle autorizzazioni AWS Identity and Access Management (IAM) richieste per creare e gestire le tabelle dei metadati. Per ulteriori informazioni, consulta [the section called “Autorizzazioni per le tabelle di metadati”](#).

Archiviazione, organizzazione e crittografia delle tabelle dei metadati

Quando si crea la configurazione della tabella dei metadati, le tabelle dei metadati vengono archiviate in un bucket di tabelle gestito da AWS. Tutte le configurazioni delle tabelle di metadati nel tuo account e nella stessa regione vengono archiviate in un unico bucket di tabelle gestito. AWS. Questi bucket di tabelle AWS gestiti sono denominati `aws-s3` e hanno il seguente formato Amazon Resource Name (ARN):

```
arn:aws:s3tables:region:account_id:bucket/aws-s3
```

Ad esempio, se l'ID del tuo account è 123456789012 e il bucket per uso generico si trova negli Stati Uniti orientali (Virginia settentrionale) (`us-east-1`), il bucket di tabelle AWS gestito viene creato anche negli Stati Uniti orientali (Virginia settentrionale) () e ha il seguente ARN: `us-east-1`

```
arn:aws:s3tables:us-east-1:123456789012:bucket/aws-s3
```

Per impostazione predefinita, i bucket di tabelle AWS gestiti sono crittografati con crittografia lato server utilizzando chiavi gestite Amazon S3 (). SSE-S3. Dopo aver creato la prima configurazione dei metadati, puoi impostare l'impostazione di crittografia predefinita per il bucket di tabelle AWS gestite in modo che utilizzi la crittografia lato server con () keys (). AWS Key Management Service AWS KMS SSE-KMS. Per ulteriori informazioni, vedere [Crittografia per AWS i bucket di tabelle gestiti e. the section called “Specificando SSE-KMS”](#)

All'interno del bucket di tabelle AWS gestite, le tabelle di metadati per la configurazione sono in genere archiviate in uno spazio dei nomi con il seguente formato di denominazione:

b_*general-purpose-bucket-name*

Note

- Se il nome del bucket per uso generico contiene punti, questi vengono convertiti in caratteri di sottolineatura (_) nel nome del namespace.
- Se il bucket per uso generico è stato creato prima del 1° marzo 2018, il suo nome potrebbe contenere lettere maiuscole e caratteri di sottolineatura, inoltre potrebbe anche essere lungo fino a 255 caratteri. Se il nome del bucket presenta queste caratteristiche, il namespace di tabelle dei metadati avrà un formato diverso. Il nome del bucket per uso generico viene preceduto da b_, troncato a 63 caratteri, convertito in lettere minuscole e contrassegnato con il suffisso hash.

Le tabelle dei metadati hanno il seguente formato di nome della risorsa Amazon (ARN), che include l'ID della tabella dei metadati:

arn:aws:s3tables:*region-code*:*account-id*:bucket/aws-s3/table/*table-id*

Ad esempio, una tabella dei metadati nella Regione Stati Uniti orientali (Virginia settentrionale) avrebbe un ARN simile al seguente:

arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/
a12bc345-67d8-912e-3456-7f89123g4h56

Le tabelle del diario hanno il nome `journal` e le tabelle di inventario in tempo reale hanno il nome `inventory`.

Quando crei la configurazione della tabella dei metadati, puoi scegliere di crittografare le tabelle di metadati AWS gestite con la crittografia lato server utilizzando le chiavi () . AWS Key Management Service AWS KMS SSE-KMS Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket generico. È possibile impostare il tipo di crittografia per le tabelle solo durante la creazione della tabella. Dopo aver creato una tabella gestita da AWS , non è possibile modificarne le impostazioni di crittografia. SSE-KMS Per specificare le tabelle di metadati, devi disporre di determinate autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni per SSE-KMS](#)

L'impostazione di crittografia per una tabella dei metadati ha la precedenza sull'impostazione di crittografia predefinita a livello di bucket. Se non specifichi la crittografia, la tabella erediterà l'impostazione di crittografia predefinita del bucket.

AWS i bucket di tabelle gestiti non vengono conteggiati ai fini delle quote di S3 Tables. Per ulteriori informazioni sull'utilizzo dei bucket di tabelle AWS gestiti e delle tabelle gestite, vedi [Lavorare con AWS i bucket di tabelle AWS gestiti](#).

Per monitorare gli aggiornamenti della configurazione della tabella dei metadati, si può usare AWS CloudTrail. Per ulteriori informazioni, consulta [the section called “Azioni a livello di bucket di Amazon S3 tracciate mediante registrazione CloudTrail”](#).

Manutenzione della tabella dei metadati e scadenza dei record

Per far sì che le tabelle di metadati funzionino al meglio, Amazon S3 esegue attività di manutenzione periodica sulle tabelle, come la compattazione e la rimozione dei file non referenziati. Queste attività di manutenzione aiutano a minimizzare i costi di archiviazione delle tabelle di metadati e a ottimizzare le prestazioni delle query. La manutenzione della tabella avviene automaticamente, senza bisogno di opt-in o di una gestione continua da parte dell'utente.

Note

- Non è possibile controllare la scadenza degli snapshot della tabella del diario o della tabella di inventario. Per ogni tabella, Amazon S3 archivia almeno 1 snapshot per un massimo di 24 ore.
- Per ridurre al minimo i costi, puoi configurare la scadenza dei record della tabella del diario. Per impostazione predefinita, i record delle tabelle del diario non scadono e devono essere mantenuti per un minimo di 7 giorni. Per ulteriori informazioni, consulta [the section called “Scadenza dei record della tabella del diario”](#).

Argomenti

- [Limitazioni e restrizioni delle tabelle di metadati](#)
- [Schema delle tabelle del diario di S3 Metadata](#)
- [Schema delle tabelle di inventario in tempo reale di S3 Metadata](#)
- [Schema della tabella di annotazione dei metadati S3](#)

- [Configurazione delle tabelle di metadati](#)
- [Query di tabelle di metadati](#)
- [Risoluzione dei problemi relativi a S3 Metadata](#)

Limitazioni e restrizioni delle tabelle di metadati

Amazon S3 Metadata presenta le seguenti restrizioni e limitazioni:

- Al momento, S3 Metadata è disponibile solo in alcune Regioni. Per ulteriori informazioni, consulta [the section called “Metadati S3 Regioni AWS”](#).
- S3 Metadata supporta tutte le classi di archiviazione supportate dai bucket per uso generico. Per la classe di Intelligent-Tiering storage S3, il livello specifico non è mostrato nella tabella dei metadati.
- Quando crei la configurazione di una tabella dei metadati, le tabelle dei metadati vengono archiviate in un bucket di tabelle gestito da AWS . Non puoi archiviare la configurazione in un bucket di tabelle gestito dal cliente.
- S3 Metadata non è supportato per i bucket di directory o i bucket vettoriali. È possibile creare configurazioni di tabelle di metadati solo per i bucket per uso generico. La tabella del diario acquisisce i metadati solo per gli eventi di modifica (come caricamenti, aggiornamenti e cancellazioni) che si verificano dopo la creazione della configurazione della tabella dei metadati.
- Non è possibile controllare la scadenza degli snapshot della tabella del diario o della tabella di inventario. Per ogni tabella, Amazon S3 archivia almeno 1 snapshot per un massimo di 24 ore.

Per ridurre al minimo i costi, puoi configurare la scadenza dei record della tabella del diario. Per impostazione predefinita, i record delle tabelle del diario non scadono e devono essere mantenuti per un minimo di 7 giorni. Per ulteriori informazioni, consulta [the section called “Scadenza dei record della tabella del diario”](#).

- È possibile creare configurazioni di tabelle di metadati solo per interi bucket per uso generico. Non è possibile applicare una configurazione della tabella dei metadati a livello di prefisso.
- Non è possibile sospendere e riprendere gli aggiornamenti delle tabelle dei metadati. Tuttavia, è possibile eliminare la configurazione dei metadati associata per le tabelle del diario o di inventario in tempo reale. L'eliminazione della configurazione non elimina la tabella del diario o di inventario associata. Per ricreare la configurazione, è prima necessario eliminare la vecchia tabella del diario o di inventario, quindi Amazon S3 può creare una nuova tabella del diario o di inventario. Quando riabiliti la configurazione della tabella di inventario, Amazon S3 crea una nuova tabella di inventario e ti viene nuovamente addebitato il costo del riempimento della nuova tabella di inventario.

- Le tabelle dei metadati non contengono tutti gli stessi metadati disponibili tramite Inventario S3 o tramite la REST API di Amazon S3. Ad esempio, le seguenti informazioni non sono disponibili nelle tabelle dei metadati:
 - Stato di transizione o idoneità alla scadenza del ciclo di vita S3
 - Periodo di conservazione di Object Lock o modalità di governance
 - Informazioni sulle liste di controllo degli accessi (ACL) per gli oggetti
 - Stato della replica
- Quando si utilizza Amazon Athena o Amazon Redshift per eseguire query sulle tabelle dei metadati, è necessario racchiudere i nomi dei namespace di tabelle dei metadati tra virgolette (") o apici inversi (` `), altrimenti la query potrebbe non funzionare. Per alcuni esempi, consulta [the section called “Esempi di query di tabelle di metadati”](#).
- Quando si utilizza Apache Spark su Amazon EMR o altri motori di terze parti per eseguire query sulle tabelle dei metadati, è consigliabile utilizzare l'endpoint REST Iceberg di Tabelle Amazon S3. La query potrebbe non funzionare correttamente se non utilizzi questo endpoint. Per ulteriori informazioni, consulta [the section called “Accesso alle tabelle utilizzando l'endpoint Iceberg REST di Tabelle Amazon S3”](#).

S3 Metadata Regioni AWS

I metadati S3 sono attualmente disponibili nei seguenti formati: Regioni AWS

Regione AWS nome	Regione AWS codice
Africa (Città del Capo)	af-south-1
Asia Pacifico (Hong Kong)	ap-east-1
Asia Pacifico (Giacarta)	ap-southeast-3
Asia Pacifico (Melbourne)	ap-southeast-4
Asia Pacifico (Mumbai)	ap-south-1
Asia Pacifico (Osaka)	ap-northeast-3
Asia Pacifico (Seoul)	ap-northeast-2

Regione AWS nome	Regione AWS codice
Asia Pacifico (Singapore)	ap-southeast-1
Asia Pacifico (Sydney)	ap-southeast-2
Asia Pacifico (Tokyo)	ap-northeast-1
Canada (Centrale)	ca-central-1
Canada occidentale (Calgary)	ca-west-1
Europa (Francoforte)	eu-central-1
Europa (Zurigo)	eu-central-2
Europa (Irlanda)	eu-west-1
Europa (Londra)	eu-west-2
Europa (Milano)	eu-south-1
Europa (Parigi)	eu-west-3
Europa (Spagna)	eu-south-2
Europa (Stoccolma)	eu-north-1
Israele (Tel Aviv)	il-central-1
Medio Oriente (Bahrein)	me-south-1
Medio Oriente (Emirati Arabi Uniti)	me-central-1
Sud America (San Paolo)	sa-east-1
Stati Uniti orientali (Virginia settentrionale)	us-east-1
Stati Uniti orientali (Ohio)	us-east-2
Stati Uniti occidentali (California settentrionale)	us-west-1

Regione AWS nome	Regione AWS codice
Stati Uniti occidentali (Oregon)	us-west-2
Cina (Pechino)	cn-north-1
Cina (Ningxia)	cn-northwest-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1

Schema delle tabelle del diario di S3 Metadata

La tabella del diario registra le modifiche apportate ai dati pressoché in tempo reale, aiutando a individuare i nuovi dati caricati nel bucket, a tenere traccia degli oggetti eliminati di recente, a monitorare le transizioni del ciclo di vita e altro ancora. La tabella del diario registra i nuovi oggetti e gli aggiornamenti degli oggetti e dei relativi metadati (gli aggiornamenti che richiedono un'operazione PUT o un'operazione DELETE). Poiché questa tabella è sottoponibile a query, è possibile controllare le modifiche al bucket tramite semplici query SQL.

È possibile utilizzare la tabella del diario per i casi d'uso di sicurezza, controllo e conformità al fine di monitorare gli oggetti caricati, eliminati e modificati nel bucket. Ad esempio, puoi eseguire query sulla tabella del diario per rispondere a domande come le seguenti:

- Quali oggetti sono stati eliminati nelle ultime 24 ore dal ciclo di vita S3?
- Da quali indirizzi IP provengono le richieste PUT più recenti?
- Quali AWS Key Management Service (AWS KMS) chiavi sono state utilizzate per PUT le richieste negli ultimi 7 giorni?
- Quali oggetti del bucket sono stati creati da Amazon Bedrock negli ultimi cinque giorni?

Le tabelle del diario di Amazon S3 Metadata contengono righe e colonne. Ogni riga rappresenta un evento di mutazione che ha creato, aggiornato o eliminato un oggetto nel bucket per uso generico. La maggior parte di questi eventi sono il risultato di varie azioni dell'utente, ma alcuni di essi sono il risultato di azioni intraprese da Amazon S3 per conto dell'utente, come le scadenze del ciclo di vita S3 o le transizioni della classe di archiviazione.


```
customs -> Canada, family -> Billiards, filter -> true, location -> Europe, name -> Asia, user -> United States} 111122223333 192.0.2.1 CVK7Z6XQTQ90BSRV
```

Le tabelle del diario hanno il seguente schema:

Nome della colonna	Obbligatorio?	Tipo di dati	
bucket	Sì	Stringa	Il nome del bucket per uso generico. Per ulteriori informazioni, consulta the section called “Regole di denominazione” .
key	Sì	Stringa	Nome della chiave dell'oggetto (o della chiave) che identifica in modo univoco l'oggetto in un bucket. Per ulteriori informazioni, consulta the section called “Denominazione di oggetti” .
sequence_number	Sì	Stringa	Il numero di sequenza, che è un ordinale incluso nei record di un determinato oggetto. Per ordinare i record dello stesso bucket e della stessa chiave, è possibile ordinare su <code>sequence_number</code> . Per un determinato bucket e chiave, un valore

Nome della colonna	Obbligatorio?	Tipo di dati	
			sequence_number più grande a livello di lessicografia implica che il record è stato introdotto nel bucket più recentemente.

Nome della colonna	Obbligatorio?	Tipo di dati	
record_type	Sì	Stringa	<p>Il tipo di questo record, uno tra CREATEUPDATE_METADATA ,DELETE,CREATE_AND_DELETE_METADATA ,DELETE_AND_DELETE_METADATA , oUPDATE_AND_DELETE_METADATA .</p> <p>I record CREATE indicano che un nuovo oggetto (o una nuova versione dell'oggetto) è stato scritto nel bucket.</p> <p>I record UPDATE_METADATA acquisiscono le modifiche ai metadati mutevoli di un oggetto esistente , come la classe di storage o i tag.</p> <p>I record DELETE indicano che questo oggetto (o questa versione dell'oggetto) è stato cancellato. Quando il controllo delle versioni è abilitato, i record DELETE rappresentano un marcatore</p>

Nome della colonna	Obbligatorio?	Tipo di dati	
			<p>di cancellazione o una cancellazione permanente. Vengono ulteriormente chiarite consultando la colonna facoltativa <code>is_delete_marker</code>.</p> <p><code>CREATE_ANNOTATION</code> i record introducono una nuova annotazione su un oggetto o sovrascrivono un'annotazione esistente.</p> <p><code>DELETE_ANNOTATION</code> i record indicano che un'annotazione è stata eliminata.</p> <p><code>UPDATE_ANNOTATION_METADATA</code> i record acquisiscono le modifiche ai metadati modificabili per un'annotazione esistente, ad esempio quando cambia lo stato della replica.</p> <p>Per ulteriori informazioni, consulta the</p>

Nome della colonna	Obbligatorio?	Tipo di dati	
			<div><div><div><div>section called “Eliminazione di versioni di un oggetto”.</div></div></div><div><div><div><div>Note</div><div>Un’eliminazione permanent e riporta NULL in tutte le colonne, tranne bucket, key, sequence_number , record_type , record_timestamp e version_id (ovvero le colonne contrassegnate come richieste).</div></div></div></div></div>
record_timestamp	Sì	Timestamp NTZ (nessun fuso orario)	Il timestamp associato a questo record.

Nome della colonna	Obbligatorio?	Tipo di dati	
version_id	No	Stringa	<p>L'ID versione dell'oggetto. Quando viene attivata la funzione Controllo delle versioni in un bucket, Amazon S3 assegna un numero di versione agli oggetti aggiunti al bucket. Per ulteriori informazioni, consulta the section called “Conservazione più versioni degli oggetti”.</p> <p>Gli oggetti memorizzati nel bucket prima di impostare lo stato del controllo delle versioni hanno un ID versione pari a null.</p>

 **Note**

Le righe aggiunte per i marcatori di cancellazione hanno un valore `record_type` di `DELETE`, non `UPDATE_METADATA`. Se il marcatore

Nome della colonna	Obbligatorio?	Tipo di dati	
			<p>di cancellazione viene creato come risultato di una scadenza del ciclo di vita S3, il valore requester è <code>s3.amazonaws.com</code>.</p>
size	No	Long	<p>La dimensione dell'oggetto in byte, escluse le dimensioni dei caricamenti multipart e incompleti o dei metadati dell'oggetto. Se <code>is_delete_marker</code> è TRUE, la dimensione è 0. Per ulteriori informazioni, consulta the section called “System-defined metadati degli oggetti”.</p>

Nome della colonna	Obbligatorio?	Tipo di dati	
last_modified_date	No	Timestamp NTZ (nessun fuso orario)	Data di creazione dell'oggetto o data dell'ultima modifica, scegliendo la più recente delle due. Per i caricamenti multipart e, la data di creazione dell'oggetto è la data di avvio del caricamento multipart. Per ulteriori informazioni, consulta the section called “System-defined metadata degli oggetti” .

Nome della colonna	Obbligatorio?	Tipo di dati	
e_tag	No	Stringa	Il tag dell'entità (ETag), che è un hash dell'oggetto. L'ETag riflette solo i cambiamenti ai contenuti di un oggetto, non ai suoi metadati. Questo ETag può essere o meno un digest MD5 dei dati oggetto. Il fatto che l'ETag sia un digest MD5 dipende da come è stato creato l'oggetto e da come è stato crittografato. Per ulteriori informazioni, consulta Object nella documentazione di riferimento delle API di Amazon S3.

Nome della colonna	Obbligatorio?	Tipo di dati	
storage_class	No	Stringa	La classe di archiviazione utilizzata per archiviare l'oggetto. Uno tra STANDARD, REDUCED_REDUNDANCY, STANDARD_IA, ONEZONE_IA, INTELLIGENT_TIERING, GLACIER, DEEP_ARCHIVE o GLACIER_IR. Per ulteriori informazioni, consulta the section called “Comprensione e gestione delle classi di storage” .
is_multipart	No	Booleano	Il tipo di caricamento dell'oggetto. Se l'oggetto è stato caricato come caricamento multipart e, questo valore è TRUE. In caso contrario, è FALSE. Per ulteriori informazioni, consulta the section called “Utilizzo del caricamento in più parti” .

Nome della colonna	Obbligatorio?	Tipo di dati	
encryption_status	No	Stringa	Lo stato di crittografia lato server dell'oggetto, a seconda del tipo di chiave di crittografia utilizzata: crittografia lato server con chiavi gestite Amazon S3 (), crittografia lato server con (SSE-S3) chiavi (), crittografia lato server a doppio livello con AWS Key Management Service (AWS KMS SSE-KMS) o crittografia lato server con chiavi fornite dal cliente AWS KMS keys (DSSE-KMS). SSE-C Se l'oggetto non è crittografato, questo valore è null. I valori possibili sono SSE-S3, SSE-KMS, DSSE-KMS, SSE-C o null. Per ulteriori informazioni, consulta the section called “Crittografia dei dati” .

Nome della colonna	Obbligatorio?	Tipo di dati	
is_bucket_key_enabled	No	Booleano	Stato di abilitazione della chiave S3 Bucket dell'oggetto. Se l'oggetto utilizza una TRUE chiave S3 Bucket per, questo valore SSE-KMS è. In caso contrario, è FALSE. Per ulteriori informazioni, consulta the section called “Configurazione di una chiave bucket S3 per un oggetto” .

Nome della colonna	Obbligatorio?	Tipo di dati	
kms_key_arn	No	Stringa	<p>Il nome della risorsa Amazon (ARN) per la chiave KMS con cui l'oggetto è crittografato, per le righe in cui encryption_status è SSE-KMS o DSSE-KMS. Se l'oggetto non è crittografato con SSE-KMS o DSSE-KMS, il valore è nullo. Per ulteriori informazioni, consulta the section called “chiavi KMS memorizzate in AWS KMS () SSE-KMS” e the section called “Dual-layer crittografia lato server () DSSE-KMS”.</p> <div> Note<p>Se una riga rappresenta una versione dell'oggetto che non esisteva più al momento dell'elaborazione di un evento di cancellaz</p></div>

Nome della colonna	Obbligatorio?	Tipo di dati	
			ione o sovrascrittura, kms_key_a rn contiene un valore nullo, anche se il valore della colonna encryption_status è SSE-KMS o DSSE-KMS.
checksum_algorithm	No	Stringa	L'algoritmo utilizzato per creare il checksum per l'oggetto, uno tra,,CRC64NVME,,CRC32,CRC32C,SHA1,SHA256,SHA384,SHA512, o. SHA512 Se non è presente alcun checksum, questo valore è null. Per ulteriori informazioni, consulta the section called “Utilizzo di algoritmi di checksum supportati” .

Nome della colonna	Obbligatorio?	Tipo di dati	
object_tags	No	Mappa <String, String>	<p>I tag dell'oggetto che sono associati all'oggetto. I tag degli oggetti sono memorizzati come una mappa di coppie chiave-valore. Se un oggetto non ha tag oggetto, viene memorizzata una mappa vuota ({}). Per ulteriori informazioni, consulta the section called “Etichettare gli oggetti”.</p> <div><div> Note</div><div><p>Se il valore record_type è DELETE, la colonna object_tags contiene un valore nullo. Se il valore record_type è CREATE o UPDATE_METADATA , le righe che</p></div></div>

Nome della colonna	Obbligatorio?	Tipo di dati	
			<div>rappresen tano versioni di oggetti non più esistenti al momento dell'elab orazione di un evento di cancellaz ione o sovrascrittura conterrann o un valore nullo nella colonna object_ta gs .</div>

Nome della colonna	Obbligatorio?	Tipo di dati	
user_metadata	No	Mappa <String, String>	<p>I metadati utente che sono associati all'oggetto. I metadati utente sono memorizzati come una mappa di coppie chiave-valore. Se un oggetto non ha metadati utente, viene memorizzata una mappa vuota ({}).</p> <p>Per ulteriori informazioni, consulta the section called “User-defined metadati”.</p> <div><div> Note</div><div><p>Se il valore record_type è DELETE, la colonna user_metadata contiene un valore nullo. Se il valore record_type è CREATE o UPDATE_METADATA, le righe che rappresen</p></div></div>

Nome della colonna	Obbligatorio?	Tipo di dati	
			tano versioni di oggetti non più esistenti al momento dell'elaborazione di un evento di cancellazione o sovrascrittura conterranno un valore nullo nella colonna user_metadata .
requester	No	Stringa	L' Account AWS ID del richiedente o del Servizio AWS committente che ha effettuato la richiesta . Ad esempio, se il richiedente è il ciclo di vita S3, questo valore è s3.amazonaws.com .

Nome della colonna	Obbligatorio?	Tipo di dati	
source_ip_address	No	Stringa	L'indirizzo IP di origine della richiesta . Per i record generati da una richiesta dell'utente, questa colonna contiene l'indirizzo IP di origine della richiesta. Per le azioni intraprese da Amazon S3 o da un altro per Servizio AWS conto dell'utente, questa colonna contiene un valore nullo.
request_id	No	Stringa	ID richiesta associato alla richiesta.
object_join_key	No	Stringa	Un identificatore univoco per questo oggetto, assegnato con ogni nuova versione o quando la versione nulla viene creata o sovrascritta. Usa questa colonna per unirti alla tabella delle annotazioni.

Nome della colonna	Obbligatorio?	Tipo di dati	
<code>annotation.name</code>	No	Stringa	Il nome dell'annotazione da modificare. Presente solo per <code>CREATE_ANNOTATION</code> , <code>UPDATE_ANNOTATION_METADATA</code> e tipi di <code>DELETE_ANNOTATION</code> record e.
<code>annotation.sequence_number</code>	No	Stringa	Un valore ordinale per l'ordinamento delle revisioni delle annotazioni.
<code>annotation.last_modified_date</code>	No	Time stamp	La data e l'ora dell'ultima modifica dell'annotazione.
<code>annotation.size</code>	No	Long	La dimensione del payload dell'annotazione in byte.
<code>annotation.e_tag</code>	No	Stringa	L'ETag del contenuto dell'annotazione.

Nome della colonna	Obbligatorio?	Tipo di dati	
annotation.replication_status	No	Stringa	Lo stato di replica dell'annotazione. PENDING e FAILED sono visibili solo all'origine della replica. COMPLETED REPLICATION sono visibili solo nella destinazione della replica. Se non esiste una configurazione di replica applicabile, questo valore è. NULL
annotation.checksum_algorithm	No	Stringa	L'algoritmo di checksum utilizzato per l'annotazione.

Schema delle tabelle di inventario in tempo reale di S3 Metadata

La tabella di inventario in tempo reale fornisce un inventario semplice e sottoponibile a query di tutti gli oggetti e delle relative versioni presenti nel bucket in modo da poter determinare lo stato più recente dei dati. Gli aggiornamenti degli oggetti si riflettono in genere nella tabella di inventario in tempo reale entro un'ora.

È possibile utilizzare questa tabella per semplificare e velocizzare i flussi di lavoro aziendali e i processi relativi ai big data individuando gli oggetti che si desidera elaborare per vari carichi di lavoro. Ad esempio, puoi eseguire query sulla tabella di inventario in tempo reale per effettuare le seguenti operazioni:

- Trovare tutti gli oggetti archiviati nella classe di archiviazione S3 Glacier Deep Archive.
- Creare una distribuzione di tag di oggetto o trovare oggetti senza tag.
- Trova tutti gli oggetti non crittografati utilizzando la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (). SSE-KMS

Se si abilita la tabella di inventario per la configurazione della tabella dei metadati, la tabella viene sottoposta a un processo noto come riempimento, durante il quale Amazon S3 analizza il bucket per uso generico per recuperare i metadati iniziali per tutti gli oggetti presenti nel bucket. A seconda del numero di oggetti nel bucket, questo processo può richiedere da minuti (minimo 15 minuti) a ore. Al termine del processo di riempimento, lo stato della tabella di inventario passa da Riempimento in corso ad Attivo. Una volta completato il riempimento, gli aggiornamenti degli oggetti si riflettono in genere nella tabella di inventario entro un'ora.

 Note

Il riempimento della tabella di inventario viene addebitato. Se il bucket per uso generico contiene più di un miliardo di oggetti, verrà addebitata anche una tariffa mensile per la tabella di inventario. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Le tabelle di inventario di Amazon S3 Metadata contengono righe e colonne. Ogni riga rappresenta lo stato corrente di un oggetto presente nel bucket per uso generico. La tabella di inventario in tempo reale fornisce un inventario semplice e sottoponibile a query di tutti gli oggetti presenti nel bucket in modo da poter determinare lo stato corrente dei dati.

Di seguito è riportato un esempio di tabella di inventario per un bucket per uso generico denominato `amzn-s3-demo-bucket`:

[illegible]

[illegible]

Le tabelle di inventario hanno il seguente schema:

Nome della colonna	Obbligatorio?	Tipo di dati	
bucket	Sì	Stringa	Il nome del bucket per uso generico. Per ulteriori informazioni, consulta the section called “Regole di denominazione” .
key	Sì	Stringa	Nome della chiave dell'oggetto (o della chiave) che identifica in modo univoco l'oggetto in un bucket. Per ulteriori informazioni, consulta the section called “Denominazione di oggetti” .
sequence_number	Sì	Stringa	Il numero di sequenza, che è un ordinale incluso nei record di un determinato oggetto. Per ordinare i record

Nome della colonna	Obbligatorio?	Tipo di dati	
			dello stesso bucket e della stessa chiave, è possibile ordinare su <code>sequence_number</code> . Per un determinato bucket e chiave, un valore <code>sequence_number</code> più grande a livello di lessicografia implica che il record è stato introdotto nel bucket più recentemente.
<code>object_join_key</code>	No	Stringa	Un identificatore univoco per l'oggetto , assegnato con ogni nuova versione o quando viene creata o sovrascritta la versione nulla. Usa questa colonna per unirti alla tabella delle annotazioni.

Nome della colonna	Obbligatorio?	Tipo di dati	
version_id	No	Stringa	<p>L'ID versione dell'oggetto. Quando viene attivata la funzione Controllo delle versioni in un bucket, Amazon S3 assegna un numero di versione agli oggetti aggiunti al bucket. Per ulteriori informazioni, consulta the section called “Conservazione più versioni degli oggetti”.</p> <p>Gli oggetti memorizzati nel bucket prima di impostare lo stato del controllo delle versioni hanno un ID versione pari a null.</p>

Nome della colonna	Obbligatorio?	Tipo di dati	
is_delete _marker	No	Booleano	<p>Stato del marcatore di cancellazione dell'oggetto. Se l'oggetto è un marcatore di cancellazione, questo valore è True. In caso contrario, è False. Per ulteriori informazioni, consulta the section called “Utilizzo dei contrassegni di eliminazione”.</p> <div><div> Note</div><p>Le righe aggiunte per i marcatori di cancellazione hanno un valore record_type di DELETE, non UPDATE_METADATA. Se il marcatore di cancellazione viene creato come risultato di una scadenza del ciclo di vita S3,</p></div>

Nome della colonna	Obbligatorio?	Tipo di dati	
			il valore requester è s3.amazonaws.com .
size	No	Long	La dimensione dell'oggetto in byte, escluse le dimensioni dei caricamenti multipart e incompleti o dei metadati dell'oggetto. Se is_delete_marker è True, la dimensione è 0. Per ulteriori informazioni, consulta the section called “System-defined metadati degli oggetti” .

Nome della colonna	Obbligatorio?	Tipo di dati	
last_modified_date	No	Timestamp NTZ (nessun fuso orario)	Data di creazione dell'oggetto o data dell'ultima modifica, scegliendo la più recente delle due. Per i caricamenti multipart e, la data di creazione dell'oggetto è la data di avvio del caricamento multipart. Per ulteriori informazioni, consulta the section called “System-defined metadata degli oggetti” .

Nome della colonna	Obbligatorio?	Tipo di dati	
e_tag	No	Stringa	Il tag dell'entità (ETag), che è un hash dell'oggetto. L'ETag riflette solo i cambiamenti ai contenuti di un oggetto, non ai suoi metadati. Questo ETag può essere o meno un digest MD5 dei dati oggetto. Il fatto che l'ETag sia un digest MD5 dipende da come è stato creato l'oggetto e da come è stato crittografato. Per ulteriori informazioni, consulta Object nella documentazione di riferimento delle API di Amazon S3.

Nome della colonna	Obbligatorio?	Tipo di dati	
storage_class	No	Stringa	La classe di archiviazione utilizzata per archiviare l'oggetto. Uno tra STANDARD, REDUCED_REDUNDANCY, STANDARD_IA, ONEZONE_IA, INTELLIGENT_TIERING, GLACIER, DEEP_ARCHIVE o GLACIER_IR. Per ulteriori informazioni, consulta the section called “Comprensione e gestione delle classi di storage” .
is_multipart	No	Booleano	Il tipo di caricamento dell'oggetto. Se l'oggetto è stato caricato come caricamento multipart e, questo valore è True. In caso contrario, è False. Per ulteriori informazioni, consulta the section called “Utilizzo del caricamento in più parti” .

Nome della colonna	Obbligatorio?	Tipo di dati	
encryption_status	No	Stringa	<p>Lo stato di crittografia lato server dell'oggetto, a seconda del tipo di chiave di crittografia utilizzata: crittografia lato server con chiavi gestite Amazon S3 (), crittografia lato server con (SSE-S3) chiavi (), crittografia lato server a doppio livello con AWS Key Management Service (AWS KMS SSE-KMS) o crittografia lato server con chiavi fornite dal cliente AWS KMS keys (DSSE-KMS). SSE-C</p> <p>Se l'oggetto non è crittografato, questo valore è null. I valori possibili sono SSE-S3, SSE-KMS, DSSE-KMS, SSE-C o null.</p> <p>Per ulteriori informazioni, consulta the section called “Crittografia dei dati”.</p>

Nome della colonna	Obbligatorio?	Tipo di dati	
is_bucket_key_enabled	No	Booleano	Stato di abilitazione della chiave S3 Bucket dell'oggetto. Se l'oggetto utilizza una <code>True</code> chiave S3 Bucket per, questo valore SSE-KMS è. In caso contrario, è <code>False</code> . Per ulteriori informazioni, consulta the section called “Configurazione di una chiave bucket S3 per un oggetto” .

Nome della colonna	Obbligatorio?	Tipo di dati	
kms_key_arn	No	Stringa	<p>Il nome della risorsa Amazon (ARN) per la chiave KMS con cui l'oggetto è crittografato, per le righe in cui encryption_status è SSE-KMS o DSSE-KMS. Se l'oggetto non è crittografato con SSE-KMS o DSSE-KMS, il valore è nullo. Per ulteriori informazioni, consulta the section called “chiavi KMS memorizzate in AWS KMS () SSE-KMS” e the section called “Dual-layer crittografia lato server () DSSE-KMS”.</p> <div> Note<p>Se una riga rappresenta una versione dell'oggetto che non esisteva più al momento dell'elaborazione di un evento di cancellaz</p></div>

Nome della colonna	Obbligatorio?	Tipo di dati	
			ione o sovrascrittura, kms_key_a rn contiene un valore nullo, anche se il valore della colonna encryption_status è SSE-KMS o DSSE-KMS.
checksum_algorithm	No	Stringa	L'algoritmo utilizzato per creare il checksum per l'oggetto, uno tra,,CRC64-NVM E ,,CRC32,CRC32C,SHA1,SHA256,SHA384,SHA512, o. SHA512 Se non è presente alcun checksum, questo valore è null. Per ulteriori informazioni, consulta the section called “Utilizzo di algoritmi di checksum supportati” .

Nome della colonna	Obbligatorio?	Tipo di dati	
object_tags	No	Mappa <String, String>	<p>I tag dell'oggetto che sono associati all'oggetto. I tag degli oggetti sono memorizzati come una mappa di coppie chiave-valore. Se un oggetto non ha tag oggetto, viene memorizzata una mappa vuota ({}). Per ulteriori informazioni, consulta the section called “Etichettare gli oggetti”.</p> <div><div> Note</div><div><p>Se il valore record_type è DELETE, la colonna object_tags contiene un valore nullo. Se il valore record_type è CREATE o UPDATE_METADATA , le righe che</p></div></div>

Nome della colonna	Obbligatorio?	Tipo di dati	
			<div>rappresen tano versioni di oggetti non più esistenti al momento dell'elab orazione di un evento di cancellaz ione o sovrascrittura conterrann o un valore nullo nella colonna object_ta gs .</div>

Nome della colonna	Obbligatorio?	Tipo di dati	
user_metadata	No	Mappa <String, String>	<p>I metadati utente che sono associati all'oggetto. I metadati utente sono memorizzati come una mappa di coppie chiave-valore. Se un oggetto non ha metadati utente, viene memorizzata una mappa vuota ({}).</p> <p>Per ulteriori informazioni, consulta the section called “User-defined metadati”.</p> <div><div> Note</div><div><p>Se il valore record_type è DELETE, la colonna user_metadata contiene un valore nullo. Se il valore record_type è CREATE o UPDATE_METADATA , le righe che rappresen</p></div></div>

Nome della colonna	Obbligatorio?	Tipo di dati	
			tano versioni di oggetti non più esistenti al momento dell'elaborazione di un evento di cancellazione o sovrascrittura conterranno un valore nullo nella colonna <code>user_metadata</code> .

Schema della tabella di annotazione dei metadati S3

La tabella delle annotazioni tiene traccia delle annotazioni più recenti sugli oggetti nel bucket generico. Ogni riga rappresenta un'annotazione su una versione specifica dell'oggetto. È possibile utilizzare la tabella delle annotazioni per scoprire e recuperare oggetti in base al contenuto delle annotazioni. Ad esempio, è possibile interrogare la tabella delle annotazioni per trovare tutti gli oggetti con un'annotazione specifica, recuperare il contenuto delle annotazioni che corrisponde a un predicato in base alla dimensione dell'oggetto o al prefisso della chiave o correlare le annotazioni tra oggetti.

Quando abiliti la tabella di annotazione per la configurazione della tabella dei metadati, la tabella viene sottoposta a un processo noto come `backfill`, durante il quale Amazon S3 esegue la scansione del bucket generico per recuperare i dati di annotazione per tutti gli oggetti. A seconda del numero di oggetti nel bucket, questo processo può richiedere da minuti a ore. Al termine del riempimento, lo stato cambia da `Backfill` a `Attivo`.

 Note

Ti verrà addebitato il costo del riempimento della tabella delle annotazioni. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Le tabelle di annotazione hanno lo schema seguente:

Nome della colonna	Obbligatorio?	Tipo di dati	Description
bucket	Sì	Stringa	Il nome del secchio per uso generico.
object_key	Sì	Stringa	Nome della chiave dell'oggetto (o della chiave) che identifica in modo univoco l'oggetto in un bucket.
object_version_id	No	Stringa	L'ID versione dell'oggetto.
object_join_key	Sì	Stringa	Un identificatore univoco per l'oggetto , assegnato con ogni nuova versione o quando viene creata o sovrascritta la versione nulla. Usa questa colonna per unirti alle tabelle dell'inventario o del giornale.
name	Sì	Stringa	Il nome dell'annotazione.

Nome della colonna	Obbligatorio?	Tipo di dati	Description
sequence_number	Sì	Stringa	Un valore ordinale per l'ordinamento delle revisioni delle annotazioni. Per un dato bucket, e object_key y object_version_id , un valore lessicograficamente più grande implica che il record è stato introdotto più sequence_number recentemente.
last_modified_date	No	Timestamp NTZ (nessun fuso orario)	La data e l'ora dell'ultima modifica dell'annotazione.
size	No	Long	La dimensione del payload dell'annotazione in byte.
e_tag	No	Stringa	L'ETag del contenuto dell'annotazione.
checksum_algorithm	No	Stringa	L'algoritmo di checksum utilizzato per l'annotazione. Se non è presente alcun checksum, questo valore è null.

Nome della colonna	Obbligatorio?	Tipo di dati	Description
<code>replication_status</code>	No	Stringa	Lo stato di replica dell'annotazione. PENDING e FAILED sono visibili solo all'origine della replica. COMPLETED REPLICATION sono visibili solo nella destinazione della replica. Se non esiste una configurazione di replica applicabile, questo valore è nullo.
<code>text_value</code>	No	Stringa	Il contenuto dell'annotazione (testo) UTF-8.

Configurazione delle tabelle di metadati

Amazon S3 Metadata accelera il reperimento dei dati acquisendo automaticamente i metadati per gli oggetti nei bucket per uso generico e memorizzandoli in tabelle Apache Iceberg di sola lettura e completamente gestite che possono essere interrogate. Queste tabelle di sola lettura sono chiamate tabelle di metadati. Quando gli oggetti vengono aggiunti, aggiornati e rimossi dai bucket per uso generico, S3 Metadata aggiorna automaticamente le tabelle di metadati corrispondenti per riflettere le ultime modifiche.

Con S3 Metadata, puoi trovare, archiviare e interrogare facilmente i metadati per i tuoi oggetti S3, in modo da poter preparare rapidamente i dati da utilizzare nell'analisi aziendale, nella formazione sui modelli di intelligenza artificiale e machine learning () e altro ancora. AI/ML

Per generare e archiviare i metadati degli oggetti in tabelle di metadati AWS gestite, crei una configurazione della tabella di metadati per il tuo bucket generico. Amazon S3 è progettato per aggiornare continuamente la tabella dei metadati e riflettere le ultime modifiche ai dati, purché la configurazione sia attiva nel bucket. Inoltre, Amazon S3 ottimizza continuamente le tabelle di metadati per ridurre i costi di archiviazione e migliorare le prestazioni delle query di analisi.

Per creare una configurazione di tabelle di metadati, assicurati di disporre delle autorizzazioni AWS Identity and Access Management (IAM) necessarie per creare e gestire le tabelle di metadati.

Per monitorare gli aggiornamenti della configurazione della tabella dei metadati, si può usare AWS CloudTrail. Per ulteriori informazioni, consulta [the section called “Azioni a livello di bucket di Amazon S3 tracciate mediante registrazione CloudTrail”](#).

Argomenti

- [Impostazione delle autorizzazioni per la configurazione delle tabelle di metadati](#)
- [Creazione di configurazioni delle tabelle di metadati](#)
- [Controllo dell'accesso alle tabelle di metadati](#)
- [Scadenza dei record della tabella del diario](#)
- [Abilitazione o disabilitazione delle tabelle di inventario in tempo reale](#)
- [Abilitazione o disabilitazione delle tabelle di annotazione](#)
- [Visualizzazione delle configurazioni delle tabelle dei metadati](#)
- [Cancellazione di configurazioni delle tabelle di metadati](#)
- [Cancellazione di tabelle di metadati](#)

Impostazione delle autorizzazioni per la configurazione delle tabelle di metadati

Per creare una configurazione della tabella di metadati, devi disporre delle autorizzazioni AWS Identity and Access Management (IAM) necessarie sia per creare e gestire la configurazione della tabella di metadati sia per creare e gestire le tabelle di metadati e il bucket di tabelle in cui sono archiviate le tabelle di metadati.

Per creare e gestire la configurazione delle tabelle di metadati, è necessario disporre di queste autorizzazioni:

- `s3:CreateBucketMetadataTableConfiguration` - Questa autorizzazione consente di creare una configurazione della tabella dei metadati per il bucket per uso generico. Per creare una configurazione della tabella dei metadati, sono necessarie autorizzazioni aggiuntive, incluse le autorizzazioni di Tabelle S3, come spiegato nelle sezioni successive. Per un riepilogo delle autorizzazioni richieste, consulta [the section called “Operazioni e autorizzazioni del bucket”](#).
- `s3:GetBucketMetadataTableConfiguration` - Questa autorizzazione consente di recuperare informazioni sulla configurazione della tabella dei metadati.

- `s3:DeleteBucketMetadataTableConfiguration` - Questa autorizzazione consente di eliminare la configurazione della tabella di metadati.
- `s3:UpdateBucketMetadataJournalTableConfiguration` - Questa autorizzazione consente di aggiornare la configurazione della tabella del diario con la scadenza dei record della tabella del diario.
- `s3:UpdateBucketMetadataInventoryTableConfiguration` - Questa autorizzazione consente di aggiornare la configurazione della tabella di inventario per abilitare o disabilitare la tabella di inventario. Per aggiornare la configurazione di una tabella di inventario, sono necessarie autorizzazioni aggiuntive, incluse le autorizzazioni di Tabelle S3. Per un elenco delle autorizzazioni richieste, consulta [the section called "Operazioni e autorizzazioni del bucket"](#).
- `s3:UpdateBucketMetadataAnnotationTableConfiguration`— Questa autorizzazione consente di aggiornare la configurazione della tabella di annotazione per abilitare o disabilitare la tabella di annotazione. Per aggiornare la configurazione di una tabella di annotazione, sono necessarie autorizzazioni aggiuntive, incluse le autorizzazioni per le tabelle S3. Per un elenco delle autorizzazioni richieste, consulta [the section called "Operazioni e autorizzazioni del bucket"](#).

 Note

Le autorizzazioni `s3:CreateBucketMetadataTableConfiguration`, `s3:GetBucketMetadataTableConfiguration` e `s3:DeleteBucketMetadataTableConfiguration` vengono utilizzate per le configurazioni di S3 Metadata V1 e V2. Per V2, i nomi delle operazioni API corrispondenti sono `CreateBucketMetadataConfiguration`, `GetBucketMetadataConfiguration` e `DeleteBucketMetadataConfiguration`.

- `iam:PassRole`— Per creare una configurazione di metadati di Amazon S3 che includa una tabella di annotazioni, è necessaria questa autorizzazione per passare il ruolo IAM della tabella di annotazione. Aggiungi la seguente dichiarazione alla policy IAM del chiamante:

```
{
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::123456789012:role/annotation-table-role",
  "Condition": {"StringEquals": {"iam:PassedToService":
    "metadata.s3.amazonaws.com"}}
}
```

Per creare e lavorare con le tabelle e i bucket di tabelle, è necessario disporre di determinate autorizzazioni `s3tables`. Come minimo, per creare la configurazione di una tabella di metadati, è necessario disporre delle seguenti autorizzazioni `s3tables`:

- `s3tables:CreateTableBucket` - Questa autorizzazione consente di creare un bucket di tabella gestito da AWS. Tutte le configurazioni delle tabelle di metadati nel tuo account e nella stessa regione sono archiviate in un unico bucket di tabelle AWS gestito denominato `aws-s3`. Per ulteriori informazioni, consulta [the section called “Come funzionano le tabelle di metadati”](#) e [Utilizzo dei bucket di tabelle gestiti AWS](#).
- `s3tables:CreateNamespace` - Questa autorizzazione consente di creare uno spazio dei nomi in un bucket di tabella. Le tabelle dei metadati utilizzano in genere il namespace `b_general_purpose_bucket_name`. Per ulteriori informazioni sui namespace di tabelle dei metadati, consulta [the section called “Come funzionano le tabelle di metadati”](#).
- `s3tables:CreateTable` - Questa autorizzazione consente di creare le tabelle dei metadati.
- `s3tables:GetTable` - Questa autorizzazione consente di recuperare informazioni sulle tabelle dei metadati.
- `s3tables:PutTablePolicy` - Questa autorizzazione consente di aggiungere o aggiornare le policy delle tabelle dei metadati.
- `s3tables:PutTableEncryption` - Questa autorizzazione consente di impostare la crittografia lato server per le tabelle dei metadati. Sono necessarie autorizzazioni aggiuntive se desideri crittografare le tabelle di metadati con la crittografia lato server con chiavi (`()`). AWS Key Management Service AWS KMS SSE-KMS Per ulteriori informazioni, consulta [Autorizzazioni per SSE-KMS](#).
- `kms:DescribeKey` - Questa autorizzazione consente di recuperare informazioni su una chiave KMS.
- `s3tables:PutTableBucketPolicy`— Questa autorizzazione consente di creare o aggiornare una nuova policy del bucket della tabella.

Per informazioni dettagliate su tutte le autorizzazioni per le tabelle e i bucket delle tabelle, consulta [Gestione degli accessi per le tabelle S3](#).

⚠ Important

Se desideri integrare il tuo table bucket anche con i servizi di AWS analisi in modo da poter interrogare la tabella dei metadati, hai bisogno di autorizzazioni aggiuntive. Per ulteriori informazioni, consulta [Integrazione delle tabelle Amazon S3 con i servizi di analisi. AWS](#)

Autorizzazioni per SSE-KMS

Per crittografare le tabelle di metadati con la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS), devi disporre di autorizzazioni aggiuntive.

1. L'utente o il ruolo AWS Identity and Access Management (IAM) necessita delle seguenti autorizzazioni. Puoi concedere queste autorizzazioni utilizzando la console IAM: <https://console.aws.amazon.com/iam/>
 - a. `s3tables:PutTableEncryption` per configurare la crittografia delle tabelle
 - b. `kms:DescribeKeys` sulla AWS KMS chiave utilizzata
2. Per la policy delle risorse per la chiave KMS, sono necessarie le seguenti autorizzazioni. Puoi concedere queste autorizzazioni utilizzando la AWS KMS console: <https://console.aws.amazon.com/kms>.
 - a. Autorizzazione `kms:GenerateDataKey` a `metadata.s3.amazonaws.com` e `maintenance.s3tables.amazonaws.com`.
 - b. Autorizzazione `kms:Decrypt` a `metadata.s3.amazonaws.com` e `maintenance.s3tables.amazonaws.com`.
 - c. Concedi `kms:DescribeKey` il permesso al preponente che richiama. AWS

Oltre a queste autorizzazioni, è necessario che la chiave KMS gestita dal cliente utilizzata per crittografare le tabelle esista ancora, sia attiva e si trovi nella stessa Regione del bucket per uso generico.

Policy di esempio

Per creare e lavorare con le tabelle di metadati e i bucket di tabelle, si può utilizzare il seguente esempio di policy. In questa policy, il bucket per uso generico a cui si applica la configurazione della tabella dei metadati è indicato come *amzn-s3-demo-bucket*. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

Quando si crea la configurazione della tabella dei metadati, le tabelle dei metadati vengono archiviate in un bucket di tabelle gestito da AWS . Tutte le configurazioni delle tabelle di metadati nel tuo account e nella stessa regione sono archiviate in un unico bucket di tabelle AWS gestito denominato. `aws-s3`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermissionsToWorkWithMetadataTables",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucketMetadataTableConfiguration",
        "s3:GetBucketMetadataTableConfiguration",
        "s3>DeleteBucketMetadataTableConfiguration",
        "s3:UpdateBucketMetadataJournalTableConfiguration",
        "s3:UpdateBucketMetadataInventoryTableConfiguration",
        "s3:UpdateBucketMetadataAnnotationTableConfiguration",
        "s3tables:*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/*",
        "arn:aws:kms:Region:Account:key/KmsKeyId"
      ]
    }
  ]
}
```

Per eseguire query sulle tabelle dei metadati, è possibile utilizzare la seguente policy di esempio. Se le tabelle dei metadati sono state crittografate con SSE-KMS, avrai bisogno dell'autorizzazione come mostrato. `kms:Decrypt` Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermissionsToQueryMetadataTables",
      "Effect": "Allow",
```

```

    "Action": [
        "s3tables:GetTable",
        "s3tables:GetTableData",
        "s3tables:GetTableMetadataLocation",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/*",
        "arn:aws:kms:Region:Account:key/KmsKeyId"
    ]
}

```

Creazione di configurazioni delle tabelle di metadati

Per generare e archiviare i metadati Amazon S3 in una tabella dei metadati Apache Iceberg completamente gestita, si crea una configurazione della tabella dei metadati per il bucket per uso generico. Amazon S3 è progettato per aggiornare continuamente la tabella dei metadati e riflettere le ultime modifiche ai dati, purché la configurazione sia attiva nel bucket. Inoltre, Amazon S3 ottimizza continuamente le tabelle di metadati per ridurre i costi di archiviazione e migliorare le prestazioni delle query di analisi.

Per ogni bucket per uso generico, è possibile creare una configurazione della tabella delle annotazioni che contiene fino a tre tabelle di metadati complementari:

- **Tabella del diario:** per impostazione predefinita, la configurazione della tabella dei metadati contiene una tabella del diario, che acquisisce gli eventi che si verificano per gli oggetti nel bucket. La tabella del diario registra le modifiche apportate ai dati pressoché in tempo reale, aiutando a individuare i nuovi dati caricati nel bucket, a tenere traccia degli oggetti eliminati di recente, a monitorare le transizioni del ciclo di vita e altro ancora. La tabella del diario registra i nuovi oggetti e gli aggiornamenti degli oggetti e dei relativi metadati (gli aggiornamenti che richiedono un'operazione PUT o un'operazione DELETE).

La tabella del diario acquisisce i metadati solo per gli eventi di modifica (come caricamenti, aggiornamenti ed eliminazioni) che si verificano dopo la creazione della configurazione della tabella dei metadati. Poiché questa tabella è sottoponibile a query, è possibile controllare le modifiche al bucket tramite semplici query SQL.

La tabella del diario è obbligatoria per ogni configurazione della tabella dei metadati. Nella versione iniziale di S3 Metadata, la tabella del diario era denominata “tabella dei metadati”.

Per ulteriori informazioni sui dati archiviati nelle tabelle del diario, consulta [the section called “Schema delle tabelle del diario”](#).

Per ridurre al minimo i costi di archiviazione, è possibile scegliere la scadenza dei record della tabella del diario. Per ulteriori informazioni, consulta [the section called “Scadenza dei record della tabella del diario”](#).

- Tabella di inventario in tempo reale: facoltativamente, è possibile aggiungere una tabella di inventario in tempo reale alla configurazione della tabella dei metadati. La tabella di inventario in tempo reale fornisce un inventario semplice e sottoponibile a query di tutti gli oggetti e delle relative versioni presenti nel bucket in modo da poter determinare lo stato più recente dei dati.

È possibile utilizzare la tabella di inventario in tempo reale per semplificare e velocizzare i flussi di lavoro aziendali e i processi relativi ai big data individuando gli oggetti che si desidera elaborare per vari carichi di lavoro. Ad esempio, puoi interrogare la tabella di inventario attiva per trovare tutti gli oggetti archiviati in una particolare classe di archiviazione, tutti gli oggetti con determinati tag, tutti gli oggetti che non sono crittografati con la crittografia lato server tramite AWS Key Management Service (AWS KMS) keys (SSE-KMS) e altro ancora.

Se si abilita la tabella di inventario in tempo reale per la configurazione della tabella dei metadati, la tabella viene sottoposta a un processo noto come riempimento, durante il quale Amazon S3 analizza il bucket per uso generico per recuperare i metadati iniziali per tutti gli oggetti presenti nel bucket. A seconda del numero di oggetti nel bucket, questo processo può richiedere da minuti (minimo 15 minuti) a ore. Al termine del processo di riempimento, lo stato della tabella di inventario in tempo reale passa da Riempimento in corso ad Attivo. Una volta completato il riempimento, gli aggiornamenti degli oggetti si riflettono in genere nella tabella di inventario in tempo reale entro un'ora.

Il riempimento della tabella di inventario in tempo reale viene addebitato. Se il bucket per uso generico contiene più di un miliardo di oggetti, verrà addebitata anche una tariffa mensile per la tabella di inventario in tempo reale. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Per ulteriori informazioni sui dati memorizzati nelle tabelle di inventario in tempo reale, consulta [the section called “Schema delle tabelle di inventario in tempo reale”](#).

- Tabella delle annotazioni: facoltativamente, puoi aggiungere una tabella delle annotazioni alla configurazione della tabella dei metadati. La tabella delle annotazioni tiene traccia delle annotazioni più recenti sugli oggetti nel bucket e rende il contenuto delle annotazioni direttamente interrogabile. La tabella delle annotazioni non è abilitata per impostazione predefinita. Per ulteriori informazioni, consulta [the section called “Attivazione o disabilitazione delle tabelle di annotazione”](#).

Le tabelle dei metadati hanno il seguente formato di nome della risorsa Amazon (ARN), che include l'ID della tabella dei metadati:

```
arn:aws:s3tables:region-code:account-id:bucket/aws-s3/table/table-id
```

Ad esempio, una tabella dei metadati nella Regione Stati Uniti orientali (Virginia settentrionale) avrebbe un ARN simile al seguente:

```
arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/
a12bc345-67d8-912e-3456-7f89123g4h56
```

Le tabelle del diario hanno il nome `journal`, le tabelle di inventario attive hanno il nome `inventory` e le tabelle di annotazione hanno il nome `annotation`.

Quando si crea la configurazione della tabella dei metadati, le tabelle dei metadati vengono archiviate in un bucket di tabelle gestito da AWS. Tutte le configurazioni delle tabelle di metadati nel tuo account e nella stessa regione vengono archiviate in un unico AWS bucket di tabelle gestito. Questi bucket di tabelle AWS gestiti sono denominati `aws-s3` e hanno il seguente formato Amazon Resource Name (ARN):

```
arn:aws:s3tables:region:account_id:bucket/aws-s3
```

Ad esempio, se l'ID del tuo account è 123456789012 e il bucket per uso generico si trova negli Stati Uniti orientali (Virginia settentrionale) (`us-east-1`), il bucket di tabelle AWS gestito viene creato anche negli Stati Uniti orientali (Virginia settentrionale) () e ha il seguente ARN: `us-east-1`

```
arn:aws:s3tables:us-east-1:123456789012:bucket/aws-s3
```

Per impostazione predefinita, i bucket di tabelle AWS gestiti sono crittografati con crittografia lato server utilizzando chiavi gestite Amazon S3 (`aws:kms`). SSE-S3 Dopo aver creato la prima configurazione dei metadati, puoi impostare l'impostazione di crittografia predefinita per il bucket di tabelle AWS gestite in modo che utilizzi la crittografia lato server con (`aws:kms`) keys (`aws:kms`). AWS Key Management Service AWS KMS SSE-KMS Per ulteriori informazioni, vedere [Crittografia per AWS i bucket di tabelle gestiti e. the section called “Specificando SSE-KMS”](#)

All'interno del bucket di tabelle AWS gestite, le tabelle di metadati per la configurazione sono in genere archiviate in uno spazio dei nomi con il seguente formato di denominazione:

b_*general-purpose-bucket-name*

Per ulteriori informazioni sui namespace di tabelle dei metadati, consulta [the section called “Come funzionano le tabelle di metadati”](#).

Quando crei la configurazione della tabella dei metadati, puoi scegliere di crittografare le tabelle di metadati AWS gestite con la crittografia lato server utilizzando le chiavi (). AWS Key Management Service AWS KMS SSE-KMS Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket generico. È possibile impostare il tipo di crittografia per le tabelle solo durante la creazione della tabella. Dopo aver creato una tabella gestita da AWS , non è possibile modificarne le impostazioni di crittografia. SSE-KMS Per specificare le tabelle di metadati, devi disporre di determinate autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni per SSE-KMS](#)

L'impostazione di crittografia per una tabella dei metadati ha la precedenza sull'impostazione di crittografia predefinita a livello di bucket. Se non specifichi la crittografia, la tabella erediterà l'impostazione di crittografia predefinita del bucket.

AWS i bucket di tabelle gestiti non vengono conteggiati ai fini delle quote di S3 Tables. Per ulteriori informazioni sull'utilizzo dei bucket di tabelle AWS gestiti e delle tabelle gestite, vedi [Lavorare con AWS i bucket di tabelle AWS gestiti](#).

Puoi creare una configurazione della tabella di metadati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Note

- Se hai creato la configurazione dei metadati di S3 prima del 15 luglio 2025, ti consigliamo di eliminare e ricreare la configurazione in modo da poter far scadere i record delle tabelle del journal, creare una tabella di inventario e creare una tabella di annotazioni. Per ulteriori informazioni, consulta [the section called “Abilitazione delle tabelle di inventario e annotazione sulle configurazioni di metadati create prima del 15 luglio 2025”](#).
- Se hai eliminato la configurazione della tabella dei metadati e desideri ricreare una configurazione per lo stesso bucket generico, devi prima eliminare manualmente le vecchie tabelle del diario, dell'inventario e delle annotazioni dal bucket di tabelle AWS gestito. In caso contrario, la creazione della nuova configurazione della tabella dei metadati non

riesce perché tali tabelle esistono già. Per eliminare le tabelle dei metadati, consulta [the section called “Cancellazione di tabelle di metadati”](#).

L'eliminazione della configurazione della tabella dei metadati elimina solo la configurazione. Il bucket di tabelle AWS gestito e le tabelle di metadati esistono ancora, anche se elimini la configurazione della tabella di metadati.

Prerequisiti

Prima di creare una configurazione di tabelle dei metadati, è necessario soddisfare i prerequisiti seguenti:

- Per creare una configurazione di tabelle dei metadati, è necessario disporre delle autorizzazioni AWS Identity and Access Management (IAM) richieste per creare e gestire le tabelle dei metadati. Per ulteriori informazioni, consulta [the section called “Autorizzazioni per le tabelle di metadati”](#).
- Se prevedi di interrogare le tue tabelle di metadati con Amazon Athena o un altro motore di AWS query, assicurati di integrare il bucket di tabelle gestite con i servizi di analisi. AWS Per ulteriori informazioni, consulta [the section called “Integrazione delle tabelle S3 con AWS i servizi di analisi”](#).

Se hai già integrato un table bucket esistente in questa regione, anche il bucket di tabelle AWS gestito viene integrato automaticamente. Per determinare lo stato di integrazione dei bucket di tabelle nella Regione, apri la console Amazon S3 e scegli Bucket di tabelle nel riquadro di navigazione a sinistra. In Integrazione con i servizi di AWS analisi, controlla la regione e se lo stato dell'integrazione indica Abilitato.

Creazione di configurazioni delle tabelle di metadati

Utilizzo della console S3

Per creare configurazioni delle tabelle di metadati

Prima di creare la configurazione di una tabella di metadati, assicurati di aver esaminato e soddisfatto i [prerequisiti](#) e di aver rivisto [the section called “Limitazioni e restrizioni”](#).

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.

3. Scegli il bucket per uso generico per il quale si desidera creare una configurazione di tabella di metadati.

 Note

Assicurati che questo secchio per uso generico sia un contenitore Regione AWS in cui siano disponibili secchi da tavolo. I bucket di tabelle sono disponibili solo nelle Regioni Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio) e Stati Uniti occidentali (Oregon).

4. Nella pagina dei dettagli del bucket, scegli la scheda Metadati.
5. Nella scheda Metadati, scegli Crea configurazione dei metadati.
6. Nella pagina di configurazione Create metadata, nella tabella Journal, puoi scegliere se crittografare la tabella con la crittografia lato server utilizzando le chiavi (). AWS Key Management Service AWS KMS SSE-KMS Per impostazione predefinita, le tabelle journal sono crittografate con crittografia lato server utilizzando le chiavi gestite di Amazon S3 (). SSE-S3

Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket generico.

 Important

È possibile impostare il tipo di crittografia per le tabelle dei metadati solo durante la creazione della tabella. Dopo aver creato una tabella AWS gestita, non puoi modificarne le impostazioni di crittografia.

- Per crittografare la tabella del journal con SSE-S3 (impostazione predefinita), scegli Non specificare il tipo di crittografia.
- Per crittografare la tabella del journal con SSE-KMS, scegli Specifica il tipo di crittografia. In Tipo di crittografia, scegliete Server-side la crittografia utilizzando le chiavi AWS Key Management Service (AWS KMS) (SSE-KMS). In Chiave AWS KMS , scegli tra le chiavi KMS esistenti o inserisci l'ARN di una chiave KMS. Se non disponi già di una chiave KMS, scegli Inserisci l'ARN della chiave KMS, quindi scegli Crea una chiave KMS.

Assicurati di aver impostato le autorizzazioni necessarie per SSE-KMS. Per ulteriori informazioni, consulta [Autorizzazioni per. SSE-KMS](#)

7. (Facoltativo) Per impostazione predefinita, i record della tabella del diario non scadono. Per ridurre al minimo i costi di archiviazione per la tabella del diario, scegli Abilitato per Scadenza dei record.

Se abiliti la scadenza dei record della tabella del diario, puoi impostare il numero di giorni per mantenere i record della tabella del diario. Per impostare il valore di Giorni dopo i quali scadono i record, puoi specificare qualsiasi numero intero compreso tra 7 e 2147483647. Ad esempio, per mantenere i record della tabella del diario per un anno, imposta questo valore su 365.

I record scadono entro 24-48 ore dal momento in cui sono diventati idonei alla scadenza.

 Important

Dopo la scadenza, i record della tabella del diario non possono essere recuperati.

Per i record della tabella del diario scadono dopo il numero di giorni specificato, seleziona la casella di controllo.

8. (Facoltativo) Se desideri aggiungere una tabella di inventario alla configurazione della tabella dei metadati, in Tabella di inventario in tempo reale, scegli Abilitato per Stato di configurazione.

Puoi scegliere se crittografare la tabella con la crittografia lato server utilizzando le chiavi AWS Key Management Service (AWS KMS) (). SSE-KMS Per impostazione predefinita, le tabelle di inventario sono crittografate con crittografia lato server utilizzando le chiavi gestite di Amazon S3 (). SSE-S3

Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket generico.

 Important

È possibile impostare il tipo di crittografia per le tabelle dei metadati solo durante la creazione della tabella. Dopo aver creato una tabella AWS gestita, non puoi modificarne le impostazioni di crittografia.

- Per crittografare la tabella dell'inventario con SSE-S3 (impostazione predefinita), scegli Non specificare il tipo di crittografia.

- Per crittografare la tabella dell'inventario con SSE-KMS, scegli Specifica il tipo di crittografia. In Tipo di crittografia, scegli Server-side la crittografia utilizzando le chiavi AWS Key Management Service (AWS KMS) (SSE-KMS). In Chiave AWS KMS, scegli tra le chiavi KMS esistenti o inserisci l'ARN di una chiave KMS. Se non disponi già di una chiave KMS, scegli Inserisci l'ARN della chiave KMS, quindi scegli Crea una chiave KMS.

Assicurati di aver impostato le autorizzazioni necessarie per SSE-KMS. Per ulteriori informazioni, consulta [Autorizzazioni per SSE-KMS](#)

9. (Facoltativo) Se desideri aggiungere una tabella di annotazioni alla configurazione della tabella dei metadati, in Tabella di annotazione, scegli Abilitato per lo stato di configurazione.

Nel ruolo IAM, scegli uno dei seguenti metodi di selezione del ruolo IAM:

- Crea un nuovo ruolo IAM: Amazon S3 crea un nuovo ruolo IAM con le autorizzazioni richieste per la tabella di annotazione.
- Scegli tra i ruoli IAM esistenti: seleziona un ruolo IAM esistente dal menu a discesa dei ruoli IAM. Il ruolo deve disporre delle autorizzazioni necessarie per leggere le annotazioni dal bucket.
- Inserisci l'ARN del ruolo IAM: inserisci l'ARN di un ruolo IAM esistente con le autorizzazioni richieste.

Per ulteriori informazioni sulle autorizzazioni richieste per il ruolo IAM della tabella delle annotazioni, consulta [Ruolo IAM della tabella di annotazione](#).

Puoi scegliere se crittografare la tabella delle annotazioni con la crittografia lato server utilizzando le chiavi (). AWS Key Management Service AWS KMS SSE-KMS Per impostazione predefinita, le tabelle di annotazione sono crittografate con crittografia lato server utilizzando le chiavi gestite di Amazon S3 (). SSE-S3

Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket generico.

Important

È possibile impostare il tipo di crittografia per le tabelle dei metadati solo durante la creazione della tabella. Dopo aver creato una tabella AWS gestita, non puoi modificarne le impostazioni di crittografia.

- Per crittografare la tabella delle annotazioni con SSE-S3 (impostazione predefinita), scegli Non specificare il tipo di crittografia.
- Per crittografare la tabella delle annotazioni con SSE-KMS, scegli Specifica il tipo di crittografia. In Tipo di crittografia, scegliete Server-side la crittografia utilizzando le chiavi AWS Key Management Service (AWS KMS) (SSE-KMS). In Chiave AWS KMS , scegli tra le chiavi KMS esistenti o inserisci l'ARN di una chiave KMS. Se non disponi già di una chiave KMS, scegli Inserisci l'ARN della chiave KMS, quindi scegli Crea una chiave KMS.

Assicurati di aver impostato le autorizzazioni necessarie per SSE-KMS. Per ulteriori informazioni, consulta [Autorizzazioni per SSE-KMS](#)

10. Scegli Creazione di configurazioni delle tabelle di metadati.

Se la configurazione della tabella dei metadati è riuscita, i nomi e gli ARN delle tabelle dei metadati vengono visualizzati nella scheda Metadati, insieme al nome del bucket della tabella gestita da AWS e del namespace.

Se hai scelto di abilitare una tabella di inventario per la configurazione della tabella dei metadati, la tabella viene sottoposta a un processo noto come riempimento, durante il quale Amazon S3 analizza il bucket per uso generico per recuperare i metadati iniziali per tutti gli oggetti presenti nel bucket. A seconda del numero di oggetti nel bucket, questo processo può richiedere da minuti (minimo 15 minuti) a ore. Al termine del processo di riempimento, lo stato della tabella di inventario passa da Riempimento in corso ad Attivo. Una volta completato il riempimento, gli aggiornamenti degli oggetti si riflettono in genere nella tabella di inventario entro un'ora.

Per monitorare gli aggiornamenti della configurazione della tabella dei metadati, si può usare AWS CloudTrail. Per ulteriori informazioni, consulta [the section called "Azioni a livello di bucket di Amazon S3 tracciate mediante registrazione CloudTrail"](#).

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano AWS CLI installati e configurati. Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

In alternativa, puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da Console

di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Per creare una configurazione della tabella di metadati utilizzando AWS CLI

Prima di creare la configurazione di una tabella di metadati, assicurati di aver esaminato e soddisfatto i [prerequisiti](#) e di aver rivisto [the section called "Limitazioni e restrizioni"](#).

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le informazioni appropriate.

1. Crea un file JSON contenente la configurazione della tabella dei metadati e salvalo (ad esempio, `metadata-config.json`). Di seguito è riportato un esempio di configurazione.

È necessario specificare se abilitare o disabilitare la scadenza dei record della tabella del diario. Se si sceglie di abilitare la scadenza dei record, è necessario specificare anche il numero di giorni dopo i quali scadranno i record della tabella del diario. Per impostare il valore di `Days`, è possibile specificare qualsiasi numero intero compreso tra 7 e 2147483647. Ad esempio, per mantenere i record della tabella del diario per un anno, imposta questo valore su 365.

Facoltativamente, puoi scegliere di configurare una tabella di inventario e una tabella di annotazione.

Per le tabelle di registrazione, le tabelle di inventario e le tabelle di annotazione, è possibile specificare facoltativamente una configurazione di crittografia. Per impostazione predefinita, le tabelle di metadati sono crittografate con crittografia lato server utilizzando le chiavi gestite di Amazon S3 (SSE-S3), che puoi specificare impostando su `SseAlgorithm AES256`

Per crittografare le tabelle di metadati con la crittografia lato server utilizzando `() keys ()`, imposta su `AWS Key Management Service AWS KMS SSE-KMS SseAlgorithm aws:kms` È inoltre necessario impostare `KmsKeyArn` sull'ARN di una chiave KMS gestita dal cliente nella stessa Regione in cui si trova il bucket per uso generico.

```
{
  "JournalTableConfiguration": {
    "RecordExpiration": {
      "Expiration": "ENABLED",
      "Days": 10
    },
    "EncryptionConfiguration": {
      "SseAlgorithm": "AES256"
    }
  }
}
```

```
    }
  },
  "InventoryTableConfiguration": {
    "ConfigurationState": "ENABLED",
    "EncryptionConfiguration": {
      "SseAlgorithm": "aws:kms",
      "KmsKeyArn": "arn:aws:kms:us-east-2:account-id:key/key-id"
    }
  },
  "AnnotationTableConfiguration": {
    "ConfigurationState": "ENABLED",
    "Role": "arn:aws:iam:account-id:role/annotation-table-role",
    "EncryptionConfiguration": {
      "SseAlgorithm": "AES256"
    }
  }
}
```

2. Utilizza il seguente comando per applicare la configurazione della tabella dei metadati al bucket per uso generico (ad esempio, *amzn-s3-demo-bucket*):

```
aws s3api create-bucket-metadata-configuration \
--bucket amzn-s3-demo-bucket \
--metadata-configuration file://./metadata-config.json \
--region us-east-2
```

3. Per verificare che la configurazione sia stata creata, usa il seguente comando:

```
aws s3api get-bucket-metadata-configuration \
--bucket amzn-s3-demo-bucket \
--region us-east-2
```

Per monitorare gli aggiornamenti della configurazione della tabella dei metadati, si può usare AWS CloudTrail. Per ulteriori informazioni, consulta [the section called “Azioni a livello di bucket di Amazon S3 tracciate mediante registrazione CloudTrail”](#).

Utilizzo della REST API

È possibile inviare richieste REST per creare la configurazione di una tabella di metadati. Per ulteriori informazioni, consulta [CreateBucketMetadataConfiguration](#) nella documentazione di riferimento delle API di Amazon S3.

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per creare una configurazione di tabelle di metadati in Amazon S3. Per informazioni, consulta [l'elenco degli SDK supportati](#) nella documentazione di riferimento delle API di Amazon S3.

Abilitazione delle tabelle di inventario e annotazione sulle configurazioni di metadati create prima del 15 luglio 2025

Se hai creato la configurazione dei metadati S3 prima del 15 luglio 2025, ti consigliamo di eliminare e ricreare la configurazione in modo da poter far scadere i record della tabella del journal, creare una tabella di inventario e creare una tabella di annotazioni. Eventuali modifiche al bucket per uso generico che si verificano tra l'eliminazione della vecchia configurazione e la creazione di quella nuova non vengono registrate in nessuna delle tabelle del diario.

Per eseguire la migrazione da una vecchia configurazione dei metadati a una nuova configurazione, procedi come segue:

1. Elimina la configurazione esistente della tabella dei metadati. Per istruzioni dettagliate, consulta [the section called "Cancellazione di configurazioni delle tabelle di metadati"](#).
2. Crea una nuova configurazione della tabella dei metadati. Per istruzioni dettagliate, consulta [the section called "Creazione di tabelle di metadati"](#).

Se hai bisogno di assistenza per la migrazione della configurazione, contatta. [Supporto AWS](#)

Dopo aver creato la nuova configurazione dei metadati, avrai due tabelle del diario. Se non hai più bisogno della vecchia tabella del diario, puoi eliminarla. Per istruzioni dettagliate, consulta [the section called "Cancellazione di tabelle di metadati"](#). Se hai mantenuto la vecchia tabella del diario e desideri unirla a quella nuova, consulta [the section called "Unione di metadati personalizzati"](#) per alcuni esempi su come unire due tabelle.

Dopo la migrazione, puoi effettuare quanto segue:

1. Per visualizzare la configurazione, ora puoi utilizzare l'operazione API `GetBucketMetadataConfiguration`. Per determinare se la configurazione è vecchia o nuova, puoi esaminare il seguente attributo della risposta dell'API `GetBucketMetadataConfiguration`. Un tipo di bucket gestito da AWS ("aws") indica una nuova configurazione e un tipo di bucket gestito dal cliente ("customer") indica una vecchia configurazione.

```
"MetadataTableConfigurationResult": {  
    "TableBucketType": ["aws" | "customer"]
```

Per ulteriori informazioni, consulta [the section called “Visualizzazione delle configurazioni delle tabelle dei metadati”](#).

Note

È possibile utilizzare le operazioni API `GetBucketMetadataConfiguration` e `DeleteBucketMetadataConfiguration` con configurazioni di tabelle dei metadati vecchie o nuove. Tuttavia, se provi a utilizzare le operazioni API `GetBucketMetadataTableConfiguration` e `DeleteBucketMetadataTableConfiguration` con nuove configurazioni, verranno visualizzati errori HTTP 405 Method Not Allowed. Assicurati di aggiornare i processi per utilizzare le nuove operazioni API (`CreateBucketMetadataConfiguration`, `GetBucketMetadataConfiguration` e `DeleteBucketMetadataConfiguration`) anziché le vecchie operazioni API.

2. Se prevedi di interrogare le tue tabelle di metadati con Amazon Athena o un altro motore di AWS query, assicurati di integrare il bucket di tabelle AWS gestite con i servizi di analisi. AWS Se hai già integrato un table bucket esistente in questa regione, anche il bucket di tabelle AWS gestito viene integrato automaticamente. Per ulteriori informazioni, consulta [the section called “Integrazione delle tabelle S3 con AWS i servizi di analisi”](#).

Controllo dell'accesso alle tabelle di metadati

Per controllare l'accesso alle tabelle di metadati di Amazon S3, puoi utilizzare policy basate sulle risorse AWS Identity and Access Management (IAM) allegate al bucket di tabelle e alle tabelle di metadati. In altre parole, è possibile controllare l'accesso alle tabelle di metadati a livello sia di bucket sia di tabella.

Per ulteriori informazioni sul controllo degli accessi alle tabelle e ai bucket delle tabelle, consulta [Gestione degli accessi per le tabelle S3](#).

 Important

Quando crei o aggiorni le policy di bucket o tabelle, assicurati di non limitare la scrittura dei principali del servizio `metadata.s3.amazonaws.com` e `maintenance.s3tables.amazonaws.com` Amazon S3 sul bucket o sulla tabella dei metadati.

Se Amazon S3 non è in grado di scrivere sul bucket di tabelle o sulle tabelle dei metadati, è necessario eliminare la configurazione dei metadati, eliminare le tabelle dei metadati e quindi creare una nuova configurazione. Se nella configurazione era presente una tabella di inventario, è necessario crearne una nuova e verranno nuovamente addebitati i costi per il riempimento della nuova tabella di inventario.

Puoi anche controllare l'accesso alle righe e alle colonne nelle tabelle di metadati tramite AWS Lake Formation. Per ulteriori informazioni, consulta [Gestione dei permessi di Lake Formation](#) e [Filtraggio dei dati e sicurezza a livello di cella in Lake Formation](#) nella Guida per gli sviluppatori di AWS Lake Formation.

Scadenza dei record della tabella del diario

Per impostazione predefinita, i record della tabella del diario non scadono. Per ridurre al minimo i costi di archiviazione per la tabella del diario, è possibile abilitare la scadenza dei record della tabella del diario.

 Note

Se la configurazione di S3 Metadata è stata creata prima del 15 luglio 2025, non puoi abilitare la scadenza dei record della tabella del diario su quella configurazione. È consigliabile eliminare e ricreare la configurazione in modo da poter impostare la scadenza dei record della tabella del diario e creare una tabella di inventario. Per ulteriori informazioni, consulta [the section called “Abilitazione delle tabelle di inventario e annotazione sulle configurazioni di metadati create prima del 15 luglio 2025”](#).

Se abiliti la scadenza dei record della tabella del diario, puoi impostare il numero di giorni per mantenere i record della tabella del diario. Per impostare questo valore, specifica un numero intero compreso tra 7 e 2147483647. Ad esempio, per mantenere i record della tabella del diario per un anno, imposta questo valore su 365.

 Important

Dopo la scadenza, i record della tabella del diario non possono essere recuperati.

I record scadono entro 24-48 ore dal momento in cui sono diventati idonei alla scadenza. I record del diario vengono rimossi dallo snapshot più recente. I dati e l'archiviazione dei record eliminati vengono rimossi tramite le operazioni di manutenzione delle tabelle.

Se hai abilitato la scadenza dei record della tabella del diario, puoi disabilitarla in qualsiasi momento per arrestare la scadenza dei record della tabella del diario.

Puoi far scadere i record delle tabelle del journal utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Come impostare la scadenza dei record della tabella del diario

Utilizzo della console S3

Come impostare la scadenza dei record della tabella del diario

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Scegli il bucket per uso generico che contiene la configurazione della tabella dei metadati con la tabella del diario di cui desideri impostare la scadenza dei record.
4. Nella pagina dei dettagli del bucket, scegli la scheda Metadati.
5. Nella scheda Metadati scegli Modifica, quindi scegli Modifica la scadenza del record della tabella del diario.
6. Nella pagina Modifica la scadenza del record della tabella del diario, scegli Abilitato in Scadenza dei record.
7. Imposta il numero di giorni di conservazione dei record della tabella del diario. Per impostare il valore di Giorni dopo i quali scadono i record, specifica qualsiasi numero intero compreso tra 7 e 2147483647. Ad esempio, per mantenere i record della tabella del diario per un anno, imposta questo valore su 365.

 Important

Dopo la scadenza, i record della tabella del diario non possono essere recuperati.

8. Per i record della tabella del diario scadono dopo il numero di giorni specificato, seleziona la casella di controllo.
9. Scegli Save changes (Salva modifiche).

Se desideri disabilitare la scadenza dei record della tabella del diario, ripeti i passaggi precedenti, ma scegli Disabilitato anziché Abilitato alla fase 6.

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano AWS CLI installati e configurati. Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Puoi anche eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da Console di gestione AWS. Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Per far scadere i record della tabella del diario utilizzando AWS CLI

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le informazioni appropriate.

1. Crea un file JSON contenente la configurazione della tabella del diario e salvalo (ad esempio, `journal-config.json`). Di seguito è riportato un esempio di configurazione.

Per impostare il valore Days, specifica un numero intero compreso tra 7 e 2147483647. Ad esempio, per mantenere i record della tabella del diario per un anno, imposta questo valore su 365.

```
{
  "RecordExpiration": {
    "Expiration": "ENABLED",
    "Days": 10
  }
}
```

```
}
```

Per disabilitare la scadenza dei record della tabella del diario, crea la seguente configurazione di esempio. Se `Expiration` è impostato su `DISABLED`, non è necessario specificare un valore `Days` nella configurazione.

```
{
  "RecordExpiration": {
    "Expiration": "DISABLED"
  }
}
```

2. Utilizza il seguente comando per impostare la scadenza dei record dalla tabella del diario nel bucket per uso generico (ad esempio, *amzn-s3-demo-bucket*):

```
aws s3api update-bucket-metadata-journal-table-configuration \
--bucket amzn-s3-demo-bucket \
--journal-table-configuration file:///./journal-config.json \
--region us-east-2
```

Utilizzo della REST API

Per impostare la scadenza dei record della tabella del diario è possibile inviare richieste REST. Per ulteriori informazioni, consulta [UpdateBucketMetadataJournalTableConfiguration](#).

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per far scadere i record delle tabelle di journal in Amazon S3. Per informazioni, consulta [l'elenco degli SDK supportati](#).

Abilitazione o disabilitazione delle tabelle di inventario in tempo reale

Per impostazione predefinita, la configurazione della tabella dei metadati contiene una tabella del diario che registra gli eventi che si verificano per gli oggetti presenti nel bucket. La tabella del diario è obbligatoria per ogni configurazione della tabella dei metadati.

Facoltativamente, puoi aggiungere una tabella di inventario in tempo reale alla configurazione della tabella dei metadati. La tabella di inventario in tempo reale fornisce un inventario semplice e sottoponibile a query di tutti gli oggetti e delle relative versioni presenti nel bucket in modo da poter determinare lo stato più recente dei dati.

 Note

Se la configurazione di S3 Metadata è stata creata prima del 15 luglio 2025, non puoi abilitare una tabella di inventario su quella configurazione. È consigliabile eliminare e ricreare la configurazione in modo da poter creare una tabella di inventario e impostare la scadenza dei record della tabella del diario. Per ulteriori informazioni, consulta [the section called “Abilitazione delle tabelle di inventario e annotazione sulle configurazioni di metadati create prima del 15 luglio 2025”](#).

La tabella di inventario contiene i metadati più recenti per tutti gli oggetti presenti nel bucket. È possibile utilizzare questa tabella per semplificare e velocizzare i flussi di lavoro aziendali e i processi relativi ai big data individuando gli oggetti che si desidera elaborare per vari carichi di lavoro. Ad esempio, puoi eseguire query sulla tabella di inventario in tempo reale per effettuare le seguenti operazioni:

- Trovare tutti gli oggetti archiviati nella classe di archiviazione S3 Glacier Deep Archive.
- Creare una distribuzione di tag di oggetto o trovare oggetti senza tag.
- Trova tutti gli oggetti non crittografati utilizzando la crittografia lato server con AWS Key Management Service () keys ()AWS KMS. SSE-KMS
- Confronta la tabella di inventario in due momenti diversi per comprendere la crescita degli oggetti con tag specifici.

Se hai scelto di abilitare una tabella di inventario per la configurazione della tabella dei metadati, la tabella viene sottoposta a un processo noto come riempimento, durante il quale Amazon S3 analizza il bucket per uso generico per recuperare i metadati iniziali per tutti gli oggetti presenti nel bucket. A seconda del numero di oggetti nel bucket, questo processo può richiedere da minuti (minimo 15 minuti) a ore. Al termine del processo di riempimento, lo stato della tabella di inventario passa da Riempimento in corso ad Attivo. Una volta completato il riempimento, gli aggiornamenti degli oggetti si riflettono in genere nella tabella di inventario entro un'ora.

 Note

- Il riempimento della tabella di inventario viene addebitato. Se il bucket per uso generico contiene più di un miliardo di oggetti, verrà addebitata anche una tariffa mensile per la tabella di inventario. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

- Non puoi sospendere gli aggiornamenti della tabella di inventario e poi riprenderli. Tuttavia, puoi disabilitare la configurazione della tabella di inventario. La disabilitazione della tabella di inventario non la elimina. La tabella di inventario viene mantenuta per riferimento fino a quando non decidi di eliminarla.

Se hai disabilitato la tabella di inventario e successivamente desideri riattivarla, devi prima eliminare la vecchia tabella di inventario dal bucket delle tabelle AWS gestito. Quando riabiliti la configurazione della tabella di inventario, Amazon S3 crea una nuova tabella di inventario e vengono nuovamente addebitati i costi per il riempimento della nuova tabella di inventario.

Puoi abilitare o disabilitare le tabelle di inventario utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Prerequisiti

Se hai disabilitato la tabella di inventario e ora desideri riattivarla, devi prima eliminare manualmente la vecchia tabella di inventario dal bucket di tabelle gestito. AWS In caso contrario, la riabilitazione della tabella di inventario non riesce perché una tabella di inventario esiste già nel bucket di tabelle. Per eliminare la tabella di inventario, consulta [the section called “Cancellazione di tabelle di metadati”](#).

Quando riabiliti la configurazione della tabella di inventario, Amazon S3 crea una nuova tabella di inventario e vengono nuovamente addebitati i costi per il riempimento della nuova tabella di inventario.

Abilitazione o disabilitazione delle tabelle di inventario

Utilizzo della console S3

Come abilitare o disabilitare le tabelle di inventario

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Scegli il bucket per uso generico con la configurazione della tabella dei metadati per cui desideri abilitare o disabilitare una tabella di inventario.

4. Nella pagina dei dettagli del bucket, scegli la scheda Metadati.
5. Nella scheda Metadati, scegli Modifica, quindi scegli Modifica la configurazione della tabella di inventario.
6. Nella pagina Modifica la configurazione della tabella di inventario, scegli Abilitato o Disabilitato in Tabella di inventario.

 Note

Prima di scegliere Abilitato, assicurati di aver esaminato e soddisfatto i [prerequisiti](#).

- Se hai scelto Abilitato, puoi scegliere se crittografare la tua tabella con la crittografia lato server utilizzando le chiavi AWS Key Management Service (AWS KMS) (). SSE-KMS Per impostazione predefinita, le tabelle di inventario sono crittografate con crittografia lato server utilizzando chiavi gestite da Amazon S3 (). SSE-S3

Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket generico.

 Important

È possibile impostare il tipo di crittografia per le tabelle dei metadati solo durante la creazione della tabella. Dopo aver creato una tabella AWS gestita, non puoi modificarne le impostazioni di crittografia.

- Per crittografare la tabella dell'inventario con SSE-S3 (impostazione predefinita), scegli Non specificare il tipo di crittografia.
 - Per crittografare la tabella dell'inventario con SSE-KMS, scegli Specifica il tipo di crittografia. In Tipo di crittografia, scegli Server-side la crittografia utilizzando le chiavi AWS Key Management Service (AWS KMS) (SSE-KMS). In Chiave AWS KMS , scegli tra le chiavi KMS esistenti o inserisci l'ARN di una chiave KMS. Se non disponi già di una chiave KMS, scegli Inserisci l'ARN della chiave KMS, quindi scegli Crea una chiave KMS.
 - Se scegli Disabilitato, seleziona la casella di controllo in Dopo la disabilitazione della tabella di inventario, la tabella non verrà più aggiornata e gli aggiornamenti non possono essere ripresi.
7. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano AWS CLI installati e configurati. Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

In alternativa, puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Per abilitare o disabilitare le tabelle di inventario utilizzando AWS CLI

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le informazioni appropriate.

Note

Prima di abilitare una configurazione di inventario, assicurati di aver esaminato e soddisfatto i [prerequisiti](#).

1. Crea un file JSON contenente la configurazione della tabella di inventario e salvalo (ad esempio, `inventory-config.json`). Di seguito è riportato un esempio di configurazione per abilitare una nuova tabella di inventario.

Quando abiliti una tabella di inventario, puoi facoltativamente specificare una configurazione di crittografia. Per impostazione predefinita, le tabelle di metadati sono crittografate con crittografia lato server utilizzando le chiavi gestite di Amazon S3 (SSE-S3), che puoi specificare impostando su. `SseAlgorithm AES256`

Per crittografare la tabella di inventario con la crittografia lato server utilizzando AWS Key Management Service (AWS KMS), imposta su. `SSE-KMS SseAlgorithm aws:kms` È inoltre necessario impostare `KmsKeyArn` sull'ARN di una chiave KMS gestita dal cliente nella stessa Regione in cui si trova il bucket per uso generico.

```
{
  "ConfigurationState": "ENABLED",
  "EncryptionConfiguration": {
    "SseAlgorithm": "aws:kms",
```

```
"KmsKeyArn": "arn:aws:kms:us-east-2:account-id:key/key-id"
}
```

Se desideri disabilitare una tabella di inventario esistente, utilizza la seguente configurazione:

```
{
  "ConfigurationState": "DISABLED" }
}
```

2. Utilizza il seguente comando per aggiornare la configurazione della tabella di inventario per il bucket per uso generico (ad esempio, *amzn-s3-demo-bucket*):

```
aws s3api update-bucket-metadata-inventory-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--inventory-table-configuration file://./inventory-config.json \
--region us-east-2
```

Utilizzo della REST API

È possibile inviare richieste REST per abilitare o disabilitare le tabelle di inventario. Per ulteriori informazioni, consulta [UpdateBucketMetadataInventoryTableConfiguration](#).

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per abilitare o disabilitare le tabelle di inventario in Amazon S3. Per informazioni, consulta l'[elenco degli SDK supportati](#).

Abilitazione o disabilitazione delle tabelle di annotazione

Per impostazione predefinita, la configurazione della tabella dei metadati contiene una tabella del diario che registra gli eventi che si verificano per gli oggetti presenti nel bucket. La tabella del diario è obbligatoria per ogni configurazione della tabella dei metadati.

Facoltativamente, puoi aggiungere una tabella delle annotazioni alla configurazione della tabella dei metadati. La tabella delle annotazioni tiene traccia di tutte le annotazioni sugli oggetti nel bucket in modo da poter interrogare i dati delle annotazioni su larga scala.

La tabella delle annotazioni contiene le annotazioni più recenti per tutti gli oggetti del bucket. È possibile utilizzare questa tabella per semplificare e velocizzare i flussi di lavoro aziendali e i processi

relativi ai big data identificando gli oggetti in base alle relative annotazioni. Ad esempio, puoi eseguire query sulla tabella delle annotazioni per effettuare le seguenti operazioni:

- Trova tutti gli oggetti con una chiave o un valore di annotazione specifico.
- Crea una distribuzione delle chiavi di annotazione tra gli oggetti del bucket.
- Trova tutti gli oggetti a cui sono state applicate annotazioni da un principale specifico.

Se hai scelto di abilitare una tabella di annotazioni per la configurazione della tabella di metadati, la tabella viene sottoposta a un processo noto come `backfill`, durante il quale Amazon S3 esegue la scansione del bucket generico per recuperare e compilare le annotazioni per tutti gli oggetti presenti nel bucket. A seconda del numero di oggetti nel bucket, questo processo può richiedere da minuti a ore. Al termine del processo di `backfill`, lo stato della tabella delle annotazioni passa da `Backfill` a `Attivo`. Una volta completato il `backfill`, gli aggiornamenti agli oggetti si riflettono in genere nella tabella delle annotazioni entro un'ora.

Note

- Ti viene addebitato il costo del riempimento della tabella delle annotazioni. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).
- Non puoi sospendere gli aggiornamenti della tabella delle annotazioni e poi riprenderli. Tuttavia, puoi disabilitare la configurazione della tabella delle annotazioni. La disabilitazione della tabella di annotazione non la elimina. La tabella delle annotazioni viene mantenuta come riferimento fino a quando non decidi di eliminarla.

Se hai disabilitato la tabella di annotazioni e successivamente desideri riattivarla, devi prima eliminare la vecchia tabella di annotazioni dal bucket delle tabelle gestite. AWS
Quando riabiliti la configurazione della tabella delle annotazioni, Amazon S3 ne crea una nuova e vengono nuovamente addebitati i costi per il riempimento della nuova tabella delle annotazioni.

Puoi abilitare o disabilitare le tabelle di annotazione utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Prerequisiti

Se hai disabilitato la tabella di annotazioni e ora desideri riattivarla, devi prima eliminare manualmente la vecchia tabella di annotazioni dal bucket di tabelle gestito. AWS In caso contrario, la riattivazione della tabella di annotazione non riesce perché esiste già una tabella di annotazioni nel bucket della tabella. Per eliminare la tabella di annotazione, vedere. [the section called “Cancellazione di tabelle di metadati”](#)

Quando riabiliti la configurazione della tabella delle annotazioni, Amazon S3 ne crea una nuova e vengono nuovamente addebitati i costi per il riempimento della nuova tabella delle annotazioni.

Ruolo IAM della tabella delle annotazioni

La tabella delle annotazioni richiede un ruolo IAM che conceda ad Amazon S3 Metadata l'autorizzazione a leggere le annotazioni dal bucket. Utilizza le seguenti politiche di fiducia e autorizzazioni quando crei questo ruolo.

Policy di attendibilità

La seguente politica di fiducia identifica Amazon S3 Metadata come l'entità del servizio che può assumere il ruolo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "metadata.s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
      }
    }
  ]
}
```

Policy delle autorizzazioni

La seguente politica di autorizzazione concede al ruolo IAM le autorizzazioni minime richieste per leggere le annotazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermissionForGetAnnotation",
      "Effect": "Allow",
      "Action": [
        "s3:GetObjectAnnotation",
        "s3:GetObjectVersionAnnotation"
      ],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    },
    {
      "Sid": "PermissionsForListBucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"]
    },
    {
      "Sid": "PermissionsForDecryptAnnotation",
      "Effect": "Allow",
      "Action": ["kms:Decrypt"],
      "Resource": ["*"]
    }
  ]
}
```

Se gli oggetti utilizzano la SSE-KMS crittografia, l'`kms:Decrypt` autorizzazione copre la decrittografia della AWS KMS chiave utilizzata per crittografare gli oggetti. È inoltre necessaria `iam:PassRole` l'autorizzazione per assegnare il ruolo alla configurazione della tabella di annotazione.

Abilita o disabilita le tabelle di annotazione

Utilizzo della console S3

Per abilitare o disabilitare le tabelle di annotazione

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Scegli il bucket generico con la configurazione della tabella di metadati per cui desideri abilitare o disabilitare una tabella di annotazioni.
4. Nella pagina dei dettagli del bucket, scegli la scheda Metadati.
5. Nella scheda Metadati, scegli Modifica, quindi scegli Modifica configurazione della tabella di annotazione.
6. Nella pagina Modifica configurazione della tabella di annotazione, scegliete Abilitato o Disabilitato in Tabella di annotazione.

Note

Prima di scegliere Abilitato, assicurati di aver esaminato e soddisfatto i [prerequisiti](#).

- Se hai scelto Abilitato, nel ruolo IAM, scegli uno dei seguenti metodi di selezione del ruolo IAM:
 - Crea un nuovo ruolo IAM: Amazon S3 crea un nuovo ruolo IAM con le autorizzazioni richieste per la tabella delle annotazioni.
 - Scegli tra i ruoli IAM esistenti: seleziona un ruolo IAM esistente dal menu a discesa dei ruoli IAM. Il ruolo deve disporre delle autorizzazioni necessarie per leggere le annotazioni dal bucket.
 - Inserisci l'ARN del ruolo IAM: inserisci l'ARN di un ruolo IAM esistente con le autorizzazioni richieste.

Per ulteriori informazioni sulle autorizzazioni richieste per il ruolo IAM della tabella delle annotazioni, consulta [Ruolo IAM della tabella di annotazione](#).

Puoi anche scegliere se crittografare la tabella con la crittografia lato server utilizzando AWS Key Management Service () keys ().AWS KMS SSE-KMS Per impostazione predefinita, le

tabelle di annotazione sono crittografate con crittografia lato server utilizzando le chiavi gestite di Amazon S3 (). SSE-S3

Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket generico.

 Important

È possibile impostare il tipo di crittografia per le tabelle dei metadati solo durante la creazione della tabella. Dopo aver creato una tabella AWS gestita, non puoi modificarne le impostazioni di crittografia.

- Per crittografare la tabella delle annotazioni con SSE-S3 (impostazione predefinita), scegli Non specificare il tipo di crittografia.
- Per crittografare la tabella delle annotazioni con SSE-KMS, scegli Specifica il tipo di crittografia. In Tipo di crittografia, scegliete Server-side la crittografia utilizzando le chiavi AWS Key Management Service (AWS KMS) (SSE-KMS). In Chiave AWS KMS , scegli tra le chiavi KMS esistenti o inserisci l'ARN di una chiave KMS. Se non disponi già di una chiave KMS, scegli Inserisci l'ARN della chiave KMS, quindi scegli Crea una chiave KMS.
- Se hai scelto Disabilitato, in Dopo la disattivazione della tabella di annotazione, la tabella non verrà più aggiornata e gli aggiornamenti non potranno essere ripresi, seleziona la casella di controllo.

7. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano installati e configurati AWS CLI . Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

In alternativa, puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Per abilitare o disabilitare le tabelle di annotazione utilizzando AWS CLI

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le informazioni appropriate.

Note

Prima di abilitare una configurazione di annotazione, assicurati di aver esaminato e soddisfatto i [prerequisiti](#).

1. Crea un file JSON che contenga la configurazione della tabella delle annotazioni e salvalo (ad esempio). `annotation-config.json` Di seguito è riportata una configurazione di esempio per abilitare una nuova tabella di annotazioni.

Se stai abilitando una tabella di annotazioni, puoi facoltativamente specificare una configurazione di crittografia. Per impostazione predefinita, le tabelle di metadati sono crittografate con crittografia lato server utilizzando le chiavi gestite di Amazon S3 (SSE-S3), che puoi specificare impostando su. `SseAlgorithm AES256`

Per crittografare la tabella di annotazioni con la crittografia lato server utilizzando AWS Key Management Service (AWS KMS), imposta su. `AWS KMS SSE-KMS SseAlgorithm aws:kms` È inoltre necessario impostare `KmsKeyArn` sull'ARN di una chiave KMS gestita dal cliente nella stessa Regione in cui si trova il bucket per uso generico.

```
{
  "ConfigurationState": "ENABLED",
  "Role": "arn:aws:iam::account-id:role/annotation-table-role",
  "EncryptionConfiguration": {
    "SseAlgorithm": "aws:kms",
    "KmsKeyArn": "arn:aws:kms:us-east-2:account-id:key/key-id"
  }
}
```

Il `Role` campo è obbligatorio quando si abilita una tabella di annotazioni per la prima volta o quando si modifica il ruolo IAM. Il ruolo deve concedere ad Amazon S3 Metadata l'autorizzazione a leggere le annotazioni dal bucket. Per ulteriori informazioni, [consulta il ruolo IAM della tabella delle annotazioni](#).

Se desideri disabilitare una tabella di annotazione esistente, utilizza la seguente configurazione:

```
{  
  "ConfigurationState": "DISABLED" }
```

2. Usa il comando seguente per aggiornare la configurazione della tabella di annotazione per il tuo bucket generico (ad esempio,): *amzn-s3-demo-bucket*

```
aws s3api update-bucket-metadata-annotation-table-configuration \  
--bucket amzn-s3-demo-bucket \  
--annotation-table-configuration file:///./annotation-config.json \  
--region us-east-2
```

Utilizzo della REST API

È possibile inviare richieste REST per abilitare o disabilitare le tabelle di annotazione. Per ulteriori informazioni, consulta [UpdateBucketMetadataAnnotationTableConfiguration](#).

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per abilitare o disabilitare le tabelle di annotazione in Amazon S3. Per informazioni, consulta l'[elenco degli SDK supportati](#).

Visualizzazione delle configurazioni delle tabelle dei metadati

Se hai creato una configurazione di tabella di metadati per un bucket generico, puoi visualizzare informazioni sulla configurazione, ad esempio se è stata abilitata una tabella di inventario o una tabella di annotazione o se è stata abilitata la scadenza dei record della tabella di diario. Puoi anche visualizzare lo stato del diario, dell'inventario e delle tabelle di annotazione.

Puoi visualizzare la configurazione della tabella di metadati per un bucket generico utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Visualizzazione di una configurazione della tabella dei metadati

Utilizzo della console S3

Come visualizzare la configurazione della tabella dei metadati

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Scegli il bucket per uso generico per contenere la configurazione della tabella dei metadati da visualizzare.
4. Nella pagina dei dettagli del bucket, scegli la scheda Metadati.
5. Nella scheda Metadati, scorri verso il basso fino alla sezione Configurazione metadati. Nelle sezioni Tabella Journal, Inventory table e Annotation table, puoi visualizzare varie informazioni relative a queste configurazioni, come Amazon Resource Names (ARN), lo stato delle tabelle e se hai abilitato la scadenza dei record delle tabelle del journal, una tabella di inventario o una tabella di annotazione.

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano installati e configurati AWS CLI . Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

In alternativa, puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Per visualizzare la configurazione di una tabella di metadati utilizzando AWS CLI

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

1. Utilizza il seguente comando per visualizzare la configurazione della tabella dei metadati per il bucket per uso generico (ad esempio, *amzn-s3-demo-bucket*):

```
aws s3api get-bucket-metadata-configuration \
--bucket amzn-s3-demo-bucket \
--region us-east-2
```

2. Visualizza l'output di questo comando per vedere lo stato della configurazione della tabella dei metadati. Ad esempio:

```
{
  "GetBucketMetadataConfigurationResult": {
    "MetadataConfigurationResult": {
```

```

    "DestinationResult": {
      "TableBucketType": "aws",
      "TableBucketArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/
aws-managed-s3-111122223333-us-east-2",
      "TableNamespace": "b_general-purpose-bucket-name"
    },
    "JournalTableConfigurationResult": {
      "TableStatus": "ACTIVE",
      "TableName": "journal",
      "TableArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/aws-
managed-s3-111122223333-us-east-2/table/0f01234c-fe7a-492f-a4c7-adec3864ea85",
      "EncryptionConfiguration": {
        "SseAlgorithm": "AES256"
      },
      "RecordExpiration": {
        "Expiration": "ENABLED",
        "Days": 10
      }
    },
    "InventoryTableConfigurationResult": {
      "ConfigurationState": "ENABLED",
      "TableStatus": "BACKFILL_COMPLETE",
      "TableName": "inventory",
      "TableArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/aws-
managed-s3-111122223333-us-east-2/table/e123456-b876-4e5e-af29-bb055922ee4d",
      "EncryptionConfiguration": {
        "SseAlgorithm": "AES256"
      }
    },
    "AnnotationTableConfigurationResult": {
      "ConfigurationState": "ENABLED",
      "TableStatus": "ACTIVE",
      "TableName": "annotation",
      "TableArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/aws-
managed-s3-111122223333-us-east-2/table/f234567-a890-1b2c-d345-e678901f2345",
      "EncryptionConfiguration": {
        "SseAlgorithm": "AES256"
      },
      "Role": "arn:aws:iam::111122223333:role/annotation-table-role"
    }
  }
}

```

Utilizzo della REST API

È possibile inviare richieste REST per eliminare una configurazione della tabella dei metadati. Per ulteriori informazioni, consulta [GetBucketMetadataTableConfiguration](#).

Note

È possibile utilizzare l'operazione API `GetBucketMetadataConfiguration V2` con le configurazioni delle tabelle dei metadati V1 o V2. Tuttavia, se provi a utilizzare l'operazione API `GetBucketMetadataTableConfiguration V1` con le configurazioni V2, verrà visualizzato un errore HTTP 405 Method Not Allowed.

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per visualizzare la configurazione di una tabella di metadati in Amazon S3. Per informazioni, consulta l'[elenco degli SDK supportati](#).

Cancellazione di configurazioni delle tabelle di metadati

Se si desidera interrompere l'aggiornamento della configurazione della tabella dei metadati per un bucket per uso generico Amazon S3, è possibile eliminare la configurazione della tabella dei metadati collegata al bucket. L'eliminazione della configurazione della tabella dei metadati elimina solo la configurazione. Il bucket di tabelle AWS gestite e le tabelle di metadati esistono ancora, anche se elimini la configurazione della tabella di metadati. Tuttavia, le tabelle dei metadati non verranno più aggiornate.

Note

Se elimini la configurazione della tabella di metadati e desideri ricreare una configurazione per lo stesso bucket generico, devi prima eliminare manualmente le vecchie tabelle di diario, inventario e annotazioni dal bucket di tabelle gestito. AWS In caso contrario, la creazione della nuova configurazione della tabella dei metadati non riesce perché tali tabelle esistono già. Per eliminare le tabelle dei metadati, consulta [the section called “Cancellazione di tabelle di metadati”](#).

Per eliminare le tabelle dei metadati, consulta [the section called “Cancellazione di tabelle di metadati”](#). Per eliminare il bucket della tabella, consulta [Eliminazione di bucket di tabelle](#) e [DeleteTableBucket](#) nella documentazione di riferimento delle API di Amazon S3.

Puoi eliminare una configurazione della tabella di metadati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli SDK o l'API REST di Amazon S3. AWS

Cancellazione di configurazioni delle tabelle di metadati

Utilizzo della console S3

Per eliminare configurazioni delle tabelle di metadati

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Scegli il bucket per uso generico dal quale desideri rimuovere una configurazione di tabella di metadati.
4. Nella pagina dei dettagli del bucket, scegli la scheda Metadati.
5. Nella scheda Metadati, scegli Elimina.
6. Nella finestra di dialogo Elimina configurazione metadati, immetti **confirm** per confermare l'eliminazione della configurazione. Scegli Elimina.

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano AWS CLI installati e configurati. Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

In alternativa, puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Per eliminare una configurazione della tabella di metadati utilizzando AWS CLI

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le informazioni appropriate.

1. Utilizza il seguente comando per eliminare la configurazione della tabella dei metadati dal bucket per uso generico (ad esempio, *amzn-s3-demo-bucket*):

```
aws s3api delete-bucket-metadata-configuration \
```



```
--bucket amzn-s3-demo-bucket \  
--region us-east-2
```

2. Per verificare che la configurazione sia stata eliminata, usa il seguente comando:

```
aws s3api get-bucket-metadata-configuration \  
--bucket amzn-s3-demo-bucket \  
--region us-east-2
```

Utilizzo della REST API

È possibile inviare richieste REST per eliminare la configurazione di una tabella di metadati. Per ulteriori informazioni, consulta [DeleteBucketMetadataConfiguration](#).

Note

È possibile utilizzare l'operazione API `DeleteBucketMetadataConfiguration V2` con le configurazioni delle tabelle dei metadati V1 o V2. Tuttavia, se provi a utilizzare l'operazione API `DeleteBucketMetadataTableConfiguration V1` con le configurazioni V2, verrà visualizzato un errore HTTP 405 Method Not Allowed.

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per eliminare una configurazione della tabella di metadati in Amazon S3. Per informazioni, consulta l'[elenco degli SDK supportati](#).

Cancellazione di tabelle di metadati

Se desideri eliminare le tabelle di metadati che hai creato per un bucket generico di Amazon S3, puoi eliminare le tabelle di metadati dal bucket di tabelle gestito. AWS

Important

- L'eliminazione di una tabella è permanente e non può essere annullata. Prima di eliminare una tabella, assicurati di aver eseguito il backup dei dati importanti.

- Prima di eliminare una tabella dei metadati, è necessario eliminare la configurazione della tabella dei metadati associata nel bucket per uso generico. Per ulteriori informazioni, consulta [the section called “Cancellazione di configurazioni delle tabelle di metadati”](#).

Per eliminare il bucket di tabelle AWS gestito, consulta Eliminazione dei bucket di tabelle e nella sezione Amazon [S3 API Reference. DeleteTableBucket](#) Prima di eliminare il bucket di tabelle AWS gestito, ti consigliamo di eliminare tutte le configurazioni della tabella di metadati associate a questo bucket. È anche necessario eliminare tutte le tabelle dei metadati presenti nel bucket.

Puoi eliminare una tabella di metadati utilizzando AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Cancellazione di tabelle di metadati

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano installati e configurati AWS CLI . Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

In alternativa, puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Per eliminare una configurazione della tabella di metadati utilizzando AWS CLI

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le informazioni appropriate.

1. Usa il comando seguente per eliminare la tabella dei metadati dal bucket di tabelle gestite AWS :

```
aws s3tables delete-table \  
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/aws-s3 \  
--namespace b_general-purpose-bucket-name \  
--name journal \  
--region us-east-2
```

2. Per verificare che la tabella sia stata eliminata, usa il seguente comando:

```
aws s3tables get-table \  
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/aws-s3 \  
--namespace b_general-purpose-bucket-name \  
--name journal \  
--region us-east-2
```

Utilizzo della REST API

È possibile inviare richieste REST per eliminare la configurazione di una tabella di metadati. Per ulteriori informazioni, consulta [DeleteTable](#) nella documentazione di riferimento delle API di Amazon S3.

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per eliminare una configurazione della tabella di metadati in Amazon S3. Per informazioni, consulta l'[elenco degli SDK supportati](#) nella documentazione di riferimento delle API di Amazon S3.

Query di tabelle di metadati

Le tabelle di metadati di Amazon S3 sono archiviate in un bucket di tabelle S3 AWS gestito, che fornisce uno storage ottimizzato per i dati tabulari. Per interrogare i metadati, puoi integrare il tuo table bucket con Amazon Lakehouse. SageMaker Questa integrazione, che utilizza AWS Glue Data Catalog and AWS Lake Formation, consente ai servizi di AWS analisi di scoprire e accedere automaticamente ai dati delle tabelle.

Dopo aver integrato il table bucket con AWS Glue Data Catalog, puoi interrogare direttamente le tabelle di metadati con servizi di AWS analisi come Amazon Athena, Amazon EMR e Amazon Redshift. Puoi anche creare dashboard interattive con i dati delle tue query utilizzando Amazon Quick.

Per ulteriori informazioni sull'integrazione del bucket di tabelle S3 AWS gestito con Amazon SageMaker Lakehouse, consulta [the section called “Integrazione delle tabelle S3 con AWS i servizi di analisi”](#)

Puoi anche interrogare le tue tabelle di metadati con e qualsiasi altra applicazione che supporti il Apache Iceberg formato utilizzando l'endpoint REST Apache SparkApache Trino, l'endpoint AWS Glue Iceberg REST di Amazon S3 Tables o il catalogo Amazon S3 Tables Iceberg Catalog for client.

Apache Iceberg Per ulteriori informazioni sull'accesso alle tabelle dei metadati, consulta [the section called “Accesso alle tabelle”](#).

È possibile analizzare le tabelle dei metadati con qualsiasi motore di query che supporti il formato Apache Iceberg. Ad esempio, puoi eseguire query sulle tabelle dei metadati per effettuare quanto segue:

- Scopri i modelli e le tendenze di utilizzo dello storage
- Audit AWS Key Management Service (AWS KMS) utilizzo della chiave di crittografia tra i tuoi oggetti
- Ricerca di oggetti in base ai metadati e ai tag dell'oggetto definiti dall'utente
- Comprensione delle modifiche dei metadati degli oggetti nel tempo
- Scopri quando gli oggetti vengono aggiornati o eliminati, incluso l' Account AWS ID o l'indirizzo IP che ha effettuato la richiesta

Puoi anche unire le tabelle dei metadati gestite da S3 con tabelle dei metadati personalizzate, in modo da eseguire query su più set di dati.

Considerazioni sul prezzo delle query

Per l'esecuzione di query sulle tabelle di metadati si applica un prezzo aggiuntivo. Per ulteriori informazioni, consulta le informazioni sui prezzi del motore di query in uso.

Per informazioni su come rendere le query più efficienti dal punto di vista dei costi, consulta [Ottimizzazione delle prestazioni delle query sulle tabelle di metadati](#).

Argomenti

- [Autorizzazioni per le query sulle tabelle dei metadati](#)
- [Interrogazione delle tabelle di metadati con AWS servizi di analisi](#)
- [Query di tabelle di metadati con motori di query open-source](#)
- [Ottimizzazione delle prestazioni delle query sulle tabelle di metadati](#)
- [Esempi di query di tabelle di metadati](#)

Autorizzazioni per le query sulle tabelle dei metadati

Prima di poter eseguire query sulle tabelle di inventario in tempo reale e del diario di S3 Metadata, è necessario disporre di determinate autorizzazioni di Tabelle S3. Se le tabelle dei metadati sono state

crittografate con la crittografia lato server utilizzando AWS Key Management Service (AWS KMS) keys (SSE-KMS), devi avere anche l'`kms:Decrypt` autorizzazione per decrittografare i dati della tabella.

Quando si crea la configurazione della tabella dei metadati, le tabelle dei metadati vengono archiviate in un bucket di tabelle gestito da AWS. Tutte le configurazioni delle tabelle di metadati nel tuo account e nella stessa regione sono archiviate in un unico bucket di tabelle gestito denominato `aws-s3`.

Per eseguire query sulle tabelle dei metadati, è possibile utilizzare la seguente policy di esempio. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermissionsToQueryMetadataTables",
      "Effect": "Allow",
      "Action": [
        "s3tables:GetTable",
        "s3tables:GetTableData",
        "s3tables:GetTableMetadataLocation",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/*",
        "arn:aws:kms:us-east-1:111122223333:key/01234567-89ab-
cdef-0123-456789abcdef"
      ]
    }
  ]
}
```

Interrogazione delle tabelle di metadati con AWS servizi di analisi

Puoi interrogare le tue tabelle di metadati gestite da S3 con servizi di AWS analisi come Amazon Athena, Amazon Redshift e Amazon EMR.

Prima di poter eseguire le query, devi innanzitutto [integrare i](#) bucket di tabelle S3 AWS gestiti nella tua regione e nella tua regione con i servizi di analisi. Account AWS AWS

Query di tabelle di metadati con Amazon Athena

Dopo aver [integrato i bucket di tabelle S3 AWS gestiti](#) con i servizi di AWS analisi, puoi iniziare a interrogare le tabelle di metadati in Athena. Nelle query effettua quanto segue:

- Specifica il catalogo come `s3tablescatalog/aws-s3` e il database come `b_general-purpose-bucket-name` (che è in genere il namespace per le tabelle dei metadati).
- Assicurati di racchiudere i nomi dei namespace di tabelle dei metadati tra virgolette (") o apice inverso (`), in caso contrario la query potrebbe non funzionare.

Per ulteriori informazioni, consulta [Query di tabelle Amazon S3 con Athena](#).

Puoi eseguire query in Athena anche dalla console Amazon S3.

Utilizzo della console S3 e Amazon Athena

La procedura seguente utilizza la console Amazon S3 per accedere all'editor di query Athena in modo da poter eseguire query su una tabella con Amazon Athena.

Come eseguire query su una tabella dei metadati

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nella scheda Bucket per uso generico, scegli il bucket che contiene la configurazione dei metadati per la tabella di metadati da sottoporre a query.
4. Nella pagina dei dettagli del bucket, scegli la scheda Metadati.
5. Scegli Interroga tabella con Athena, quindi scegli una delle query di esempio per le tabelle del diario o di inventario.
6. Si apre la console Amazon Athena e viene visualizzato l'editor di query Athena con una query di esempio caricata automaticamente. Modifica questa query in base alle esigenze del caso d'uso.

Nell'editor di query, il campo Catalogo deve essere compilato con `s3tablescatalog/aws-s3`. Il campo Database deve essere compilato con lo spazio dei nomi in cui è memorizzata la tabella (ad esempio, `b_`). ***general-purpose-bucket-name***

 Note

Se non vedi questi valori nei campi **Catalogo** e **Database**, assicurati di aver integrato il bucket di tabelle AWS gestite con i servizi di AWS analisi in questa regione. Per ulteriori informazioni, consulta [the section called “Integrazione delle tabelle S3 con AWS i servizi di analisi”](#).

7. Per eseguire la query, scegli **Run** (Esegui).

 Note

- Se ricevi l'errore “Insufficient permissions to execute the query. Principal does not have any privilege on specified resource” quando provi a eseguire una query in Athena, assicurati di disporre delle necessarie autorizzazioni Lake Formation sulla tabella. Per ulteriori informazioni, consulta [the section called “Concessione dell'autorizzazione Lake Formation per una tabella o un database”](#).

Assicurati inoltre di disporre delle autorizzazioni AWS Identity and Access Management (IAM) appropriate per interrogare le tabelle di metadati. Per ulteriori informazioni, consulta [the section called “Autorizzazioni per le query sulle tabelle dei metadati”](#).

- Se ricevi l'errore «Iceberg non può accedere alla risorsa richiesta» quando provi a eseguire la query, accedi alla AWS Lake Formation console e assicurati di aver concesso le autorizzazioni per il catalogo e il database (namespace) delle tabelle che hai creato. Non specificare una tabella quando fornisci queste autorizzazioni. Per ulteriori informazioni, consulta [the section called “Concessione dell'autorizzazione Lake Formation per una tabella o un database”](#).

Query di tabelle di metadati con Amazon Redshift

Dopo aver [integrato i bucket di tabelle S3 AWS gestiti](#) con AWS i servizi di analisi, procedi come segue:

- [Crea un collegamento alle risorse](#) per il namespace di tabelle dei metadati (in genere `b_general_purpose_bucket_name`).

- Assicurati di racchiudere i nomi dei namespace di tabelle dei metadati tra virgolette (") o apice inverso (`), in caso contrario la query potrebbe non funzionare.

Al termine, puoi iniziare a eseguire query sulle tabelle dei metadati nella console di Amazon Redshift. Per ulteriori informazioni, consulta [Accesso alle tabelle Amazon S3 con Amazon Redshift](#).

Query di tabelle di metadati con Amazon EMR

Per eseguire query sulle tabelle dei metadati utilizzando Amazon EMR, crei un cluster Amazon EMR configurato per Apache Iceberg e lo colleghi alle tabelle dei metadati utilizzando Apache Spark. Puoi configurarlo integrando i bucket di tabelle S3 AWS gestiti con i servizi di AWS analisi o utilizzando il catalogo open source Amazon S3 Tables Catalog for client. Iceberg

Note

Quando si utilizza Apache Spark su Amazon EMR o altri motori di terze parti per eseguire query sulle tabelle dei metadati, è consigliabile utilizzare l'endpoint REST Iceberg di Tabelle Amazon S3. La query potrebbe non funzionare correttamente se non utilizzi questo endpoint. Per ulteriori informazioni, consulta [the section called "Accesso alle tabelle utilizzando l'endpoint Iceberg REST di Tabelle Amazon S3"](#).

Per ulteriori informazioni, consulta [Accesso alle tabelle Amazon S3 con Amazon EMR](#).

Query di tabelle di metadati con motori di query open-source

È possibile eseguire query sulle tabelle dei metadati gestite da S3 utilizzando motori di query open-source, come Apache Spark. Quando si utilizza Apache Spark su Amazon EMR o altri motori di terze parti per eseguire query sulle tabelle dei metadati, è consigliabile utilizzare l'endpoint REST Iceberg di Tabelle Amazon S3. La query potrebbe non funzionare correttamente se non utilizzi questo endpoint. Per ulteriori informazioni, consulta [the section called "Accesso alle tabelle utilizzando l'endpoint Iceberg REST di Tabelle Amazon S3"](#).

Ottimizzazione delle prestazioni delle query sulle tabelle di metadati

Poiché S3 Metadata si basa sul formato di tabella Apache Iceberg, è possibile ottimizzare le prestazioni e i [costi](#) delle query sulle tabelle del diario utilizzando intervalli di tempo specifici.

Ad esempio, la seguente query SQL fornisce il livello di sensibilità dei nuovi oggetti in un bucket per uso generico S3:


```
SELECT key, object_tags['SensitivityLevel']  
FROM "b_general-purpose-bucket-name".journal"  
WHERE record_type = 'CREATE'  
GROUP BY object_tags['SensitivityLevel']
```

Questa query esegue la scansione dell'intera tabella del diario, il che potrebbe richiedere molto tempo. Per migliorare le prestazioni, è possibile includere la colonna `record_timestamp` per concentrarsi su un intervallo di tempo specifico. È inoltre consigliabile utilizzare il nome di tabella completo, che puoi trovare nella console Amazon S3 nella pagina dei dettagli di configurazione dei metadati della scheda Metadati del bucket per uso generico. Ecco una versione aggiornata della precedente query che analizza i nuovi oggetti dell'ultimo mese:

```
SELECT key, object_tags['SensitivityLevel']  
FROM b_general-purpose-bucket-name".aws-s3.b_general-purpose-bucket-name.journal"  
WHERE record_type = 'CREATE'  
AND record_timestamp > (CURRENT_TIMESTAMP - interval '1' month)  
GROUP BY object_tags['SensitivityLevel']
```

Per migliorare le prestazioni delle query sulle tabelle di inventario, assicurati di eseguirle solo sul numero minimo di colonne necessarie.

Esempi di query di tabelle di metadati

Gli esempi seguenti mostrano come sia possibile ottenere informazioni di diverso tipo dalle tabelle dei metadati S3 utilizzando query SQL standard.

Quando utilizzi questi esempi, ricorda che:

- Gli esempi sono scritti per funzionare con Amazon Athena. Potrebbe essere necessario modificare gli esempi per lavorare con un motore di query diverso.
- Assicurati di capire come [ottimizzare le query](#).
- Sostituisci `b_general-purpose-bucket-name` con il nome del namespace.
- Per l'elenco completo delle colonne supportate, consulta [Schema delle tabelle del diario di S3 Metadata](#) e [the section called "Schema delle tabelle di inventario in tempo reale"](#).

Indice

- [Query sulle tabelle del diario di esempio](#)

- [Ricerca di oggetti per estensione di file](#)
- [Elenco delle eliminazioni di oggetti](#)
- [Elenco AWS KMS chiavi di crittografia utilizzate dai tuoi oggetti](#)
- [Elenco di oggetti che non utilizzano le chiavi KMS](#)
- [Elenco AWS KMS chiavi di crittografia utilizzate per le operazioni PUT negli ultimi 7 giorni](#)
- [Elenco degli oggetti eliminati nelle ultime 24 ore dal ciclo di vita S3](#)
- [Visualizzazione dei metadati forniti da Amazon Bedrock](#)
- [Comprensione dello stato attuale degli oggetti](#)
- [Query sulle tabelle di inventario di esempio](#)
 - [Individuazione dei set di dati che utilizzano tag specifici](#)
 - [Elencare oggetti non crittografati con SSE-KMS](#)
 - [Elenco degli oggetti non crittografati](#)
 - [Elenco degli oggetti generati da Amazon Bedrock](#)
 - [Riconciliazione della tabella di inventario con la tabella del diario](#)
 - [Individuazione delle versioni correnti degli oggetti](#)
- [Query di esempio nella tabella di annotazione](#)
 - [Elenca tutte le annotazioni per un oggetto specifico](#)
 - [Ricerca di tutti gli oggetti con un'annotazione specifica](#)
 - [Unire la tabella delle annotazioni alla tabella dell'inventario](#)
- [Unione di metadati personalizzati con le tabelle di metadati S3](#)
- [Visualizzazione dei dati della tabella di metadati con Amazon Quick](#)

Query sulle tabelle del diario di esempio

È possibile utilizzare le seguenti query di esempio per eseguire query sulle tabelle del diario.

Ricerca di oggetti per estensione di file

La seguente query restituisce gli oggetti con una specifica estensione di file (in questo caso .jpg):

```
SELECT key FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal"  
WHERE key LIKE '%.jpg'  
AND record_type = 'CREATE'
```

Elenco delle eliminazioni di oggetti

La seguente query restituisce gli eventi di eliminazione degli oggetti, incluso l' Account AWS ID o l'entità del AWS servizio che ha effettuato la richiesta:

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp, requester,  
    source_ip_address, version_id  
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal"  
WHERE record_type = 'DELETE';
```

Elenco AWS KMS chiavi di crittografia utilizzate dai tuoi oggetti

La seguente query restituisce gli ARN delle chiavi AWS Key Management Service (AWS KMS) che crittografano gli oggetti:

```
SELECT DISTINCT kms_key_arn  
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal";
```

Elenco di oggetti che non utilizzano le chiavi KMS

La seguente query restituisce oggetti che non sono crittografati con AWS KMS chiavi:

```
SELECT DISTINCT kms_key_arn  
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal"  
WHERE encryption_status NOT IN ('SSE-KMS', 'DSSE-KMS')  
AND record_type = 'CREATE';
```

Elenco AWS KMS chiavi di crittografia utilizzate per **le operazioni** PUT negli ultimi 7 giorni

La seguente query restituisce gli ARN delle chiavi AWS Key Management Service (AWS KMS) che crittografano gli oggetti:

```
SELECT DISTINCT kms_key_arn  
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal"  
WHERE record_timestamp > (current_date - interval '7' day)  
AND kms_key_arn is NOT NULL;
```

Elenco degli oggetti eliminati nelle ultime 24 ore dal ciclo di vita S3

La seguente query restituisce l'elenco degli oggetti scaduti nell'ultimo giorno del ciclo di vita S3:

```
SELECT bucket, key, version_id, last_modified_date, record_timestamp, requester
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal"
WHERE requester = 's3.amazonaws.com'
AND record_type = 'DELETE'
AND record_timestamp > (current_date - interval '1' day)
```

Visualizzazione dei metadati forniti da Amazon Bedrock

Alcuni AWS servizi (come [Amazon Bedrock](#)) caricano oggetti su Amazon S3. È possibile interrogare i metadati degli oggetti forniti da questi servizi. Ad esempio, la seguente query include la colonna `user_metadata` per determinare se vi sono oggetti caricati da Amazon Bedrock in un bucket per uso generico:

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp,
  user_metadata
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal"
WHERE record_type = 'CREATE'
AND user_metadata['content-source'] = 'AmazonBedrock';
```

Se Amazon Bedrock ha caricato un oggetto nel bucket, la colonna `user_metadata` mostrerà i seguenti metadati associati all'oggetto nel risultato della query:

```
user_metadata
{content-additional-params -> requestid="CVK8FWYRW0M9JW65",
  signedContentSHA384="38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe",
  content-model-id -> bedrock-model-arn, content-source -> AmazonBedrock}
```

Comprensione dello stato attuale degli oggetti

La seguente query può aiutare a determinare lo stato attuale degli oggetti. La query identifica la versione più recente di ogni oggetto, filtra gli oggetti eliminati e contrassegna la versione più recente di ogni oggetto in base ai numeri di sequenza. I risultati sono ordinati in base alle colonne `bucket`, `key` e `sequence_number`.

```
WITH records_of_interest as (
  -- Start with a query that can narrow down the records of interest.
  SELECT * from "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal"
),

version_stacks as (
  SELECT *,
```

```

        -- Introduce a column called 'next_sequence_number', which is the next larger
        -- sequence_number for the same key version_id in sorted order.
        LEAD(sequence_number, 1) over (partition by (bucket, key,
coalesce(version_id, '')) order by sequence_number ASC) as next_sequence_number
    from records_of_interest
),

-- Pick the 'tip' of each version stack triple: (bucket, key, version_id).
-- The tip of the version stack is the row of that triple with the largest sequencer.
-- Selecting only the tip filters out any row duplicates.
-- This isn't typical, but some events can be delivered more than once to the table
-- and include rows that might no longer exist in the bucket (since the
-- table contains rows for both extant and extinct objects).
-- In the next subquery, eliminate the rows that contain deleted objects.
current_versions as (
    SELECT * from version_stacks where next_sequence_number is NULL
),

-- Eliminate the rows that are extinct from the bucket by filtering with
-- record_type. An object version has been deleted from the bucket if its tip is
-- record_type==DELETE.
existing_current_versions as (
    SELECT * from current_versions where not (record_type = 'DELETE' and
is_delete_marker = FALSE)
),

-- Optionally, to determine which of several object versions is the 'latest',
-- you can compare their sequence numbers. A version_id is the latest if its
-- tip's sequencer is the largest among all other tips in the same key.
with_is_latest as (
    SELECT *,
        -- Determine if the sequence_number of this row is the same as the largest
        sequencer for the key that still exists.
        sequence_number = (MAX(sequence_number) over (partition by (bucket, key)))
    as is_latest_version
    FROM existing_current_versions
)

SELECT * from with_is_latest
ORDER BY bucket, key, sequence_number;

```

Query sulle tabelle di inventario di esempio

È possibile utilizzare le seguenti query di esempio per eseguire query sulle tabelle di inventario.

Individuazione dei set di dati che utilizzano tag specifici

La query seguente restituisce il set di dati che utilizza i tag specificati:

```
SELECT *  
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."inventory"  
WHERE object_tags['key1'] = 'value1'  
AND object_tags['key2'] = 'value2';
```

Elencare oggetti non crittografati con SSE-KMS

La seguente query restituisce oggetti non crittografati con SSE-KMS:

```
SELECT key, encryption_status  
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."inventory"  
WHERE encryption_status != 'SSE-KMS';
```

Elenco degli oggetti non crittografati

La seguente query restituisce gli oggetti non crittografati:

```
SELECT bucket, key, version_id  
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."inventory"  
WHERE encryption_status IS NULL;
```

Elenco degli oggetti generati da Amazon Bedrock

La seguente query elenca gli oggetti generati da Amazon Bedrock:

```
SELECT DISTINCT bucket, key, sequence_number, user_metadata  
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."inventory"  
WHERE user_metadata['content-source'] = 'AmazonBedrock';
```

Riconciliazione della tabella di inventario con la tabella del diario

La seguente query genera un elenco simile a una tabella di inventario aggiornato con il contenuto corrente del bucket. Più precisamente, l'elenco risultante combina l'ultimo snapshot della tabella di inventario con gli eventi più recenti della tabella del diario.

Affinché questa query produca risultati accurati, sia la tabella del diario che quella di inventario devono essere nello stato Attivo.

È consigliabile utilizzare questa query per bucket per uso generico contenenti meno di un miliardo (10^9) di oggetti.

Questa query di esempio applica le seguenti semplificazioni ai risultati dell'elenco (rispetto alla tabella di inventario):

- Omissioni di colonne: le colonne `bucket`, `is_multipart`, `encryption_status`, `is_bucket_key_enabled`, `kms_key_arn` e `checksum_algorithm` non fanno parte dei risultati finali. Mantenendo al minimo il numero di colonne facoltative si migliorano le prestazioni.
- Inclusione di tutti i record: la query restituisce tutte le chiavi e le versioni degli oggetti, inclusa la versione null (in bucket senza controllo delle versioni o con controllo delle versioni sospeso) e gli indicatori di eliminazione. Per esempi su come filtrare i risultati per mostrare solo le chiavi che ti interessano, vedi la clausola `WHERE` alla fine della query.
- Riconciliazione accelerata: la query potrebbe, in rari casi, includere temporaneamente oggetti che non sono più nel bucket. Queste discrepanze vengono eliminate non appena diventa disponibile il successivo snapshot della tabella di inventario. Questo comportamento è un compromesso tra prestazioni e precisione.

Per eseguire questa query in Amazon Athena, assicurati di selezionare il catalogo `s3tablescatalog/aws-s3` e il database `b_`*general-purpose-bucket-name* per la configurazione dei metadati del bucket per uso generico che contiene le tabelle del diario e di inventario.

```
WITH inventory_time_cte AS (  
    SELECT COALESCE(inventory_time_from_property, inventory_time_default) AS  
    inventory_time FROM  
    (  
        SELECT * FROM  
        (VALUES (TIMESTAMP '2024-12-01 00:00')) AS T (inventory_time_default)  
        LEFT OUTER JOIN  
        (  
            SELECT from_unixtime(CAST(value AS BIGINT) / 1000.0) AS  
            inventory_time_from_property FROM "journal$properties"  
            WHERE key = 'aws.s3metadata.oldest-uncoalesced-record-timestamp' LIMIT 1  
        )  
        ON TRUE  
    )  
)  
,
```

```
working_set AS (  
    SELECT  
        key,  
        sequence_number,  
        version_id,  
        is_delete_marker,  
        size,  
        COALESCE(last_modified_date, record_timestamp) AS last_modified_date,  
        e_tag,  
        storage_class,  
        object_tags,  
        user_metadata,  
        (record_type = 'DELETE' AND NOT COALESCE(is_delete_marker, FALSE)) AS  
_is_perm_delete  
    FROM journal j  
    CROSS JOIN inventory_time_cte t  
    WHERE j.record_timestamp > (t.inventory_time - interval '15' minute)  
  
    UNION ALL  
  
    SELECT  
        key,  
        sequence_number,  
        version_id,  
        is_delete_marker,  
        size,  
        last_modified_date,  
        e_tag,  
        storage_class,  
        object_tags,  
        user_metadata,  
        FALSE AS _is_perm_delete  
    FROM inventory i  
) ,  
  
updated_inventory AS (  
    SELECT * FROM (  
        SELECT *,  
            MAX(sequence_number) OVER (PARTITION BY key, version_id) AS _supremum_sn  
        FROM working_set  
    )  
    WHERE sequence_number = _supremum_sn  
)
```



```
SELECT
    key,
    sequence_number,
    version_id,
    is_delete_marker,
    size,
    last_modified_date,
    e_tag,
    storage_class,
    object_tags,
    user_metadata
FROM updated_inventory
-- This filter omits only permanent deletes from the results. Delete markers will still
   be shown.
WHERE NOT _is_perm_delete
-- You can add additional filters here. Examples:
--     AND object_tags['department'] = 'billing'
--     AND starts_with(key, 'reports/')
ORDER BY key ASC, sequence_number DESC;
```

Individuazione delle versioni correnti degli oggetti

La seguente query utilizza la tabella di inventario per generare una nuova tabella di output che mostra le versioni correnti degli oggetti. La tabella di output è intenzionalmente simile a un report di Inventario S3. La tabella di output include un campo `is_latest` che indica se l'oggetto è alla versione corrente. Il `is_latest` campo è equivalente al `IsLatest` campo in un report [di inventario S3](#).

Questa query funziona per bucket per uso generico con [Controllo delle versioni S3](#) nello stato di controllo delle versioni abilitato o di controllo delle versioni sospeso.

Prerequisiti

La query restituisce i risultati in una nuova tabella S3 per supportare ulteriori query e per ottenere prestazioni più elevate rispetto all'output di righe sullo schermo. Pertanto, prima di eseguire questa query, assicurati che siano soddisfatte le seguenti condizioni. Se scegli di non inviare i risultati in una nuova tabella, puoi saltare queste fasi.

- È necessario disporre di un bucket di tabelle gestito dal cliente esistente con un namespace esistente come posizione in cui generare la nuova tabella. Per ulteriori informazioni, consulta [the section called “Creare un bucket di tabelle”](#) e [the section called “Creare un namespace”](#).

- Per eseguire query sulla nuova tabella di output, è necessario configurare un metodo di accesso per le query. Per ulteriori informazioni, consulta [the section called “Accesso alle tabelle”](#). Se desideri interrogare la tabella di output con servizi di AWS analisi come Amazon Athena, il bucket di tabelle gestito dal cliente deve essere integrato con i servizi di analisi. AWS Per ulteriori informazioni, consulta [the section called “Panoramica dell'integrazione di Tabelle S3”](#).

Per utilizzare questa query, sostituisci *amzn-s3-demo-table-bucket* con il nome del bucket di tabelle gestito dal cliente esistente in cui desideri creare la nuova tabella di output. Sostituisci *existing_namespace* con il nome del namespace in cui desideri creare la tabella di output nel bucket di tabelle. Sostituisci *new_table* con il nome che desideri utilizzare per la tabella di output. Assicurati che il nome della tabella di output segua le [regole di denominazione delle tabelle](#).

Per eseguire questa query in Amazon Athena, assicurati di selezionare il catalogo `s3tablescatalog/aws-s3` e il database `b_`*general-purpose-bucket-name* per la configurazione dei metadati del bucket per uso generico che contiene la tabella di inventario.

```
-- If you don't want to output the results to a new table, remove the following two
lines
-- (everything before the WITH clause).
CREATE TABLE "s3tablescatalog/amzn-s3-demo-table-
bucket"."existing_namespace"."new_table"
as (
WITH
my_inventory AS (
    SELECT
        bucket,
        key,
        version_id,
        sequence_number,
        is_delete_marker,
        size,
        last_modified_date,
        storage_class
    FROM inventory
-- For prefix filtering, use a WHERE clause with % at the end.
--     WHERE key LIKE 'prefix%'
),

inventory_with_is_latest as (
SELECT *,
    ROW_NUMBER() OVER (
```

```
        PARTITION BY key
        ORDER BY sequence_number DESC
    ) = 1 AS is_latest
FROM my_inventory
    )

SELECT
    bucket,
    key,
    version_id,
    sequence_number,
    is_delete_marker,
    size,
    last_modified_date,
    storage_class,
    is_latest

FROM inventory_with_is_latest

-- If you want only the current version of each key, uncomment the following WHERE
-- clause.
-- WHERE is_latest = TRUE
-- If you aren't outputting the results to a new table, remove the next line:
);
```

Query di esempio nella tabella di annotazione

Se hai abilitato una tabella di annotazione nella configurazione dei metadati di S3, puoi interrogare i dati delle annotazioni utilizzando Athena o altri servizi di analisi che supportano le tabelle. Apache Iceberg La tabella di annotazione utilizza la convenzione di denominazione. "s3tablescatalog/aws-s3"."b_*bucket-name*". "annotation"

Elenca tutte le annotazioni per un oggetto specifico

La seguente query restituisce tutte le annotazioni per un oggetto specifico:

```
SELECT name, size, last_modified_date, replication_status
FROM "s3tablescatalog/aws-s3"."b_amzn-s3-demo-bucket". "annotation"
WHERE object_key = 'documents/report.pdf'
ORDER BY name
```

Ricerca di tutti gli oggetti con un'annotazione specifica

La seguente query restituisce tutti gli oggetti con un'annotazione specifica:

```
SELECT object_key, object_version_id, size, last_modified_date
FROM "s3tablescatalog/aws-s3"."b_amzn-s3-demo-bucket"."annotation"
WHERE name = 'classification'
ORDER BY last_modified_date DESC
```

Unire la tabella delle annotazioni alla tabella dell'inventario

La seguente query unisce la tabella delle annotazioni alla tabella dell'inventario per combinare i dati delle annotazioni con i metadati dell'inventario:

```
SELECT i.key, i.storage_class, a.name, a.size, a.text_value
FROM "s3tablescatalog/aws-s3"."b_amzn-s3-demo-bucket"."inventory" i
JOIN "s3tablescatalog/aws-s3"."b_amzn-s3-demo-bucket"."annotation" a
  ON i.bucket = a.bucket
  AND i.key = a.object_key
  AND i.object_join_key = a.object_join_key
WHERE a.name = 'classification'
LIMIT 10
```

Utilizza la `object_join_key` colonna per unire le tabelle di annotazione e di inventario per garantire la coerenza. Questa colonna contiene un identificatore univoco per l'oggetto, assegnato con ogni nuova versione o quando viene creata o sovrascritta la versione nulla. Garantisce che la riga di annotazione corrisponda allo stato corretto della versione dell'oggetto.

Unione di metadati personalizzati con le tabelle di metadati S3

Puoi analizzare i dati nelle tabelle di metadati AWS gestite e nelle tabelle di metadati dei clienti (autogestite). Utilizzando un operatore SQL standard JOIN, è possibile interrogare i dati provenienti da più fonti.

L'esempio seguente di query SQL trova i record corrispondenti tra una tabella di journal AWS gestita ("journal") e una tabella di metadati autogestita (`my_self_managed_metadata_table`). La query filtra anche le informazioni in base agli eventi CREATE, che indicano che un nuovo oggetto (o una nuova versione dell'oggetto) è stato scritto nel bucket. (Per ulteriori informazioni, consulta la [Schema delle tabelle del diario di S3 Metadata](#).)

```
SELECT *
```

```
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "journal" a
JOIN "my_namespace". "my_self_managed_metadata_table" b
ON a.bucket = b.bucket AND a.key = b.key AND a.version_id = b.version_id
WHERE a.record_type = 'CREATE';
```

L'esempio seguente di query SQL trova i record corrispondenti tra una tabella di inventario AWS gestita ("inventory") e una tabella di metadati autogestita ():

my_self_managed_metadata_table

```
SELECT *
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name". "inventory" a
JOIN "my_namespace". "my_self_managed_metadata_table" b
ON a.bucket = b.bucket AND a.key = b.key AND a.version_id = b.version_id;
```

Visualizzazione dei dati della tabella di metadati con Amazon Quick

Con Amazon Quick, puoi creare dashboard interattive per analizzare e visualizzare i risultati delle query SQL sulle tabelle di metadati gestite da S3. Le dashboard rapide possono aiutarti a monitorare le statistiche, tenere traccia delle modifiche e ottenere informazioni operative sulle tabelle di metadati.

Una dashboard sulla tabella del diario può mostrare:

- Qual è la percentuale di caricamenti di oggetti rispetto alle eliminazioni?
- Quali oggetti sono stati eliminati nelle ultime 24 ore dal ciclo di vita S3?
- Da quali indirizzi IP provengono le richieste PUT più recenti?

Una dashboard sulla tabella di inventario può mostrare:

- Quanti oggetti sono presenti nelle diverse classi di storage?
- Quale percentuale dei dati di archiviazione è costituita da oggetti di piccole dimensioni rispetto a quelli di grandi dimensioni?
- Quali tipi di oggetti sono presenti nel bucket?

Dopo aver [integrato i bucket di tabelle S3](#) con i servizi di AWS analisi, puoi creare set di dati dalle tabelle di metadati e utilizzarli in Amazon Quick utilizzando SPICE o indirizzando le query SQL dal tuo motore di query. Quick supporta Amazon Athena e Amazon Redshift come fonti di dati.

Per ulteriori informazioni, consulta [Visualizzazione dei dati delle tabelle con Amazon Quick](#).

Risoluzione dei problemi relativi a S3 Metadata

Le seguenti informazioni ti consentono di diagnosticare e risolvere i problemi comuni che potresti incontrare quando utilizzi Amazon S3 Metadata.

Non riesco a eliminare il mio AWS bucket di tabelle e tabelle di metadati gestiti

Prima di poter eliminare una tabella di metadati, è necessario eliminare la configurazione della tabella di metadati associata sul bucket per uso generico. Per ulteriori informazioni, consulta [the section called “Cancellazione di configurazioni delle tabelle di metadati”](#).

Prima di poter eliminare il bucket di tabelle AWS gestite, è necessario eliminare tutte le configurazioni della tabella di metadati associate a questo bucket e tutte le tabelle di metadati nel bucket. Per ulteriori informazioni, consulta [the section called “Cancellazione di configurazioni delle tabelle di metadati”](#) e [the section called “Cancellazione di tabelle di metadati”](#).

Non riesco a impostare o modificare le impostazioni di crittografia per il mio AWS tabella di metadati gestita

Quando crei la configurazione della tabella dei metadati, puoi scegliere di crittografare le tabelle di metadati AWS gestite con la crittografia lato server utilizzando le chiavi (). AWS Key Management Service AWS KMS SSE-KMS Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket generico. È possibile impostare il tipo di crittografia per le tabelle solo durante la creazione della tabella. Dopo aver creato una tabella gestita da AWS , non è possibile modificarne le impostazioni di crittografia. SSE-KMS Per specificare le tabelle di metadati, devi disporre di determinate autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni per SSE-KMS](#)

L'impostazione di crittografia per una tabella dei metadati ha la precedenza sull'impostazione di crittografia predefinita a livello di bucket. Se non specifichi la crittografia, la tabella erediterà l'impostazione di crittografia predefinita del bucket.

Per impostazione predefinita, i bucket di tabelle AWS gestiti sono crittografati con crittografia lato server utilizzando chiavi gestite Amazon S3 (). SSE-S3 Dopo aver creato la prima configurazione dei metadati, puoi impostare l'impostazione di crittografia predefinita per il bucket di tabelle AWS gestite in modo che utilizzi la crittografia lato server con () keys (). AWS Key Management Service AWS KMS SSE-KMS Per ulteriori informazioni, vedere [Crittografia per AWS i bucket di tabelle gestiti e the section called “Specificando SSE-KMS”](#)

Quando provo a ricreare la configurazione della tabella dei metadati, ricevo un errore

L'eliminazione della configurazione della tabella dei metadati elimina solo la configurazione. Il bucket di tabelle AWS gestite e le tabelle di metadati esistono ancora, anche se si elimina la configurazione della tabella di metadati.

Se elimini la configurazione della tabella di metadati e desideri ricreare una configurazione per lo stesso bucket generico, devi prima eliminare manualmente le vecchie tabelle di diario, inventario e annotazioni dal bucket di tabelle gestito. AWS In caso contrario, la creazione della nuova configurazione della tabella dei metadati non riesce perché tali tabelle esistono già.

Per eliminare le tabelle dei metadati, consulta [the section called “Cancellazione di tabelle di metadati”](#).

Non riesco ad abilitare una tabella di inventario nella configurazione

Se la configurazione di S3 Metadata è stata creata prima del 15 luglio 2025, non puoi abilitare una tabella di inventario su quella configurazione. È consigliabile eliminare e ricreare la configurazione in modo da poter creare una tabella di inventario e impostare la scadenza dei record della tabella del diario. Per ulteriori informazioni, consulta [the section called “Abilitazione delle tabelle di inventario e annotazione sulle configurazioni di metadati create prima del 15 luglio 2025”](#).

Non riesco ad abilitare una tabella di annotazioni sulla mia configurazione

Se hai creato la configurazione dei metadati S3 prima del 15 luglio 2025, non puoi abilitare una tabella di annotazioni su quella configurazione. Ti consigliamo di eliminare e ricreare la configurazione in modo da poter creare una tabella di annotazioni, creare una tabella di inventario e far scadere i record della tabella del diario. Per ulteriori informazioni, consulta [the section called “Abilitazione delle tabelle di inventario e annotazione sulle configurazioni di metadati create prima del 15 luglio 2025”](#).

Non riesco ad abilitare la scadenza dei record della tabella del diario nella configurazione

Se la configurazione di S3 Metadata è stata creata prima del 15 luglio 2025, non puoi abilitare la scadenza dei record della tabella del diario su quella configurazione. È consigliabile eliminare e ricreare la configurazione in modo da poter impostare la scadenza dei record della tabella del diario e creare una tabella di inventario. Per ulteriori informazioni, consulta [the section called “Abilitazione delle tabelle di inventario e annotazione sulle configurazioni di metadati create prima del 15 luglio 2025”](#).

Non riesco a eseguire query sulle tabelle dei metadati

Se non riesci a eseguire query sulle tabelle dei metadati, verifica quanto segue:

- Quando si utilizza Amazon Athena o Amazon Redshift per eseguire query sulle tabelle dei metadati, è necessario racchiudere i nomi dei namespace di tabelle dei metadati tra virgolette (") o apici inversi (`), altrimenti la query potrebbe non funzionare.
- Quando si utilizza Apache Spark su Amazon EMR o altri motori di terze parti per eseguire query sulle tabelle dei metadati, è consigliabile utilizzare l'endpoint REST Iceberg di Tabelle Amazon S3. La query potrebbe non funzionare correttamente se non utilizzi questo endpoint. Per ulteriori informazioni, consulta [the section called "Accesso alle tabelle utilizzando l'endpoint Iceberg REST di Tabelle Amazon S3"](#).
- Assicurati di disporre delle autorizzazioni AWS Identity and Access Management (IAM) appropriate per interrogare le tabelle di metadati. Per ulteriori informazioni, consulta [the section called "Autorizzazioni per le query sulle tabelle dei metadati"](#).
- Se utilizzi Amazon Athena e ricevi errori quando provi a eseguire le query, procedi come segue:
 - Se ricevi l'errore "Insufficient permissions to execute the query. Principal does not have any privilege on specified resource" quando provi a eseguire una query in Athena, assicurati di disporre delle necessarie autorizzazioni Lake Formation sulla tabella. Per ulteriori informazioni, consulta [the section called "Concessione dell'autorizzazione Lake Formation per una tabella o un database"](#).
 - Se ricevi l'errore «Iceberg non può accedere alla risorsa richiesta» quando provi a eseguire la query, accedi alla AWS Lake Formation console e assicurati di esserti concesso le autorizzazioni per il catalogo e il database (namespace) delle tabelle che hai creato. Non specificare una tabella quando fornisci queste autorizzazioni. Per ulteriori informazioni, consulta [the section called "Concessione dell'autorizzazione Lake Formation per una tabella o un database"](#).

Ricevo 405 errori quando cerco di utilizzare determinati metadati S3 AWS CLI comandi e operazioni API

La chiamata all'operazione GetBucketMetadataTableConfiguration API V1 o l'utilizzo del comando get-bucket-metadata-table-configuration AWS Command Line Interface (AWS CLI) su una configurazione della tabella di metadati V2 genera un errore HTTP. 405 Method Not Allowed Allo stesso modo, anche la chiamata all'operazione DeleteBucketMetadataTableConfiguration API V1 o l'utilizzo del delete-bucket-metadata-table-configuration AWS CLI comando causa un errore 405.

È possibile utilizzare l'operazione `GetBucketMetadataConfiguration` API V2 o il `get-bucket-metadata-configuration` AWS CLI comando su una configurazione della tabella di metadati V1 o V2. Allo stesso modo, è possibile utilizzare l'operazione `DeleteBucketMetadataConfiguration` API V2 o il `delete-bucket-metadata-configuration` AWS CLI comando su una configurazione di tabella di metadati V1 o V2.

È consigliabile aggiornare i processi per utilizzare le nuove operazioni API V2 (`CreateBucketMetadataConfiguration`, `GetBucketMetadataConfiguration` e `DeleteBucketMetadataConfiguration`) anziché le operazioni API V1. Per ulteriori informazioni sulla migrazione dalla V1 di S3 Metadata alla V2, consulta [the section called “Abilitazione delle tabelle di inventario e annotazione sulle configurazioni di metadati create prima del 15 luglio 2025”](#).

Per determinare se la configurazione è V1 o V2, puoi esaminare il seguente attributo della risposta dell'API `GetBucketMetadataConfiguration`. Un tipo di bucket AWS gestito ("aws") indica una configurazione V2 e un tipo di bucket gestito dal cliente () indica una configurazione V1. "customer"

```
"MetadataTableConfigurationResult": {  
    "TableBucketType": ["aws" | "customer"]
```

Per ulteriori informazioni, consulta [the section called “Visualizzazione delle configurazioni delle tabelle dei metadati”](#).

Caricamento degli oggetti

Quando un file viene caricato in Amazon S3, viene archiviato come oggetto S3. Gli oggetti sono composti dai dati e dai metadati dei file che descrivono l'oggetto. Un bucket può avere un numero illimitato di oggetti. Per caricare file e cartelle in un bucket Amazon S3, è necessario disporre delle autorizzazioni in scrittura per il bucket. Per ulteriori informazioni sulle autorizzazioni di accesso, consultare [Identity and Access Management per Amazon S3](#).

In un bucket S3 è possibile caricare qualsiasi tipo di file: immagini, backup, dati, film e così via. La dimensione massima di un file che è possibile caricare utilizzando la console di Amazon S3 è 160 GB. Per caricare un file di dimensioni superiori a 160 GB, utilizza AWS Command Line Interface (AWS CLI), AWS SDK o l'API REST di Amazon S3.

Se si carica un oggetto con un nome della chiave già esistente in un bucket che supporta la funzione Controllo delle versioni, Amazon S3 crea un'altra versione dell'oggetto anziché sostituire l'oggetto esistente. Per ulteriori informazioni sull'abilitazione del controllo delle versioni, consulta [Abilitazione della funzione Controllo delle versioni sui bucket](#).

A seconda della dimensione dei dati da caricare, in Amazon S3 sono disponibili le seguenti opzioni:

- Carica un oggetto in un'unica operazione utilizzando AWS gli SDK, l'API REST oppure AWS CLI: con una singola PUT operazione, puoi caricare un singolo oggetto di dimensioni fino a 5 GB.
- Carica un singolo oggetto tramite la console di Amazon S3: con la console di Amazon S3, è possibile caricare un singolo oggetto fino a 160 GB di dimensioni.
- Carica un oggetto in parti utilizzando AWS gli SDK, l'API REST oppure AWS CLI: utilizzando l'operazione API di caricamento in più parti, puoi caricare un singolo oggetto di grandi dimensioni, fino a 50 TB di dimensione.

L'operazione API per il caricamento in più parti è concepita per migliorare l'esperienza di caricamento per gli oggetti di dimensioni maggiori. È possibile caricare un oggetto in parti. Queste parti possono essere caricate in modo indipendente, in qualsiasi ordine e in parallelo. Puoi utilizzare un caricamento in più parti per oggetti di dimensioni comprese tra 5 MB e 50 TB. Per ulteriori informazioni, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Per caricare file di dimensioni superiori a 5 TB, utilizza S3 Transfer Manager in Java v1/v2, Python o SDK. AWS CLI Per ottenere prestazioni ottimali, utilizzate la versione più recente di AWS Common Runtime (CRT) con questi SDK, che è stata ottimizzata per un migliore utilizzo delle risorse.

Quando si caricano oggetti di grandi dimensioni da un flusso di memoria, il CRT memorizza in buffer ogni parte fino a 5 GB di memoria, limitando il throughput complessivo in base alla memoria allocata. È possibile regolare il limite di memoria CRT utilizzando opzioni di configurazione come Java SDK. `maxNativeMemoryLimitInBytes` Per i caricamenti da disco, CRT passa automaticamente allo streaming diretto su disco anziché al buffering delle parti intermedie, migliorando l'utilizzo della memoria. Questo comportamento è abilitato automaticamente per oggetti di grandi dimensioni, ma può essere abilitato anche per file più piccoli tramite parametri di richiesta come `should_stream` per AWS CLI e `CRT_MEMORY_BUFFER_DISABLED` per Java SDK.

Quando carichi un oggetto, l'oggetto viene automaticamente crittografato utilizzando la crittografia lato server con chiavi gestite da Amazon S3 () SSE-S3 per impostazione predefinita. Quando lo scarichi, l'oggetto viene decrittato. Per ulteriori informazioni, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#) e [Protezione dei dati con la crittografia](#).

Quando carichi un oggetto, se desideri utilizzare un diverso tipo di crittografia predefinita, puoi anche specificare la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-

KMS) nelle PUT richieste S3 o impostare la configurazione di crittografia predefinita nel bucket di destinazione da utilizzare per crittografare i dati. SSE-KMS Per ulteriori informazioni su, consulta. SSE-KMS [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#) Se desideri utilizzare una chiave KMS di proprietà di un account diverso, devi avere l'autorizzazione necessaria per l'uso della chiave. Per ulteriori informazioni sulle autorizzazioni tra account per le chiavi KMS, vedi [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Se si verifica un errore di Accesso negato (403 Forbidden) in Amazon S3, consulta [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#) per saperne di più sulle cause comuni.

Caricamento di un oggetto

Utilizzo della console S3

Questa procedura spiega come caricare oggetti e cartelle in un bucket Amazon S3 utilizzando la console.

Quando carichi un oggetto, il nome della chiave oggetto è costituito dal nome del file e da qualsiasi prefisso facoltativo. Nella console di Amazon S3, puoi creare cartelle per organizzare i tuoi oggetti. In Amazon S3, le cartelle sono rappresentate come prefissi visualizzati nel nome della chiave oggetto. Se carichi un singolo oggetto in una cartella nella console di Amazon S3, il nome della cartella viene incluso nel nome della chiave oggetto.

Ad esempio, se carichi un oggetto denominato `sample1.jpg` in una cartella denominata `backup`, il nome della chiave è `backup/sample1.jpg`. Tuttavia, l'oggetto viene visualizzato nella console come `sample1.jpg` nella cartella `backup`. Per ulteriori informazioni sui nomi delle chiavi, consultare [Utilizzo dei metadati degli oggetti](#).

Note

Se rinomini un oggetto o modifichi una delle proprietà nella console di Amazon S3, ad esempio Classe di storage, Crittografia o Metadati, viene creato un nuovo oggetto per sostituire quello precedente. Se è abilitata la funzione Controllo delle versioni S3, viene creata una nuova versione dell'oggetto e l'oggetto esistente diventa una versione precedente. Il ruolo che modifica la proprietà diventa anche il proprietario del nuovo oggetto o della versione dell'oggetto.

Quando si carica una cartella, Amazon S3 carica nel bucket tutti i file e le sottocartelle inclusi nella cartella specificata, quindi assegna un nome della chiave dell'oggetto, ossia una combinazione del nome del file caricato e del nome della cartella. Ad esempio, se si carica una cartella denominata `/images` contenente due file, `sample1.jpg` e `sample2.jpg`, Amazon S3 carica i file, quindi assegna i nomi delle chiavi corrispondenti, `images/sample1.jpg` e `images/sample2.jpg`. I nomi delle chiavi includono il nome della cartella come prefisso. La console di Amazon S3 visualizza solo la parte del nome della chiave che segue l'ultimo simbolo `/`. Ad esempio, in una cartella di `images`, gli oggetti `images/sample1.jpg` e `images/sample2.jpg` sono visualizzati come `sample1.jpg` e `sample2.jpg`.

Per caricare cartelle e file in un bucket S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) scegliere il nome del bucket in cui si desidera caricare le cartelle o i file.
4. Scegli Carica.
5. Nella finestra Carica completa una delle seguenti operazioni:
 - Trascina e rilascia file e cartelle nella finestra Carica .
 - Scegli Aggiungi file o Aggiungi cartella, seleziona i file o le cartelle da caricare e scegli Apri.
6. Per abilitare il controllo delle versioni, in Destinazione, seleziona Abilita controllo delle versioni del bucket.
7. Per caricare i file e le cartelle elencati senza configurare opzioni di caricamento aggiuntive, scegli Carica.

Amazon S3 caricherà i tuoi oggetti e le tue cartelle. Al termine del caricamento viene visualizzato un messaggio di esito positivo nella pagina Carica: stato.

Per configurare proprietà aggiuntive dell'oggetto

1. Per modificare le autorizzazioni della lista di controllo degli accessi, scegli Permissions (Autorizzazioni).
2. In Access control list (ACL) Lista di controllo degli accessi (ACL), modifica le autorizzazioni.

Per informazioni sulle autorizzazioni di accesso agli oggetti, consulta [Utilizzo della console S3 per impostare le autorizzazioni ACL per un oggetto](#). Puoi concedere l'accesso in lettura ai tuoi oggetti al pubblico (chiunque) per tutti i file che stai caricando. Ti consigliamo di non modificare l'impostazione di default per l'accesso pubblico in lettura. La concessione dell'accesso pubblico in lettura si applica a un piccolo sottoinsieme di casi d'uso, ad esempio quando i bucket vengono usati per i siti Web. È sempre possibile apportare modifiche alle autorizzazioni dell'oggetto dopo averlo caricato.

3. Per configurare altre proprietà scegli Properties (Proprietà).
4. Nella sezione Classe di storage seleziona la classe di storage per i file che si stanno caricando.

Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

5. Per aggiornare le impostazioni di crittografia per i tuoi oggetti, in Impostazioni di Server-side crittografia, procedi come segue.
 - a. Scegli Specify an encryption key (Specifica una chiave di crittografia).
 - b. In Impostazioni di crittografia, scegli Utilizza le impostazioni del bucket per la crittografia predefinita o Ignora le impostazioni del bucket per la crittografia predefinita.
 - c. Se scegli Ignora le impostazioni del bucket per la crittografia predefinita, dovrai configurare le seguenti impostazioni di crittografia.
 - Per crittografare i file caricati utilizzando chiavi gestite da Amazon S3, scegli Amazon S3 managed key (). SSE-S3

Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).

- Per crittografare i file caricati utilizzando le chiavi memorizzate in AWS Key Management Service (AWS KMS), scegli AWS Key Management Service key (). SSE-KMS Quindi scegli una delle seguenti opzioni per Chiave AWS KMS :
 - Per scegliere da un elenco di chiavi KMS disponibili, seleziona Scegli tra le chiavi AWS KMS keys, quindi scegli la chiave KMS dall'elenco delle chiavi disponibili.

Sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente vengono visualizzate in questo elenco. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per inserire l'ARN della chiave KMS, scegli **Inserisci AWS KMS key ARN**, quindi inserisci l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli **Crea una chiave KMS**.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

 Important

È possibile utilizzare solo le chiavi KMS disponibili nello stesso bucket della Regione AWS. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, devi inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione necessaria per l'uso della chiave e quindi inserire l'ARN della chiave KMS.

Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service.

6. Per utilizzare checksum aggiuntivi, scegli **On (Attivato)**. Per **Checksum function (Funzione checksum)**, scegli la funzione che desideri utilizzare. Amazon S3 calcola e archivia il valore del checksum dopo aver ricevuto l'intero oggetto. Puoi utilizzare la casella **Precalculated value (Valore precalcolato)** per fornire un valore precalcolato. In tal caso, Amazon S3 confronta il valore specificato con il valore calcolato. Se i due valori non corrispondono, Amazon S3 genera un errore.

I checksum aggiuntivi ti consentono di specificare l'algoritmo di checksum che desideri utilizzare per verificare i dati. Per ulteriori informazioni sui checksum aggiuntivi, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

7. Per aggiungere tag a tutti gli oggetti che si stanno caricando, scegliere **Add tag (Aggiungi tag)**. Immetti un nome di tag nel campo **Chiave**. Immetti un valore per il tag.

Il tagging ti consente di catalogare lo storage. Ogni tag è una coppia chiave-valore. I valori delle chiavi e dei tag fanno distinzione tra maiuscole e minuscole. Puoi avere un massimo di 10 tag per oggetto. Una chiave di tag può essere composta da un massimo di 128 caratteri Unicode.

e i valori di tag possono essere composti da un massimo di 255 caratteri Unicode. Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#).

8. Per aggiungere metadati, seleziona Aggiungi metadati.

- a. In Tipo seleziona Definito dal sistema o Definito dall'utente.

Per i metadati definiti dal sistema, puoi selezionare intestazioni HTTP comuni, come e. Content-Type Content-Disposition Per un elenco di metadati definiti dal sistema e informazioni sulla possibilità di aggiungere il valore, consulta [System-defined metadati degli oggetti](#). Tutti i metadati che iniziano con il prefisso vengono trattati come metadati definiti dall'utente. x-amz-meta- User-defined metadati vengono archiviati con l'oggetto e vengono restituiti quando si scarica l'oggetto. Sia le chiavi che i relativi valori devono essere conformi agli standard. US-ASCII User-defined i metadati possono avere una dimensione massima di 2 KB. Per ulteriori informazioni sui metadati definiti dal sistema e definiti dall'utente, consulta [Utilizzo dei metadati degli oggetti](#).

- b. Per Chiave, seleziona una chiave.

- c. Digitare un valore per la chiave.

9. Per caricare i tuoi oggetti, scegli Carica.

Amazon S3 caricherà l'oggetto. Al termine del caricamento, sarà visualizzato un messaggio di successo nella pagina Carica: stato .

10. Scegliere Exit (Esci).

Utilizzo di AWS CLI

È possibile inviare una richiesta PUT per caricare un oggetto di un massimo di 5 GB in una singola operazione. Per ulteriori informazioni ed esempi, consulta l'esempio [PutObject](#) in Riferimento ai comandi della AWS CLI .

Utilizzo della REST API

Per caricare un oggetto puoi inviare richieste REST. È possibile inviare una richiesta PUT per caricare i dati in una singola operazione. Per ulteriori informazioni, consulta [PUT Object](#).

Utilizzo di AWS SDK

Per esempi su come caricare un oggetto con gli AWS SDK, consulta Esempi di [codice](#) nell'Amazon Simple Storage Service API Reference.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon Simple Storage Service.

Impedisci il caricamento di oggetti con nomi di chiavi identici

È possibile verificare l'esistenza di un oggetto nel bucket prima di crearlo, utilizzando una scrittura condizionale sulle operazioni di caricamento. In questo modo si può evitare la sovrascrittura dei dati esistenti. Le scritture condizionali convalidano l'assenza di oggetti esistenti con lo stesso nome chiave nel bucket durante il caricamento.

Si possono usare le scritture condizionali per richieste [PutObject](#) o [CompleteMultipartUpload](#).

Per ulteriori informazioni sulle richieste condizionali, consulta [Aggiunta di precondizioni alle operazioni S3 con richieste condizionali](#).

Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3

Il caricamento multiparte consente di caricare un singolo oggetto su Amazon S3 come un insieme di parti. Ciascuna parte è una parte contigua dei dati dell'oggetto. È possibile caricare queste parti di oggetto in modo indipendente e in qualsiasi ordine. Per i caricamenti, il AWS client aggiornato calcola automaticamente un checksum dell'oggetto e lo invia ad Amazon S3 insieme alle dimensioni dell'oggetto come parte della richiesta. Se la trasmissione di una parte non riesce, è possibile ritrasmettere tale parte senza influire sulle altre. Dopo aver caricato tutte le parti dell'oggetto, Amazon S3 le assembla per creare l'oggetto. È consigliabile utilizzare il caricamento multiparte per gli oggetti di dimensioni pari o superiori a 100 MB, anziché caricarli in un'unica operazione.

Il caricamento in più parti comporta i vantaggi riportati di seguito.

- Throughput migliorato: puoi caricare le parti in parallelo per migliorare il throughput.
- Ripristino rapido dai problemi di rete: la dimensione più piccola delle parti riduce al minimo l'impatto del riavvio di un caricamento fallito a causa di un errore di rete.
- Messa in pausa e ripresa dei caricamenti dell'oggetto: puoi caricare le parti dell'oggetto nel corso del tempo. Una volta avviato, un caricamento in più parti continua finché non viene completato o interrotto in modo esplicito.
- Inizia il caricamento prima di conoscere le dimensioni finali dell'oggetto - È possibile caricare un oggetto mentre lo si crea.

È consigliabile utilizzare il caricamento in più parti come indicato di seguito:

- Se carichi oggetti di grandi dimensioni su una rete stabile ad alta larghezza di banda, utilizza il caricamento multiparte per massimizzare l'uso della larghezza di banda disponibile caricando le parti dell'oggetto in parallelo per ottenere prestazioni multi-thread.
- Se esegui il caricamento su una rete discontinua, utilizza il caricamento multiparte per aumentare la resilienza contro gli errori di rete evitando il riavvio del caricamento. Quando si utilizza il caricamento multiparte, è necessario riprovare a caricare solo le parti interrotte durante il caricamento. Non è necessario riavviare il caricamento dell'oggetto dall'inizio.

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#). Per ulteriori informazioni sull'utilizzo del caricamento in più parti con S3 Express One Zone e i bucket di directory, consulta [Utilizzo dei caricamenti multiparte con i bucket di directory](#).

Processo di caricamento in più parti

Il caricamento multiparte è un processo in tre fasi: si avvia il caricamento, si caricano le parti dell'oggetto e, dopo aver caricato tutte le parti, si completa il caricamento multiparte. Una volta ricevuta la richiesta di caricamento multiparte completa, Amazon S3 costruisce l'oggetto a partire dalle parti caricate e si può accedere all'oggetto come a qualsiasi altro oggetto nel bucket.

È possibile elencare tutti i caricamenti in più parti in corso oppure ottenere un elenco delle parti caricate per un caricamento in più parti specifico. Ognuna di queste operazioni viene descritta in questa sezione.

Avvio del caricamento in più parti

Quando si invia una richiesta per avviare un caricamento multiparte, assicurarsi di specificare un tipo di checksum. Amazon S3 restituirà quindi una risposta con un ID di caricamento, che è un identificatore unico per il caricamento multiparte. Questo ID di caricamento è necessario quando si caricano e si elencano parti oppure si completa o interrompe un caricamento. Se si desidera fornire metadati che descrivono l'oggetto da caricare, è necessario fornirli nella richiesta di avvio del caricamento multiparte. Gli utenti anonimi non possono avviare caricamenti in più parti.

Caricamento delle parti

Quando si carica una parte, è necessario specificare un numero di parte oltre all'ID di caricamento. È possibile scegliere qualsiasi numero compreso tra 1 e 10.000. Il numero della parte identifica in modo univoco una parte e la relativa posizione nell'oggetto che si sta caricando. Il numero della parte scelto non deve essere in sequenza (ad esempio può essere 1, 5 e 14). Tieni presente che, se carichi una nuova parte usando lo stesso numero di parte di una caricata in precedenza, la parte caricata in precedenza viene sovrascritta.

Quando si carica una parte, Amazon S3 restituisce il tipo di algoritmo di checksum con il valore di checksum per ogni parte come intestazione della risposta. Per ogni caricamento di parte è necessario registrare il numero della parte e il valore ETag. Occorre includere questi valori nella successiva richiesta di completamento del caricamento in più parti. Ogni parte avrà il proprio ETag al momento del caricamento. Tuttavia, una volta completato il caricamento multiparte e consolidate tutte le parti, tutte le parti appartengono a un unico ETag come somma di controllo.

Important

Dopo aver avviato un caricamento multiparte e aver caricato una o più parti, è necessario completare o interrompere il caricamento multiparte per non incorrere nei costi di archiviazione delle parti caricate. Solo dopo aver completato o interrotto un caricamento multiparte, Amazon S3 libererà l'archiviazione di parti e smetterà di fatturare per l'archiviazione delle parti.

Dopo aver interrotto il caricamento multiparte, non è più possibile caricare alcuna parte usando l'ID di caricamento. Se il caricamento di una parte era in corso, può continuare ad avere successo o fallire anche dopo aver interrotto il caricamento. Per essere sicuri di liberare tutto lo spazio di archiviazione consumato da tutte le parti, è necessario interrompere un caricamento multiparte solo dopo che tutti i carichi di parti sono stati completati.

Completamento del caricamento in più parti

Una volta completato un caricamento in più parti, Amazon S3 crea un oggetto concatenando le parti in ordine crescente in base al numero della parte. Se nella richiesta di avvio del caricamento in più parti sono stati forniti i metadati dell'oggetto, Amazon S3 li associa all'oggetto. Una volta completata la richiesta, le parti non esisteranno più.

La richiesta di completamento del caricamento multiparte deve includere l'ID di caricamento e un elenco di numeri di parte e dei valori ETag corrispondenti. La risposta di Amazon S3 include un ETag

che identifica in modo univoco i dati oggetto combinati. Questo ETag non è necessariamente un hash MD5 dei dati dell'oggetto.

Quando fornisci un checksum completo dell'oggetto durante un caricamento in più parti, l' AWS SDK passa il checksum ad Amazon S3 e S3 convalida l'integrità dell'oggetto sul server, confrontandolo con il valore ricevuto. Quindi, S3 memorizza l'oggetto se i valori corrispondono. Se i due valori non corrispondono, Amazon S3 rifiuta la richiesta con un errore `BadDigest`. Il checksum dell'oggetto viene memorizzato anche nei metadati dell'oggetto, che verranno utilizzati in seguito per convalidare l'integrità dei dati di un oggetto.

Chiamate di caricamento in più parti di esempio

Per questo esempio, si supponga di generare un caricamento multiparte per un file di 100 GB. In questo caso, sarebbero disponibili le seguenti chiamate API per l'intero processo. Il totale delle chiamate API è di 1.002.

- Una chiamata [CreateMultipartUpload](#) per avviare il processo.
- 1.000 chiamate individuali a [UploadPart](#), ciascuna delle quali carica una parte di 100 MB, per una dimensione totale di 100 GB.
- Una chiamata a [CompleteMultipartUpload](#) per completare il processo.

Elenchi dei caricamenti in più parti

È possibile elencare le parti di un caricamento in più parti specifico o tutti i caricamenti in più parti in corso. L'operazione `Elenca parti` restituisce le informazioni sulle parti caricate per uno specifico caricamento multiparte. Per ogni richiesta di elenco delle parti, Amazon S3 restituisce informazioni sulle parti per il caricamento in più parti specificato, fino a un massimo di 1000 parti. Se il caricamento multiparte contiene più di 1.000 parti, è necessario inviare una serie di richieste `Elenca parti` per recuperare tutte le parti. Tieni presente che l'elenco di parti restituito non include le parti per le quali non è stato completato il caricamento. L'operazione `list multipart uploads` (elenco dei caricamenti in più parti) consente di ottenere l'elenco dei caricamenti in più parti in corso.

Un caricamento in più parti in corso è un caricamento avviato, ma non ancora completato o annullato. Ogni richiesta restituisce al massimo 1.000 caricamenti in più parti. Se sono in corso più di 1.000 caricamenti in più parti, è necessario inviare richieste aggiuntive per recuperare i caricamenti rimanenti. Utilizza l'elenco restituito solo per la verifica.

 Important

Non utilizzarlo per inviare la richiesta complete multipart upload (completamento del caricamento in più parti). Al contrario, mantieni il tuo elenco dei numeri delle parti specificato durante il caricamento delle parti e i valori ETag corrispondenti restituiti da Amazon S3.

Checksum con operazioni di caricamento in più parti

Quando carichi un oggetto in Amazon S3 puoi specificare un algoritmo di checksum che Amazon S3 deve utilizzare. Per impostazione predefinita, l' AWS SDK e la console S3 utilizzano un algoritmo per tutti i caricamenti di oggetti, che puoi sovrascrivere. Se utilizzi un SDK precedente e l'oggetto caricato non ha un checksum specificato, Amazon S3 utilizza automaticamente l'algoritmo di checksum (). CRC-64/NVME CRC64NVME (questa è anche l'opzione consigliata per una verifica efficiente dell'integrità dei dati). Quando si utilizza CRC-64/NVME, Amazon S3 calcola il checksum dell'intero oggetto al termine del caricamento in più parti o in una singola parte. L'algoritmo di CRC-64/NVME checksum viene utilizzato per calcolare un checksum diretto dell'intero oggetto o un checksum dei checksum per ogni singola parte.

Dopo aver caricato un oggetto su S3 utilizzando il caricamento in più parti, Amazon S3 calcola il valore del checksum per ogni parte o per l'intero oggetto e archivia i valori. Puoi utilizzare l'API o l' AWS SDK S3 per recuperare il valore del checksum nei seguenti modi:

- Per le singole parti, si può usare [GetObject](#) o [HeadObject](#). Se si desidera recuperare i valori di checksum per le singole parti dei caricamenti multipart mentre sono ancora in corso, si può usare [ListParts](#).
- Per l'intero oggetto, si può usare [PutObject](#). Se vuoi eseguire un caricamento multipart con un checksum completo dell'oggetto, utilizza i comandi [CreateMultipartUpload](#) e [CompleteMultipartUpload](#) specificando il tipo di checksum dell'oggetto completo. Per convalidare il valore del checksum dell'intero oggetto o per confermare quale tipo di checksum viene utilizzato nel caricamento multipart, usa [ListParts](#).

 Important

Se si utilizza un caricamento in più parti con Checksum, i numeri di parte per ciascun caricamento (nel caricamento in più parti) devono essere numeri consecutivi e iniziare con 1. Quando si utilizzano i Checksum, se si tenta di completare una richiesta di caricamento

multiparte con numeri di parte non consecutivi, Amazon S3 genera un errore HTTP 500 Internal Server.

Per ulteriori informazioni sul funzionamento dei checksum con gli oggetti di caricamento multiparte, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Per una procedura end-to-end che dimostra come caricare un oggetto utilizzando il caricamento multiparte con un checksum aggiuntivo, consulta [Esercitazione: caricamento di un oggetto tramite caricamento multiparte per verificarne l'integrità dei dati](#).

Operazioni simultanee di caricamento in più parti

In un ambiente di sviluppo distribuito è possibile che l'applicazione avvii più aggiornamenti sullo stesso oggetto contemporaneamente. L'applicazione potrebbe avviare vari caricamenti in più parti utilizzando la stessa chiave dell'oggetto. Per ciascuno di questi caricamenti, l'applicazione può quindi caricare le parti e inviare una richiesta di completamento del caricamento ad Amazon S3 per creare l'oggetto. Se per i bucket è abilitato il controllo delle versioni S3, il completamento di un caricamento in più parti crea sempre una nuova versione. Quando si avviano più caricamenti multiparte che utilizzano la stessa chiave oggetto in un bucket con controllo delle versioni abilitato, la versione corrente dell'oggetto è determinata da quale caricamento è stato avviato più di recente (`createdDate`).

Ad esempio, si avvia una richiesta a `CreateMultipartUpload` per un oggetto alle 10:00. Quindi, si invia una seconda richiesta a `CreateMultipartUpload` per lo stesso oggetto alle 11:00. Poiché la seconda richiesta è stata presentata più di recente, l'oggetto caricato dalla richiesta delle 11:00 diventa la versione corrente, anche se il primo caricamento è stato completato dopo il secondo. Per i bucket che non hanno il controllo delle versioni abilitato, è possibile che qualsiasi altra richiesta ricevuta tra l'avvio del caricamento multiparte e il suo completamento abbia la precedenza.

Un altro esempio di quando una richiesta di caricamento multiparte simultaneo può avere la precedenza è il caso in cui un'altra operazione cancella una chiave dopo aver avviato un caricamento multiparte con quella chiave. Prima di completare l'operazione, la risposta completa del caricamento multiparte potrebbe indicare che la creazione dell'oggetto è avvenuta con successo, senza che l'utente abbia mai visto l'oggetto.

Impedisci il caricamento di oggetti con nomi di chiavi identici durante il caricamento multiparte

È possibile verificare l'esistenza di un oggetto nel bucket prima di crearlo, utilizzando una scrittura condizionale sulle operazioni di caricamento. In questo modo si può evitare la sovrascrittura dei dati esistenti. Le scritture condizionali convalidano l'assenza di oggetti esistenti con lo stesso nome chiave nel bucket durante il caricamento.

Si possono usare le scritture condizionali per richieste [PutObject](#) o [CompleteMultipartUpload](#).

Per ulteriori informazioni, consulta [Come prevenire la sovrascrittura degli oggetti con le scritture condizionali](#).

Caricamento in più parti e prezzi

Una volta avviato un caricamento in più parti, Amazon S3 mantiene tutte le parti finché il caricamento non viene completato o interrotto. Per tutta la durata del processo, all'utente vengono fatturati i costi per lo storage, la larghezza di banda e le richieste per questo tipo di caricamento e per le parti associate.

Queste parti vengono fatturate in base alla classe di storage specificata al momento del caricamento delle parti. Tuttavia, queste parti non ti verranno addebitate se vengono caricate su S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. In-progress le parti multiple per una richiesta PUT alla classe di storage S3 Glacier Flexible Retrieval vengono fatturate come storage temporizzato S3 Glacier Flexible Retrieval alle tariffe di archiviazione S3 Standard fino al completamento del caricamento. Inoltre, sia `CreateMultipartUpload` sia `UploadPart` sono fatturati alle tariffe S3 Standard. Solo la richiesta `CompleteMultipartUpload` viene fatturata alla tariffa di Recupero flessibile S3 Glacier. Analogamente, le parti multiparte in corso per PUT alla classe di storage S3 Glacier Deep Archive sono fatturate come storage di staging Recupero flessibile S3 Glacier alle tariffe di storage S3 Standard fino al completamento del caricamento, con l'addebito della sola richiesta `CompleteMultipartUpload` alle tariffe S3 Glacier Deep Archive.

Se si interrompe il caricamento multiparte, Amazon S3 elimina gli artefatti di caricamento e tutte le parti caricate. Tali artefatti non verranno addebitati. Non sono previsti costi di cancellazione anticipata per l'eliminazione di carichi incompleti in più parti indipendentemente dalla classe di archiviazione specificata. Per ulteriori informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

 Note

Per ridurre al minimo i costi di archiviazione, ti consigliamo di configurare una regola del ciclo di vita per eliminare i caricamenti in più parti incompleti dopo un numero di giorni specificato utilizzando l'operazione `AbortIncompleteMultipartUpload`. Per ulteriori informazioni sulla creazione di una regola del ciclo di vita per eliminare i caricamenti in più parti incompleti, consulta [Configurazione del ciclo di vita del bucket per l'eliminazione dei caricamenti in più parti incompleti](#).

Supporto per l'API per il caricamento in più parti

Le seguenti sezioni di Riferimento API di Amazon Simple Storage Service descrivono la REST API per il caricamento multiparte.

Per una procedura dettagliata sul caricamento in più parti che utilizza le funzioni AWS Lambda, consulta Caricare oggetti di grandi dimensioni su Amazon S3 utilizzando l'accelerazione del caricamento e del trasferimento in più parti. <https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

- [Creazione di un caricamento in più parti](#)
- [Upload Part](#)
- [Upload Part \(Copy\)](#)
- [Completamento del caricamento in più parti](#)
- [Abort Multipart Upload](#)
- [List Parts](#)
- [Elenco dei caricamenti in più parti](#)

AWS Command Line Interface supporto per il caricamento in più parti

I seguenti argomenti AWS Command Line Interface descrivono le operazioni per il caricamento in più parti.

- [Avvio del caricamento in più parti](#)
- [Upload Part](#)
- [Upload Part \(Copy\)](#)

- [Completamento del caricamento in più parti](#)
- [Abort Multipart Upload](#)
- [List Parts](#)
- [Elenco dei caricamenti in più parti](#)

AWS Supporto SDK per il caricamento in più parti

Puoi utilizzare un AWS SDK per caricare un oggetto in parti. Per un elenco degli AWS SDK supportati dall'azione API, consulta:

- [Creazione di un caricamento in più parti](#)
- [Upload Part](#)
- [Upload Part \(Copy\)](#)
- [Completamento del caricamento in più parti](#)
- [Abort Multipart Upload](#)
- [List Parts](#)
- [Elenco dei caricamenti in più parti](#)

Autorizzazioni e API per il caricamento in più parti

Per eseguire le operazioni di caricamento in più parti, devi disporre delle autorizzazioni necessarie. Per concedere ai singoli utenti le autorizzazioni per eseguire queste operazioni, è possibile utilizzare le liste di controllo accessi (ACL), la policy di bucket o la policy utente. Nella tabella riportata di seguito sono elencate le autorizzazioni richieste per le varie operazioni di caricamento in più parti quando si utilizzano le liste di controllo accessi (ACL), la policy di bucket o la policy utente.

Operazione	Autorizzazioni richieste
Creazione di un caricamento in più parti	<p>Per creare una richiesta di caricamento multiparte, è necessario essere autorizzati a eseguire l'azione <code>s3:PutObject</code> su un oggetto.</p> <p>Il proprietario del bucket può consentire ad altri principali di eseguire l'azione <code>s3:PutObject</code>.</p>

Operazione	Autorizzazioni richieste
Avvio del caricamento in più parti	<p>Per avviare un caricamento multiparte, è necessario essere autorizzati a eseguire l'azione <code>s3:PutObject</code> su un oggetto.</p> <p>Il proprietario del bucket può consentire ad altri principali di eseguire l'azione <code>s3:PutObject</code>.</p>
Iniziatore	<p>Elemento del container che identifica l'utente che ha avviato il caricamento in più parti. Se l'iniziatore è un Account AWS, questo elemento fornisce le stesse informazioni dell'elemento Owner. Se è un utente IAM, questo elemento fornisce l'ARN e il nome visualizzato dell'utente.</p>
Upload Part	<p>Per caricare una parte, è necessario essere autorizzati a eseguire l'operazione <code>s3:PutObject</code> su un oggetto.</p> <p>Il proprietario del bucket deve consentire all'iniziatore di eseguire l'operazione <code>s3:PutObject</code> su un oggetto affinché quest'ultimo possa caricare una parte di tale oggetto.</p>
Upload Part (Copy)	<p>Per caricare una parte, è necessario essere autorizzati a eseguire l'operazione <code>s3:PutObject</code> su un oggetto. Poiché si sta caricando una parte da un oggetto esistente, è necessario essere autorizzati a eseguire <code>s3:GetObject</code> sull'oggetto di origine.</p> <p>Perché l'iniziatore possa caricare una parte di un oggetto, il proprietario del bucket deve consentire all'iniziatore di eseguire l'operazione <code>s3:PutObject</code> sull'oggetto.</p>
Completamento del caricamento in più parti	<p>Per completare il caricamento in più parti, è necessario essere autorizzati a eseguire l'operazione <code>s3:PutObject</code> su un oggetto.</p> <p>Il proprietario del bucket deve consentire all'iniziatore di eseguire l'operazione <code>s3:PutObject</code> su un oggetto affinché quest'ultimo possa completare un caricamento in più parti di tale oggetto.</p>

Operazione	Autorizzazioni richieste
Stop Multipart Upload	<p>Per interrompere un caricamento in più parti, è necessario essere autorizzati a eseguire l'operazione <code>s3:AbortMultipartUpload</code> .</p> <p>Per impostazione predefinita, il proprietario del bucket e l'iniziatore del caricamento multipart sono autorizzati a eseguire questa azione come parte delle policy IAM e del bucket S3. Se l'iniziatore è un utente IAM, anche quello di Account AWS quell'utente può interrompere il caricamento in più parti. Con le policy degli endpoint VPC, l'iniziatore del caricamento multipart non ottiene automaticamente l'autorizzazione a eseguire l'azione <code>s3:AbortMultipartUpload</code> .</p> <p>Oltre alle impostazioni predefinite, il proprietario del bucket può consentire ad altri principali di eseguire l'azione <code>s3:AbortMultipartUpload</code> su oggetti. Il proprietario del bucket può negare a qualsiasi entità di eseguire l'operazione <code>s3:AbortMultipartUpload</code> .</p>
List Parts	<p>Per elencare un caricamento in più parti, è necessario essere autorizzati a eseguire l'operazione <code>s3:ListMultipartUploadParts</code> .</p> <p>Per default, il proprietario del bucket dispone dell'autorizzazione per elencare le parti per qualsiasi caricamento in più parti nel bucket. L'iniziatore del caricamento in più parti dispone dell'autorizzazione per elencare le parti di un caricamento in più parti specifico. Se l'iniziatore del caricamento in più parti è un utente IAM, anche l'utente IAM che lo Account AWS controlla è autorizzato a elencare parti di quel caricamento.</p> <p>Oltre alle impostazioni predefinite, il proprietario del bucket può consentire ad altri principali di eseguire l'azione <code>s3:ListMultipartUploadParts</code> su oggetti. Il proprietario del bucket può anche negare alle entità l'esecuzione dell'operazione <code>s3:ListMultipartUploadParts</code> .</p>

Operazione	Autorizzazioni richieste
Elenco dei caricamenti in più parti	<p>Per elencare i caricamenti in più parti in corso in un bucket, è necessario essere autorizzati a eseguire l'operazione <code>s3:ListBucketMultipartUploads</code> su tale bucket.</p> <p>Oltre a queste impostazioni di default, il proprietario del bucket può consentire ad altre entità di eseguire l'operazione <code>s3:ListBucketMultipartUploads</code> sul bucket.</p>
AWS KMS Crittografia e decrittografia le relative autorizzazioni	<p>Per eseguire un caricamento in più parti con crittografia utilizzando una chiave KMS AWS Key Management Service (AWS KMS), il richiedente deve disporre delle seguenti autorizzazioni:</p> <ul style="list-style-type: none">• Le azioni <code>kms:Decrypt</code> e <code>kms:GenerateDataKey</code> sulla chiave.• L'azione <code>kms:GenerateDataKey</code> per l'API CreateMultipartUpload API.• L'azione <code>kms:Decrypt</code> sulle API UploadPart e UploadPartCopy. <p>Queste autorizzazioni sono obbligatorie perché Amazon S3 deve decrittografare e leggere i dati dalle parti di file crittografate prima di completare il caricamento in più parti. L'autorizzazione <code>kms:Decrypt</code> e la crittografia lato server con chiavi di crittografia fornite dal cliente sono necessarie anche per ottenere il valore di checksum di un oggetto. Se non si dispone di queste autorizzazioni necessarie quando si utilizza l'API CompleteMultipartUpload, l'oggetto viene creato senza il valore di checksum.</p> <p>Se il tuo utente o ruolo IAM è lo Account AWS stesso della chiave KMS, verifica di disporre delle autorizzazioni sia sulla chiave che sulle policy IAM. Se l'utente o il ruolo IAM appartiene a un account diverso rispetto alla chiave KMS, devi disporre delle autorizzazioni sulla policy delle chiavi e sull'utente o sul ruolo IAM.</p>

Operazione	Autorizzazioni richieste
SSE-C (crittografia lato server con chiavi di crittografia fornite dal cliente)	Quando si utilizza l' CompleteMultipartUpload API, è necessario fornire SSE-C (crittografia lato server con chiavi di crittografia fornite dal cliente), altrimenti l'oggetto verrà creato senza un checksum e non verrà restituito alcun valore di checksum.

Per informazioni sulle relazioni tra le autorizzazioni nelle liste di controllo accessi (ACL) e le autorizzazioni nelle policy di accesso, consulta la sezione [Mappatura delle autorizzazioni ACL e delle autorizzazioni della policy di accesso](#). Per informazioni su utenti, ruoli e best practice di IAM, consulta [Identità IAM \(utenti, gruppi di utenti e ruoli\)](#) nella Guida per l'utente di IAM.

Checksum con operazioni di caricamento in più parti

Esistono tre API Amazon S3 che vengono utilizzate per eseguire il caricamento multiparte: [CreateMultipartUpload](#), [UploadPart](#), e [CompleteMultipartUpload](#). La tabella seguente indica quali intestazioni e valori di checksum devono essere forniti per ciascuna API:

Algoritmo di checksum	Tipo di checksum	CreateMultipartUpload	UploadPart	CompleteMultipartUpload
CRC-64/NVME (CRC64NVME)	Oggetto completo	Intestazioni richieste: x-amz-checksum-algorithm	Intestazioni opzionali: x-amz-checksum-crc64nvme	Intestazioni opzionali: x-amz-checksum-algorithm x-amz-crc64
CRC-32 (CRC32) CRC 32-C (CRC32C)	Oggetto completo	Intestazioni richieste:	Intestazioni opzionali:	Intestazioni opzionali:

Algoritmo di checksum	Tipo di checksum	CreateMultiPartUpload	UploadPart	CompleteMultiPartUpload
		x-amz-checksum-algorithm	x-amz-checksum-crc64nvme	x-amz-checksum-algorithm
		x-amz-checksum-type		x-amz-crc32
				x-amz-crc32c

Algoritmo di checksum	Tipo di checksum	CreateMultiPartUpload	UploadPart	CompleteMultiPartUpload
CRC-32 (CRC32)	Composita	Intestazioni richieste:	Intestazioni richieste:	Intestazioni richieste:
CRC-32C (CRC32C)		x-amz-checksum-algorithm	x-amz-checksum-crc32	Tutti i checksum a livello di parte devono essere inclusi nella richiesta CompleteMultiPartUpload.
SHA-1 (SHA1)				
SHA-256 (SHA256)			x-amz-checksum-crc32c	
MD5 () MD5			x-amz-checksum-sha1	Intestazioni opzionali:
XXHash 64 () XXHASH64			x-amz-checksum-sha256	x-amz-checksum-crc32
Hash XX (3) XXHASH3			x-amz-checksum-md5	x-amz-checksum-crc32c
Hash XX (128) XXHASH128			x-amz-checksum-xxhash64	x-amz-checksum-sha1
SHA-512 (SHA512)			x-amz-checksum-xxhash3	x-amz-checksum-sha256
			x-amz-checksum-xxhash128	x-amz-checksum-md5

Algoritmo di checksum	Tipo di checksum	CreateMultiPartUpload	UploadPart	CompleteMultiPartUpload
			x-amz-checksum-sha512	x-amz-checksum-xxhash64
				x-amz-checksum-xxhash3
				x-amz-checksum-xxhash128
				x-amz-checksum-sha512

Argomenti

- [Configurazione del ciclo di vita del bucket per l'eliminazione dei caricamenti in più parti incompleti](#)
- [Caricamento di un oggetto utilizzando il caricamento in più parti](#)
- [Caricamento di una directory utilizzando la classe .NET di alto livello TransferUtility](#)
- [Elenco dei caricamenti in più parti](#)
- [Monitoraggio di un caricamento in più parti con AWS SDK](#)
- [Interruzione di un caricamento in più parti](#)
- [Copia di un oggetto utilizzando il caricamento in più parti](#)
- [Esercitazione: caricamento di un oggetto tramite caricamento multiparte per verificarne l'integrità dei dati](#)
- [Limiti dei caricamenti in più parti di Amazon S3](#)

Configurazione del ciclo di vita del bucket per l'eliminazione dei caricamenti in più parti incompleti

Consigliamo, come best practice, di configurare una regola per il ciclo di vita utilizzando l'operazione `AbortIncompleteMultipartUpload` per ridurre al minimo i costi di archiviazione. Per ulteriori informazioni sull'interruzione di un caricamento in più parti, consulta [Interruzione di un caricamento in più parti](#).

Amazon S3 supporta una regola per il ciclo di vita del bucket che può essere utilizzata per indicare ad Amazon S3 di interrompere i caricamenti in più parti che non sono stati completati entro un determinato numero di giorni dopo l'avvio. Quando un caricamento in più parti non viene completato entro il periodo di tempo specificato, diventa idoneo per un'operazione di interruzione. Quando Amazon S3 interrompe un caricamento in più parti, elimina tutte le parti associate al caricamento in più parti. Questa regola si applica sia ai caricamenti multiparte esistenti che a quelli creati successivamente.

Di seguito è riportata una configurazione del ciclo di vita di esempio che specifica una regola con l'operazione `AbortIncompleteMultipartUpload`.

```
<LifecycleConfiguration>
  <Rule>
    <ID>sample-rule</ID>
    <Prefix></Prefix>
    <Status>Enabled</Status>
    <AbortIncompleteMultipartUpload>
      <DaysAfterInitiation>7</DaysAfterInitiation>
    </AbortIncompleteMultipartUpload>
  </Rule>
</LifecycleConfiguration>
```

Nell'esempio, la regola non specifica un valore per l'elemento `Prefix` ([prefisso nome della chiave oggetto](#)). Pertanto, la regola viene applicata a tutti gli oggetti nel bucket per i quali sono stati avviati caricamenti in più parti. Tutti i caricamenti in più parti che sono stati avviati e non sono stati completati entro sette giorni diventano idonei per un'operazione di interruzione. L'azione di interruzione non ha alcun effetto sui caricamenti in più parti completati.

Per ulteriori informazioni sulla configurazione del ciclo di vita dei bucket, consulta [Gestione del ciclo di vita degli oggetti](#).

 Note

Se il caricamento in più parti viene completato entro il numero di giorni specificato nella regola, l'operazione `AbortIncompleteMultipartUpload` del ciclo di vita non viene eseguita e Amazon S3 non intraprende alcuna operazione. Inoltre, questa operazione non si applica agli oggetti. Nessun oggetto viene eliminato da questa operazione del ciclo di vita. Inoltre, non dovrai sostenere costi per l'eliminazione anticipata del ciclo di vita S3 quando rimuovi parti caricate in più parti incomplete.

Utilizzo della console S3

Per gestire automaticamente carichi in più parti incompleti, puoi utilizzare la console S3 per creare una regola del ciclo di vita per far scadere byte dei carichi in più parti incompleti dal bucket dopo un determinato numero di giorni. Nella seguente procedura viene illustrato come aggiungere una regola del ciclo di vita per eliminare carichi in più parti dopo 7 giorni. Per ulteriori informazioni sull'aggiunta di regole del ciclo di vita, consulta [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#).

Per aggiungere una regola del ciclo di vita per interrompere i carichi in più parti incompleti che risalgono a più di 7 giorni

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket per il quale si desidera creare una regola del ciclo di vita.
3. Scegliere la scheda Management (Gestione), quindi Create lifecycle rule (Crea regola ciclo di vita).
4. In Lifecycle rule name (Nome regola ciclo di vita) immettere un nome per la regola.

Il nome deve essere univoco all'interno del bucket.

5. Scegliere l'ambito della regola del ciclo di vita:
 - Per creare una regola del ciclo di vita per tutti gli oggetti con un prefisso specifico, scegli Limit the scope of this rule using one or more filters (Limita l'ambito di questa regola utilizzando uno o più filtri) e inserisci il prefisso nel campo Prefix (Prefisso).

- Per applicare una regola del ciclo di vita a tutti gli oggetti nel bucket, scegli This rule applies to all objects in the bucket (Questa regola si applica a tutti gli oggetti nel bucket) e quindi scegli I acknowledge that this rule applies to all objects in the bucket (Confermo che questa regola si applica a tutti gli oggetti nel bucket).
6. In Lifecycle rule actions (Operazioni regola ciclo di vita), seleziona Delete expired object delete markers or incomplete multipart uploads (Elimina contrassegni di eliminazione oggetti scaduti o caricamenti in più parti incompleti).
 7. In Delete expired delete markers or incomplete multipart uploads (Elimina contrassegni di eliminazione scaduti o caricamenti in più parti incompleti), seleziona Delete incomplete multipart uploads (Elimina caricamenti in più parti incompleti).
 8. Nel campo Number of days (Numero di giorni), inserisci il numero di giorni trascorsi i quali eliminare i caricamenti in più parti incompleti (per questo esempio, 7 giorni).
 9. Scegli Crea regola.

Utilizzo di AWS CLI

Il comando following put-bucket-lifecycle-configurationAWS Command Line Interface (AWS CLI) aggiunge la configurazione del ciclo di vita per il bucket specificato. Per utilizzare questo comando, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3api put-bucket-lifecycle-configuration \
    --bucket amzn-s3-demo-bucket \
    --lifecycle-configuration filename-containing-lifecycle-configuration
```

L'esempio seguente mostra come aggiungere una regola del ciclo di vita per interrompere i caricamenti in più parti incompleti utilizzando la AWS CLI. Include un esempio di configurazione del ciclo di vita JSON per interrompere i caricamenti in più parti incompleti che risalgono a più di 7 giorni.

Per utilizzare i comandi CLI in questo esempio, sostituisci *user input placeholders* con le tue informazioni.

Per aggiungere una regola del ciclo di vita per interrompere i caricamenti in più parti incompleti

1. Configura il. AWS CLI Per istruzioni, consulta [Sviluppo con Amazon S3 utilizzando l'interfaccia a riga di comando](#) nell' AWS API Reference di Amazon S3.
2. Salva la configurazione del ciclo di vita di esempio riportata di seguito in un file (ad esempio, *lifecycle.json*). Questa configurazione di esempio specifica un prefisso vuoto e pertanto

non si applica a tutti gli oggetti nel bucket. È possibile specificare un prefisso per limitare la configurazione a un sottoinsieme di oggetti.

```
{
  "Rules": [
    {
      "ID": "Test Rule",
      "Status": "Enabled",
      "Filter": {
        "Prefix": ""
      },
      "AbortIncompleteMultipartUpload": {
        "DaysAfterInitiation": 7
      }
    }
  ]
}
```

3. Esegui il comando della CLI riportato di seguito per impostare la configurazione del ciclo di vita sul bucket.

```
aws s3api put-bucket-lifecycle-configuration \
--bucket amzn-s3-demo-bucket \
--lifecycle-configuration file://lifecycle.json
```

4. Per verificare che la configurazione del ciclo di vita sia stata impostata sul bucket, recupera la configurazione del ciclo di vita utilizzando il seguente comando `get-bucket-lifecycle`.

```
aws s3api get-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

5. Per eliminare la configurazione del ciclo di vita, utilizza il seguente comando `delete-bucket-lifecycle`.

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

Caricamento di un oggetto utilizzando il caricamento in più parti

Puoi usare il caricamento in più parti per caricare un singolo oggetto a livello di programmazione su Amazon S3. Ogni oggetto viene caricato come insieme di parti. Ciascuna parte è una parte contigua dei dati dell'oggetto. È possibile caricare queste parti dell'oggetto in modo indipendente e in qualsiasi ordine. Se la trasmissione di una parte non riesce, è possibile ritrasmettere tale parte senza influire sulle altre. Una volta caricate tutte le parti dell'oggetto, Amazon S3 le assembla e crea l'oggetto. Gli utenti anonimi non possono avviare caricamenti in più parti.

Note

Per impostazione predefinita, le operazioni di caricamento e copia in più parti non copiano le annotazioni dall'oggetto sorgente. Per includere annotazioni durante la copia di oggetti utilizzando il caricamento in più parti (ad esempio, con il AWS CLI `aws s3 cp` comando per oggetti di dimensioni superiori a circa 8 MB), specificare `--copy-props all`

Per una procedura end-to-end che dimostra come caricare un oggetto utilizzando il caricamento multiparte con un checksum aggiuntivo, consulta [Esercitazione: caricamento di un oggetto tramite caricamento multiparte per verificarne l'integrità dei dati](#).

La sezione seguente mostra come utilizzare il caricamento in più parti con gli SDK, e. AWS Command Line Interface AWS

Utilizzo della console S3

In un bucket S3 è possibile caricare qualsiasi tipo di file: immagini, backup, dati, film e così via. La dimensione massima di un file che è possibile caricare utilizzando la console di Amazon S3 è 160 GB. Per caricare un file di dimensioni superiori a 160 GB, utilizza AWS Command Line Interface (AWS CLI), AWS SDK o l'API REST di Amazon S3.

Per istruzioni sul caricamento di un oggetto tramite, consulta Console di gestione AWS. [Caricamento degli oggetti](#)

Utilizzo di AWS CLI

Di seguito vengono descritte le operazioni di Amazon S3 per il caricamento multiparte utilizzando AWS CLI.

- [Avvio del caricamento in più parti](#)

- [Upload Part](#)
- [Upload Part \(Copy\)](#)
- [Completamento del caricamento in più parti](#)
- [Abort Multipart Upload](#)
- [List Parts](#)
- [Elenco dei caricamenti in più parti](#)

Utilizzo della REST API

Le sezioni seguenti della Documentazione di riferimento delle API di Amazon Simple Storage Service descrivono REST API per il caricamento in più parti.

- [Avvio del caricamento in più parti](#)
- [Upload Part](#)
- [Completamento del caricamento in più parti](#)
- [Stop Multipart Upload](#)
- [List Parts](#)
- [Elenco dei caricamenti in più parti](#)

Utilizzo di AWS SDK (API di alto livello)

Alcuni AWS SDK espongono un'API di alto livello che semplifica il caricamento in più parti combinando le diverse operazioni API necessarie per completare un caricamento in più parti in un'unica operazione. Per ulteriori informazioni, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Se è necessario sospendere e riprendere il caricamento multiparte, variare le dimensioni delle parti durante il caricamento, oppure non conosci in anticipo le dimensioni dei dati, utilizza i metodi API di basso livello. I metodi API di basso livello per il caricamento multiparte offrono ulteriori funzionalità; per ulteriori informazioni, consulta [Utilizzo di AWS SDK \(API di basso livello\)](#).

Java

Per esempi di come eseguire un caricamento in più parti con l' AWS SDK per Java, consulta [Caricare o scaricare file di grandi dimensioni da e verso Amazon S3 utilizzando un SDK nell'Amazon S3 API Reference. AWS](#)

.NET

Per caricare un file in un bucket S3, utilizzare la classe `TransferUtility`. Se si caricano dati da un file, è necessario specificare il nome della chiave dell'oggetto. In caso contrario, l'API utilizza il nome file per il nome della chiave. Durante il caricamento di dati da un flusso, è necessario specificare il nome della chiave dell'oggetto.

Per impostare opzioni di caricamento avanzate, come la dimensione delle parti, il numero di thread durante il caricamento simultaneo di parti, i metadati, la classe di storage o la lista di controllo accessi, utilizza la classe `TransferUtilityUploadRequest`.

Note

Se l'origine dei dati è costituita da un flusso, la classe `TransferUtility` non esegue caricamenti simultanei.

Il seguente esempio di codice C# consente di caricare un file in un bucket Amazon S3 in più parti. Mostra come utilizzare diversi overload `TransferUtility.Upload` per caricare un file. Ciascuna chiamata successiva al caricamento sostituisce il caricamento precedente. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET Developer Guide. AWS

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPUHighLevelAPITest
    {
        private const string bucketName = "**** provide bucket name ****";
        private const string keyName = "**** provide a name for the uploaded object ****";
        private const string filePath = "**** provide the full path name of the file to upload ****";
        // Specify your bucket region (an example region is shown).
```

```
private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
private static IAmazonS3 s3Client;

public static void Main()
{
    s3Client = new AmazonS3Client(bucketRegion);
    UploadFileAsync().Wait();
}

private static async Task UploadFileAsync()
{
    try
    {
        var fileTransferUtility =
            new TransferUtility(s3Client);

        // Option 1. Upload a file. The file name is used as the object key
name.

        await fileTransferUtility.UploadAsync(filePath, bucketName);
        Console.WriteLine("Upload 1 completed");

        // Option 2. Specify object key name explicitly.
        await fileTransferUtility.UploadAsync(filePath, bucketName,
keyName);

        Console.WriteLine("Upload 2 completed");

        // Option 3. Upload data from a type of System.IO.Stream.
        using (var fileToUpload =
            new FileStream(filePath, FileMode.Open, FileAccess.Read))
        {
            await fileTransferUtility.UploadAsync(fileToUpload,
                bucketName, keyName);
        }
        Console.WriteLine("Upload 3 completed");

        // Option 4. Specify advanced settings.
        var fileTransferUtilityRequest = new TransferUtilityUploadRequest
        {
            BucketName = bucketName,
            FilePath = filePath,
            StorageClass = S3StorageClass.StandardInfrequentAccess,
            PartSize = 6291456, // 6 MB.
            Key = keyName,
```

```

        CannedACL = S3CannedACL.PublicRead
    };
    fileTransferUtilityRequest.Metadata.Add("param1", "Value1");
    fileTransferUtilityRequest.Metadata.Add("param2", "Value2");

    await fileTransferUtility.UploadAsync(fileTransferUtilityRequest);
    Console.WriteLine("Upload 4 completed");
}
catch (AmazonS3Exception e)
{
    Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
}
catch (Exception e)
{
    Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
}
}
}
}

```

JavaScript

Example

Carica un file di grandi dimensioni.

```

import { S3Client } from "@aws-sdk/client-s3";
import { Upload } from "@aws-sdk/lib-storage";

import {
    ProgressBar,
    logger,
} from "@aws-doc-sdk-examples/lib/utils/util-log.js";

const twentyFiveMB = 25 * 1024 * 1024;

export const createString = (size = twentyFiveMB) => {
    return "x".repeat(size);
};

/**

```



```

* Create a 25MB file and upload it in parts to the specified
* Amazon S3 bucket.
* @param {{ bucketName: string, key: string }}
*/
export const main = async ({ bucketName, key }) => {
  const str = createString();
  const buffer = Buffer.from(str, "utf8");
  const progressBar = new ProgressBar({
    description: `Uploading "${key}" to "${bucketName}"`,
    barLength: 30,
  });

  try {
    const upload = new Upload({
      client: new S3Client({}),
      params: {
        Bucket: bucketName,
        Key: key,
        Body: buffer,
      },
    });

    upload.on("httpUploadProgress", ({ loaded, total }) => {
      progressBar.update({ current: loaded, total });
    });

    await upload.done();
  } catch (caught) {
    if (caught instanceof Error && caught.name === "AbortError") {
      logger.error(`Multipart upload was aborted. ${caught.message}`);
    } else {
      throw caught;
    }
  }
};

```

Example

Scarica un file di grandi dimensioni.

```

import { fileURLToPath } from "node:url";
import { GetObjectCommand, NoSuchKey, S3Client } from "@aws-sdk/client-s3";
import { createWriteStream, rmSync } from "node:fs";

```

```

const s3Client = new S3Client({});
const oneMB = 1024 * 1024;

export const getObjectRange = ({ bucket, key, start, end }) => {
  const command = new GetObjectCommand({
    Bucket: bucket,
    Key: key,
    Range: `bytes=${start}-${end}`,
  });

  return s3Client.send(command);
};

/**
 * @param {string | undefined} contentRange
 */
export const getRangeAndLength = (contentRange) => {
  const [range, length] = contentRange.split("/");
  const [start, end] = range.split("-");
  return {
    start: Number.parseInt(start),
    end: Number.parseInt(end),
    length: Number.parseInt(length),
  };
};

export const isComplete = ({ end, length }) => end === length - 1;

const downloadInChunks = async ({ bucket, key }) => {
  const writeStream = createWriteStream(
    fileURLToPath(new URL(`./${key}`, import.meta.url)),
  ).on("error", (err) => console.error(err));

  let rangeAndLength = { start: -1, end: -1, length: -1 };

  while (!isComplete(rangeAndLength)) {
    const { end } = rangeAndLength;
    const nextRange = { start: end + 1, end: end + oneMB };

    const { ContentRange, Body } = await getObjectRange({
      bucket,
      key,
      ...nextRange,
    });
  }
};

```

```

    });
    console.log(`Downloaded bytes ${nextRange.start} to ${nextRange.end}`);

    writeStream.write(await Body.transformToByteArray());
    rangeAndLength = getRangeAndLength(ContentRange);
  }
};

/**
 * Download a large object from and Amazon S3 bucket.
 *
 * When downloading a large file, you might want to break it down into
 * smaller pieces. Amazon S3 accepts a Range header to specify the start
 * and end of the byte range to be downloaded.
 *
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
  try {
    await downloadInChunks({
      bucket: bucketName,
      key: key,
    });
  } catch (caught) {
    if (caught instanceof NoSuchKey) {
      console.error(`Failed to download object. No such key "${key}".`);
      rmSync(key);
    }
  }
};

```

Go

Per ulteriori informazioni sull'esempio di codice Go per il caricamento in più parti, consulta [Caricare o scaricare file di grandi dimensioni da e verso Amazon S3 utilizzando un SDK. AWS](#)

Example

Carica un oggetto di grandi dimensioni utilizzando un gestore di caricamento per suddividere i dati in parti e caricarli contemporaneamente.

```
import (
```

```

"bytes"
"context"
"errors"
"fmt"
"io"
"log"
"os"
"time"

"github.com/aws/aws-sdk-go-v2/aws"
"github.com/aws/aws-sdk-go-v2/feature/s3/manager"
"github.com/aws/aws-sdk-go-v2/service/s3"
"github.com/aws/aws-sdk-go-v2/service/s3/types"
"github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3) actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform bucket
// and object actions.
type BucketBasics struct {
    S3Client *s3.Client
}

```

```

// UploadLargeObject uses an upload manager to upload data to an object in a bucket.
// The upload manager breaks large data into parts and uploads the parts
// concurrently.
func (basics BucketBasics) UploadLargeObject(ctx context.Context, bucketName string,
    objectKey string, largeObject []byte) error {
    largeBuffer := bytes.NewReader(largeObject)
    var partMiBs int64 = 10
    uploader := manager.NewUploader(basics.S3Client, func(u *manager.Uploader) {
        u.PartSize = partMiBs * 1024 * 1024
    })
    _, err := uploader.Upload(ctx, &s3.PutObjectInput{
        Bucket: aws.String(bucketName),
        Key:     aws.String(objectKey),
        Body:    largeBuffer,
    })
    if err != nil {
        var apiErr smithy.APIError

```

```

if errors.As(err, &apiErr) && apiErr.ErrorCode() == "EntityTooLarge" {
    log.Printf("Error while uploading object to %s. The object is too large.\n"+
        "The maximum size for a multipart upload is 5TB.", bucketName)
} else {
    log.Printf("Couldn't upload large object to %v:%v. Here's why: %v\n",
        bucketName, objectKey, err)
}
} else {
    err = s3.NewObjectExistsWaiter(basics.S3Client).Wait(
        ctx, &s3.HeadObjectInput{Bucket: aws.String(bucketName), Key:
aws.String(objectKey)}, time.Minute)
    if err != nil {
        log.Printf("Failed attempt to wait for object %s to exist.\n", objectKey)
    }
}

return err
}

```

Example

Scarica un oggetto di grandi dimensioni utilizzando un gestore di download per ottenere i dati in parti e scaricarli contemporaneamente.

```

// DownloadLargeObject uses a download manager to download an object from a bucket.
// The download manager gets the data in parts and writes them to a buffer until all
// of
// the data has been downloaded.
func (basics BucketBasics) DownloadLargeObject(ctx context.Context, bucketName
string, objectKey string) ([]byte, error) {
    var partMiBs int64 = 10
    downloader := manager.NewDownloader(basics.S3Client, func(d *manager.Downloader) {
        d.PartSize = partMiBs * 1024 * 1024
    })
    buffer := manager.NewWriteAtBuffer([]byte{})
    _, err := downloader.Download(ctx, buffer, &s3.GetObjectInput{
        Bucket: aws.String(bucketName),
        Key:    aws.String(objectKey),
    })
    if err != nil {
        log.Printf("Couldn't download large object from %v:%v. Here's why: %v\n",

```

```
    bucketName, objectKey, err)
}
return buffer.Bytes(), err
}
```

PHP

Questo argomento spiega come utilizzare la `Aws\S3\Model\MultipartUpload\UploadBuilder` classe di alto livello di AWS SDK per PHP for multipart files uploads. Per ulteriori informazioni sull'API AWS SDK for Ruby, vai a SDK for Ruby - [AWS Version 2](#).

Il seguente esempio del PHP indica come caricare un file in un bucket Amazon S3. L'esempio dimostra come impostare i parametri per l'oggetto `MultipartUploader`.

```
require 'vendor/autoload.php';

use Aws\Exception\MultipartUploadException;
use Aws\S3\MultipartUploader;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Prepare the upload parameters.
$uploader = new MultipartUploader($s3, '/path/to/large/file.zip', [
    'bucket' => $bucket,
    'key'    => $keyname
]);

// Perform the upload.
try {
    $result = $uploader->upload();
    echo "Upload complete: {$result['ObjectURL']}" . PHP_EOL;
} catch (MultipartUploadException $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

Python

Il seguente esempio di codice mostra come caricare un oggetto utilizzando l'API Python di caricamento in più parti di alto livello (la classe `TransferManager`).

```
import sys
import threading

import boto3
from boto3.s3.transfer import TransferConfig

MB = 1024 * 1024
s3 = boto3.resource("s3")

class TransferCallback:
    """
    Handle callbacks from the transfer manager.

    The transfer manager periodically calls the __call__ method throughout
    the upload and download process so that it can take action, such as
    displaying progress to the user and collecting data about the transfer.
    """

    def __init__(self, target_size):
        self._target_size = target_size
        self._total_transferred = 0
        self._lock = threading.Lock()
        self.thread_info = {}

    def __call__(self, bytes_transferred):
        """
        The callback method that is called by the transfer manager.

        Display progress during file transfer and collect per-thread transfer
        data. This method can be called by multiple threads, so shared instance
        data is protected by a thread lock.
        """
        thread = threading.current_thread()
        with self._lock:
            self._total_transferred += bytes_transferred
            if thread.ident not in self.thread_info.keys():
                self.thread_info[thread.ident] = bytes_transferred
```

```

        else:
            self.thread_info[thread.ident] += bytes_transferred

        target = self._target_size * MB
        sys.stdout.write(
            f"\r{self._total_transferred} of {target} transferred "
            f"({(self._total_transferred / target) * 100:.2f}%)."
        )
        sys.stdout.flush()

def upload_with_default_configuration(
    local_file_path, bucket_name, object_key, file_size_mb
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, using the default
    configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Callback=transfer_callback
    )
    return transfer_callback.thread_info

def upload_with_chunksize_and_meta(
    local_file_path, bucket_name, object_key, file_size_mb, metadata=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart chunk size and adding metadata to the Amazon S3 object.

    The multipart chunk size controls the size of the chunks of data that are
    sent in the request. A smaller chunk size typically results in the transfer
    manager using more threads for the upload.

    The metadata is a set of key-value pairs that are stored with the object
    in Amazon S3.
    """
    transfer_callback = TransferCallback(file_size_mb)

    config = TransferConfig(multipart_chunksize=1 * MB)
    extra_args = {"Metadata": metadata} if metadata else None
    s3.Bucket(bucket_name).upload_file(

```



```
        local_file_path,
        object_key,
        Config=config,
        ExtraArgs=extra_args,
        Callback=transfer_callback,
    )
    return transfer_callback.thread_info

def upload_with_high_threshold(local_file_path, bucket_name, object_key,
    file_size_mb):
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard upload instead of
    a multipart upload.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info

def upload_with_sse(
    local_file_path, bucket_name, object_key, file_size_mb, sse_key=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, adding server-side
    encryption with customer-provided encryption keys to the object.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)
    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).upload_file(
```

```
        local_file_path, object_key, ExtraArgs=extra_args,
        Callback=transfer_callback
    )
    return transfer_callback.thread_info

def download_with_default_configuration(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using the
    default configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Callback=transfer_callback
    )
    return transfer_callback.thread_info

def download_with_single_thread(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using a
    single thread.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(use_threads=False)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info

def download_with_high_threshold(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard download instead
```

```

of a multipart download.
"""
transfer_callback = TransferCallback(file_size_mb)
config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
s3.Bucket(bucket_name).Object(object_key).download_file(
    download_file_path, Config=config, Callback=transfer_callback
)
return transfer_callback.thread_info

def download_with_sse(
    bucket_name, object_key, download_file_path, file_size_mb, sse_key
):
    """
    Download a file from an Amazon S3 bucket to a local folder, adding a
    customer-provided encryption key to the request.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)

    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, ExtraArgs=extra_args, Callback=transfer_callback
    )
    return transfer_callback.thread_info

```

Utilizzo di AWS SDK (API di basso livello)

L'AWS SDK espone un'API di basso livello che assomiglia molto all'API REST di Amazon S3 per i caricamenti in più parti (vedi. [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#)). Utilizza l'API di basso livello quando devi mettere in pausa e riprendere i caricamenti in più parti, variare le dimensioni delle parti durante il caricamento o non conosci in anticipo la dimensione dei dati di caricamento. Se non hai questi requisiti, utilizza l'API di alto livello (vedi. [Utilizzo di AWS SDK \(API di alto livello\)](#)).

Java

L'esempio che segue mostra come utilizzare le classi Java di basso livello per il caricamento di un file. Tale esempio esegue i seguenti passaggi:

- Avvia un caricamento in più parti usando il metodo `AmazonS3Client.initiateMultipartUpload()` e passa un oggetto `InitiateMultipartUploadRequest`.
- Salva l'ID di caricamento che viene restituito dal metodo `AmazonS3Client.initiateMultipartUpload()`. Questo ID di caricamento deve essere specificato per ogni operazione di caricamento in più parti successiva.
- Carica le parti dell'oggetto. Per ogni parte, occorre chiamare il metodo `AmazonS3Client.uploadPart()`. Le informazioni sul caricamento della parte devono essere fornite usando un oggetto `UploadPartRequest`.
- Per ogni parte, salva l'ETag dalla risposta del metodo `AmazonS3Client.uploadPart()` in un elenco. I valori dell'ETag vengono utilizzati per completare il caricamento in più parti.
- Chiama il metodo `AmazonS3Client.completeMultipartUpload()` per completare il caricamento in più parti.

Example

Per istruzioni su come creare e testare un campione funzionante, consulta [Getting Started](#) nella AWS SDK per Java Developer Guide.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

public class LowLevelMultipartUpload {
```

```
public static void main(String[] args) throws IOException {
    Regions clientRegion = Regions.DEFAULT_REGION;
    String bucketName = "**** Bucket name ****";
    String keyName = "**** Key name ****";
    String filePath = "**** Path to file to upload ****";

    File file = new File(filePath);
    long contentLength = file.length();
    long partSize = 5 * 1024 * 1024; // Set part size to 5 MB.

    try {
        AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
            .withRegion(clientRegion)
            .withCredentials(new ProfileCredentialsProvider())
            .build();

        // Create a list of ETag objects. You retrieve ETags for each object
part
        // uploaded,
        // then, after each individual part has been uploaded, pass the list of
ETags to
        // the request to complete the upload.
        List<PartETag> partETags = new ArrayList<PartETag>();

        // Initiate the multipart upload.
        InitiateMultipartUploadRequest initRequest = new
InitiateMultipartUploadRequest(bucketName, keyName);
        InitiateMultipartUploadResult initResponse =
s3Client.initiateMultipartUpload(initRequest);

        // Upload the file parts.
        long filePosition = 0;
        for (int i = 1; filePosition < contentLength; i++) {
            // Because the last part could be less than 5 MB, adjust the part
size as
            // needed.
            partSize = Math.min(partSize, (contentLength - filePosition));

            // Create the request to upload a part.
            UploadPartRequest uploadRequest = new UploadPartRequest()
                .withBucketName(bucketName)
                .withKey(keyName)
                .withUploadId(initResponse.getUploadId())
```

```
        .withPartNumber(i)
        .withFileOffset(filePosition)
        .withFile(file)
        .withPartSize(partSize);

        // Upload the part and add the response's ETag to our list.
        UploadPartResult uploadResult = s3Client.uploadPart(uploadRequest);
        partETags.add(uploadResult.getPartETag());

        filePosition += partSize;
    }

    // Complete the multipart upload.
    CompleteMultipartUploadRequest compRequest = new
CompleteMultipartUploadRequest(bucketName, keyName,
        initResponse.getUploadId(), partETags);
    s3Client.completeMultipartUpload(compRequest);
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it, so it returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
```

.NET

Il seguente esempio in C# mostra come utilizzare l'API di caricamento SDK per .NET multipart di basso livello per caricare un file in un bucket S3. Per informazioni sul caricamento in più parti di Amazon S3, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Note

Quando si utilizza l' SDK per .NET API per caricare oggetti di grandi dimensioni, potrebbe verificarsi un timeout durante la scrittura dei dati nel flusso di richieste. Puoi impostare un timeout esplicito utilizzando la richiesta UploadPartRequest.

Il seguente esempio di codice #C mostra come caricare un file in un bucket S3 utilizzando l'API per il caricamento in più parti di basso livello. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella AWS SDK for .NET Developer Guide.

```
using Amazon;
using Amazon.Runtime;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPULowLevelAPITest
    {
        private const string bucketName = "**** provide bucket name ****";
        private const string keyName = "**** provide a name for the uploaded object
****";
        private const string filePath = "**** provide the full path name of the file
to upload ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Uploading an object");
            UploadObjectAsync().Wait();
        }

        private static async Task UploadObjectAsync()
        {
            // Create list to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();

            // Setup information required to initiate the multipart upload.
```

```
        InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
    {
        BucketName = bucketName,
        Key = keyName
    };

    // Initiate the upload.
    InitiateMultipartUploadResponse initResponse =
        await s3Client.InitiateMultipartUploadAsync(initiateRequest);

    // Upload parts.
    long contentLength = new FileInfo(filePath).Length;
    long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

    try
    {
        Console.WriteLine("Uploading parts");

        long filePosition = 0;
        for (int i = 1; filePosition < contentLength; i++)
        {
            UploadPartRequest uploadRequest = new UploadPartRequest
            {
                BucketName = bucketName,
                Key = keyName,
                UploadId = initResponse.UploadId,
                PartNumber = i,
                PartSize = partSize,
                FilePosition = filePosition,
                FilePath = filePath
            };

            // Track upload progress.
            uploadRequest.StreamTransferProgress +=
                new
EventHandler<StreamTransferProgressArgs>(UploadPartProgressEventCallback);

            // Upload a part and add the response to our list.
            uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

            filePosition += partSize;
        }
    }
```



```
        // Setup to complete the upload.
        CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
        {
            BucketName = bucketName,
            Key = keyName,
            UploadId = initResponse.UploadId
        };
        completeRequest.AddPartETags(uploadResponses);

        // Complete the upload.
        CompleteMultipartUploadResponse completeUploadResponse =
            await s3Client.CompleteMultipartUploadAsync(completeRequest);
    }
    catch (Exception exception)
    {
        Console.WriteLine("An AmazonS3Exception was thrown: { 0}",
exception.Message);

        // Abort the upload.
        AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
        {
            BucketName = bucketName,
            Key = keyName,
            UploadId = initResponse.UploadId
        };
        await s3Client.AbortMultipartUploadAsync(abortMPURequest);
    }
}

public static void UploadPartProgressEventCallback(object sender,
StreamTransferProgressArgs e)
{
    // Process event.
    Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
}
}
}
```

PHP

Questo argomento mostra come utilizzare il `uploadPart` metodo di basso livello della versione 3 AWS SDK per PHP per caricare un file in più parti. Per ulteriori informazioni sull'API AWS SDK for Ruby, vai a [AWS SDK for Ruby - Version 2](#).

Il seguente esempio di codice PHP mostra come caricare un file in un bucket Amazon S3 utilizzando il caricamento in più parti con l'API del PHP di basso livello.

```
require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$filename = '*** Path to and Name of the File to Upload ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

$result = $s3->createMultipartUpload([
    'Bucket'      => $bucket,
    'Key'         => $keyname,
    'StorageClass' => 'REDUCED_REDUNDANCY',
    'Metadata'    => [
        'param1' => 'value 1',
        'param2' => 'value 2',
        'param3' => 'value 3'
    ]
]);

$uploadId = $result['UploadId'];

// Upload the file in parts.
try {
    $file = fopen($filename, 'r');
    $partNumber = 1;
    while (!feof($file)) {
        $result = $s3->uploadPart([
            'Bucket'      => $bucket,
            'Key'         => $keyname,
```

```

        'UploadId'    => $uploadId,
        'PartNumber' => $partNumber,
        'Body'        => fread($file, 5 * 1024 * 1024),
    ]);
    $parts['Parts'][$partNumber] = [
        'PartNumber' => $partNumber,
        'ETag'       => $result['ETag'],
    ];
    $partNumber++;

    echo "Uploading part $partNumber of $filename." . PHP_EOL;
}
fclose($file);
} catch (S3Exception $e) {
    $result = $s3->abortMultipartUpload([
        'Bucket'    => $bucket,
        'Key'        => $keyname,
        'UploadId' => $uploadId
    ]);

    echo "Upload of $filename failed." . PHP_EOL;
}

// Complete the multipart upload.
$result = $s3->completeMultipartUpload([
    'Bucket'    => $bucket,
    'Key'        => $keyname,
    'UploadId' => $uploadId,
    'MultipartUpload' => $parts,
]);
$url = $result['Location'];

echo "Uploaded $filename to $url." . PHP_EOL;

```

Utilizzo di AWS SDK per Ruby

La AWS SDK per Ruby versione 3 supporta i caricamenti multipart di Amazon S3 in due modi. Il primo metodo prevede la possibilità di utilizzare caricamenti file gestiti. Per ulteriori informazioni, consulta la sezione [Caricamento di file in Amazon S3](#) nel Blog per sviluppatori di AWS . I caricamenti file gestiti rappresentano il metodo consigliato per caricare i file in un bucket. Offrono i seguenti vantaggi:

- Gestiscono i caricamenti in più parti per gli oggetti con una dimensione maggiore di 15 MB.
- Aprono correttamente i file in modalità binaria per evitare problemi di codifica.
- Utilizzano più thread per il caricamento in parallelo delle parti degli oggetti di grandi dimensioni.

In alternativa, è possibile utilizzare direttamente le seguenti operazioni del client di caricamento in più parti:

- [create_multipart_upload](#) - Avvia un caricamento in più parti e restituisce un ID di caricamento.
- [upload_part](#) - Carica una parte in un caricamento in più parti.
- [upload_part_copy](#) - Carica una parte copiando i dati da un oggetto esistente come origine dati.
- [complete_multipart_upload](#) - Completa un caricamento in più parti assemblando le parti caricate in precedenza.
- [abort_multipart_upload](#) - Interrompe un caricamento in più parti.

Caricamento di una directory utilizzando la classe .NET di alto livello TransferUtility

Puoi utilizzare la classe `TransferUtility` per caricare un'intera directory. Per impostazione predefinita, l'API carica solo i file nella posizione root della directory specificata. È tuttavia possibile specificare il caricamento ricorsivo dei file in tutte le sottodirectory.

Per selezionare i file nella directory specificata in base ai criteri di filtro, specificare espressioni di filtro. Ad esempio, per caricare solo i file PDF da una directory, specifica l'espressione del filtro `"*.pdf"`.

Quando si caricano file da una directory, non è possibile specificare i nomi delle chiavi per l'oggetto risultante. Amazon S3 crea i nomi delle chiavi utilizzando il percorso file originale. Supponiamo, ad esempio, di avere una directory denominata `c:\myfolder` con la seguente struttura:

Example

```
C:\myfolder
  \a.txt
  \b.pdf
  \media\
    An.mp3
```

Quando effettui un caricamento in questa directory, Amazon S3 utilizza questi nomi della chiave dell'oggetto:

Example

```
a.txt  
b.pdf  
media/An.mp3
```

Example

Il seguente esempio di codice C# consente di caricare una directory in un bucket Amazon S3. Mostra come utilizzare diversi overload `TransferUtility.UploadDirectory` per caricare la directory. Ciascuna chiamata successiva al caricamento sostituisce il caricamento precedente. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;  
using Amazon.S3;  
using Amazon.S3.Transfer;  
using System;  
using System.IO;  
using System.Threading.Tasks;  
  
namespace Amazon.DocSamples.S3  
{  
    class UploadDirMPUHighLevelAPITest  
    {  
        private const string existingBucketName = "*** bucket name ***";  
        private const string directoryPath = @"*** directory path ***";  
        // The example uploads only .txt files.  
        private const string wildCard = "*.txt";  
        // Specify your bucket region (an example region is shown).  
        private static readonly RegionEndpoint bucketRegion = RegionEndpoint.USWest2;  
        private static IAmazonS3 s3Client;  
        static void Main()  
        {  
            s3Client = new AmazonS3Client(bucketRegion);  
            UploadDirAsync().Wait();  
        }  
  
        private static async Task UploadDirAsync()  
        {  
            try  
            {
```

```
var directoryTransferUtility =
    new TransferUtility(s3Client);

// 1. Upload a directory.
await directoryTransferUtility.UploadDirectoryAsync(directoryPath,
    existingBucketName);
Console.WriteLine("Upload statement 1 completed");

// 2. Upload only the .txt files from a directory
//    and search recursively.
await directoryTransferUtility.UploadDirectoryAsync(
    directoryPath,
    existingBucketName,
    wildCard,
    SearchOption.AllDirectories);
Console.WriteLine("Upload statement 2 completed");

// 3. The same as Step 2 and some optional configuration.
//    Search recursively for .txt files to upload.
var request = new TransferUtilityUploadDirectoryRequest
{
    BucketName = existingBucketName,
    Directory = directoryPath,
    SearchOption = SearchOption.AllDirectories,
    SearchPattern = wildCard
};

await directoryTransferUtility.UploadDirectoryAsync(request);
Console.WriteLine("Upload statement 3 completed");
}
catch (AmazonS3Exception e)
{
    Console.WriteLine(
        "Error encountered ***. Message:'{0}' when writing an object",
e.Message);
}
catch (Exception e)
{
    Console.WriteLine(
        "Unknown encountered on server. Message:'{0}' when writing an
object", e.Message);
}
}
```

```
}
```

Elenco dei caricamenti in più parti

Puoi utilizzare l' AWS CLI API REST o gli AWS SDK per recuperare un elenco di caricamenti multiparte in corso in Amazon S3. Puoi usare il caricamento in più parti per caricare un singolo oggetto a livello di programmazione su Amazon S3. I caricamenti multiparte spostano gli oggetti in Amazon S3 spostando una parte dei dati di un oggetto alla volta. Per informazioni più generiche sui caricamenti multiparte, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Per una procedura end-to-end che dimostra come caricare un oggetto utilizzando il caricamento multiparte con un checksum aggiuntivo, consulta [Esercitazione: caricamento di un oggetto tramite caricamento multiparte per verificarne l'integrità dei dati](#).

La sezione seguente mostra come elencare i caricamenti multiparte in corso con l'API REST di Amazon S3 e gli AWS Command Line Interface SDK. AWS

Elencare i caricamenti in più parti utilizzando il AWS CLI

Le seguenti sezioni AWS Command Line Interface descrivono le operazioni per elencare i caricamenti composti da più parti.

- [list-parts](#): elenca le parti caricate di un caricamento in più parti specifico.
- [list-multipart-upload](#): elenca i caricamenti in più parti in corso.

Elenco dei caricamenti in più parti tramite REST API

Le sezioni seguenti della Documentazione di riferimento delle API di Amazon Simple Storage Service descrivono REST API per l'elenco dei caricamenti in più parti.

- [ListParts](#)-elenca le parti caricate per un caricamento multiparte specifico.
- [ListMultipartUploads](#)-elenca i caricamenti multiparte in corso.

Elencare i caricamenti in più parti utilizzando il AWS SDK (API di basso livello)

Java

Per elencare tutti i caricamenti multiparte in corso su un bucket utilizzando l' AWS SDK per Java, puoi utilizzare le classi API di basso livello per:

Low-level Processo di elenco dei caricamenti in più parti di API

1	Creare un'istanza della classe <code>ListMultipartUploadsRequest</code> e specificare il nome del bucket.
2	Eseguire il metodo <code>listMultipartUploads</code> <code>S3Client</code> . Questo metodo restituisce un'istanza della classe <code>ListMultipartUploadsResponse</code> che fornisce le informazioni sui caricamenti in più parti in corso.

Per esempi di come elencare i caricamenti in più parti con l' AWS SDK per Java, consulta [Elencare i caricamenti in più parti nell'Amazon S3 API Reference](#).

.NET

Per elencare tutti i caricamenti in più parti in corso in uno specifico bucket, utilizza la classe `ListMultipartUploadsRequest` dell'API di basso livello di SDK per .NET per il caricamento in più parti. Il metodo `AmazonS3Client.ListMultipartUploads` restituisce un'istanza della classe `ListMultipartUploadsResponse` che fornisce informazioni sui caricamenti in più parti in corso.

Un caricamento in più parti in corso è un caricamento che è stato avviato utilizzando la richiesta `Initiate Multipart Upload`, ma che non è ancora stato completato o interrotto. Per ulteriori informazioni sui caricamenti in più parti di Amazon S3, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Il seguente esempio in C# mostra come utilizzare per elencare tutti i caricamenti multiparte SDK per .NET in corso su un bucket. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET Developer Guide. AWS

```
ListMultipartUploadsRequest request = new ListMultipartUploadsRequest
{
    BucketName = bucketName // Bucket receiving the uploads.
};

ListMultipartUploadsResponse response = await
    AmazonS3Client.ListMultipartUploadsAsync(request);
```


PHP

Questo argomento mostra come utilizzare le classi API di basso livello della versione 3 AWS SDK per PHP per elencare tutti i caricamenti multiparte in corso su un bucket. Per ulteriori informazioni sull'API AWS SDK for Ruby, vai a [SDK for Ruby - Version 2](#). [AWS](#)

Il seguente esempio di codice PHP mostra come creare un elenco di tutti i caricamenti in più parti in corso in un bucket.

```
require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Retrieve a list of the current multipart uploads.
$result = $s3->listMultipartUploads([
    'Bucket' => $bucket
]);

// Write the list of uploads to the page.
print_r($result->toArray());
```

Monitoraggio di un caricamento in più parti con AWS SDK

È possibile seguire l'avanzamento del caricamento di un oggetto su Amazon S3 con un'interfaccia listen. L'API di caricamento multiparte di alto livello fornisce un'interfaccia listen, chiamata `ProgressListener`. Gli eventi di stato si verificano periodicamente e inviano al listener la notifica dell'avvenuto trasferimento dei dati. Per informazioni più generiche sui caricamenti multiparte, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Per una procedura end-to-end che dimostra come caricare un oggetto utilizzando il caricamento multiparte con un checksum aggiuntivo, consulta [Esercitazione: caricamento di un oggetto tramite caricamento multiparte per verificarne l'integrità dei dati](#).

La sezione seguente mostra come tenere traccia di un caricamento in più parti con gli AWS SDK.

Java

Example

Il seguente codice Java carica un file e utilizza `ExecutionInterceptor` per monitorare lo stato del caricamento. Per istruzioni su come creare e testare un campione funzionante, consulta [Getting Started](#) nella AWS SDK per Java 2.x Developer Guide.

```
import java.nio.file.Paths;

import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.core.async.AsyncRequestBody;
import software.amazon.awssdk.core.interceptor.Context;
import software.amazon.awssdk.core.interceptor.ExecutionAttributes;
import software.amazon.awssdk.core.interceptor.ExecutionInterceptor;
import software.amazon.awssdk.services.s3.S3AsyncClient;
import software.amazon.awssdk.services.s3.model.PutObjectRequest;

public class TrackMPUProgressUsingHighLevelAPI {

    static class ProgressListener implements ExecutionInterceptor {
        private long transferredBytes = 0;

        @Override
        public void beforeTransmission(Context.BeforeTransmission context,
            ExecutionAttributes executionAttributes) {
            if (context.httpRequest().firstMatchingHeader("Content-
Length").isPresent()) {
                String contentLength =
context.httpRequest().firstMatchingHeader("Content-Length").get();
                long partSize = Long.parseLong(contentLength);
                transferredBytes += partSize;
                System.out.println("Transferred bytes: " + transferredBytes);
            }
        }
    }

    public static void main(String[] args) throws Exception {
        String existingBucketName = "**** Provide bucket name ****";
        String keyName = "**** Provide object key ****";
        String filePath = "**** file to upload ****";
```

```

        S3AsyncClient s3Client = S3AsyncClient.builder()
            .credentialsProvider(ProfileCredentialsProvider.create())
            .overrideConfiguration(c -> c.addExecutionInterceptor(new
ProgressListener()))
            .build();

        // For more advanced uploads, you can create a request object
        // and supply additional request parameters (ex: progress listeners,
        // canned ACLs, etc.)
        PutObjectRequest request = PutObjectRequest.builder()
            .bucket(existingBucketName)
            .key(keyName)
            .build();

        AsyncRequestBody requestBody =
AsyncRequestBody.fromFile(Paths.get(filePath));

        // You can ask the upload for its progress, or you can
        // add a ProgressListener to your request to receive notifications
        // when bytes are transferred.
        // S3AsyncClient processes all transfers asynchronously,
        // so this call will return immediately.
        var upload = s3Client.putObject(request, requestBody);

        try {
            // You can block and wait for the upload to finish
            upload.join();
        } catch (Exception exception) {
            System.out.println("Unable to upload file, upload aborted.");
            exception.printStackTrace();
        } finally {
            s3Client.close();
        }
    }
}

```

.NET

Il seguente esempio di codice C# consente di caricare un file in un bucket S3 utilizzando la classe `TransferUtility` e monitorare lo stato di avanzamento del caricamento. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TrackMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide the bucket name ***";
        private const string keyName = "*** provide the name for the uploaded object
        ***";
        private const string filePath = " *** provide the full path name of the file
        to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
        RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            TrackMPUAsync().Wait();
        }

        private static async Task TrackMPUAsync()
        {
            try
            {
                var fileTransferUtility = new TransferUtility(s3Client);

                // Use TransferUtilityUploadRequest to configure options.
                // In this example we subscribe to an event.
                var uploadRequest =
                    new TransferUtilityUploadRequest
                    {
                        BucketName = bucketName,
                        FilePath = filePath,
                        Key = keyName
                    };
            }
        }
    }
}
```

```

        uploadRequest.UploadProgressEvent +=
            new EventHandler<UploadProgressArgs>
                (uploadRequest_UploadPartProgressEvent);

        await fileTransferUtility.UploadAsync(uploadRequest);
        Console.WriteLine("Upload completed");
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
}

static void uploadRequest_UploadPartProgressEvent(object sender,
UploadProgressArgs e)
{
    // Process event.
    Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
}
}
}

```

Interruzione di un caricamento in più parti

Dopo aver avviato un caricamento in più parti, le parti vengono caricate. Amazon S3 memorizza queste parti e crea l'oggetto solo dopo aver caricato tutte le parti e aver inviato una richiesta per completare il caricamento multiparte. Quando riceve la richiesta di completamento del caricamento in più parti, Amazon S3 assembla le parti e crea un oggetto. Se la richiesta di caricamento multiparte completa non viene inviata correttamente, S3 non assembla le parti e non crea alcun oggetto. Se si desidera non completare un caricamento multiparte dopo aver caricato le parti, è necessario interrompere il caricamento multiparte.

Ti viene addebitato tutto lo spazio di storage associato alle parti caricate. Si consiglia di completare sempre il caricamento multiparte o di interromperlo per rimuovere le parti caricate. Per ulteriori informazioni sui prezzi, consultare [Caricamento in più parti e prezzi](#).

È inoltre possibile interrompere un caricamento in più parti incompleto utilizzando una configurazione del ciclo di vita del bucket. Per ulteriori informazioni, consulta [Configurazione del ciclo di vita del bucket per l'eliminazione dei caricamenti in più parti incompleti](#).

La sezione seguente mostra come interrompere un caricamento multiparte in corso in Amazon S3 utilizzando l'API REST o gli AWS Command Line Interface SDK. AWS

Utilizzo di AWS CLI

Per ulteriori informazioni sull'utilizzo di per interrompere un caricamento in più parti, consulta <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/abort-multipart-upload.html> abort-multipart-upload nel Command Reference. AWS CLI AWS CLI

Utilizzo della REST API

Per ulteriori informazioni sull'utilizzo dell'API REST per interrompere un caricamento in più parti, consulta Amazon Simple Storage Service API [AbortMultipartUpload](#) Reference.

Utilizzo di AWS SDK (API di alto livello)

Java

Per interrompere i caricamenti in più parti in corso utilizzando l' AWS SDK per Java, puoi interrompere i caricamenti avviati prima di una data specificata e ancora in corso. Un caricamento è considerato in esecuzione dopo l'avvio e finché non viene completato o interrotto.

Per arrestare i caricamenti in più parti, puoi:

1	Creare un'istanza S3Client.
2	Utilizzare i metodi di interruzione del client passando il nome del bucket e altri parametri richiesti.

Note

È anche possibile interrompere un caricamento in più parti specifico. Per ulteriori informazioni, consulta [Utilizzo di AWS SDK \(API di basso livello\)](#).

Per esempi di come interrompere i caricamenti in più parti con l' AWS SDK per Java, consulta [Cancel a multipart upload nell'Amazon S3 API Reference](#).

.NET

L'esempio di codice C# seguente interrompe l'esecuzione di tutti i caricamenti in più parti avviati su un bucket nella settimana precedente. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET Developer Guide. AWS

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class AbortMPUUsingHighLevelAPITest
    {
        private const string bucketName = "**** provide bucket name ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
            RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            AbortMPUAsync().Wait();
        }

        private static async Task AbortMPUAsync()
        {
            try
            {
                var transferUtility = new TransferUtility(s3Client);

                // Abort all in-progress uploads initiated before the specified
                date.

                await transferUtility.AbortMultipartUploadsAsync(
                    bucketName, DateTime.Now.AddDays(-7));
            }
        }
    }
}
```

```
        catch (AmazonS3Exception e)
        {
            Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
        }
        catch (Exception e)
        {
            Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
        }
    }
}
```

Note

È anche possibile interrompere un caricamento in più parti specifico. Per ulteriori informazioni, consulta [Utilizzo di AWS SDK \(API di basso livello\)](#).

Utilizzo di AWS SDK (API di basso livello)

È possibile interrompere l'esecuzione di un caricamento in più parti chiamando il metodo `AmazonS3.abortMultipartUpload`. Questo metodo elimina tutte le parti che sono state caricate in Amazon S3 e libera le risorse. È necessario specificare l'ID di caricamento, il nome del bucket e il nome della chiave. Il seguente esempio di codice Java mostra come interrompere l'esecuzione di un caricamento in più parti.

Per interrompere un caricamento in più parti, devi fornire l'ID di caricamento e i nomi di bucket e chiave utilizzati nel caricamento. Dopo aver interrotto un caricamento in più parti, non puoi utilizzare l'ID di caricamento per caricare altre parti. Per ulteriori informazioni sui caricamenti in più parti di Amazon S3, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Java

Per interrompere uno specifico caricamento in più parti in corso utilizzando l' AWS SDK per Java, puoi utilizzare l'API di basso livello per interrompere il caricamento fornendo il nome del bucket, la chiave dell'oggetto e l'ID di caricamento.

 Note

Invece di interrompere un caricamento in più parti specifico, è possibile arrestare tutti i caricamenti in più parti avviati prima di un orario specifico che sono ancora in corso. Questa operazione di pulizia è utile per interrompere caricamenti in più parti obsoleti che sono stati avviati ma che non sono stati completati o interrotti. Per ulteriori informazioni, consulta [Utilizzo di AWS SDK \(API di alto livello\)](#).

Per esempi di come interrompere un caricamento multiparte specifico con l' AWS SDK per Java, consulta [Annullare un caricamento in più parti nell'API Reference di Amazon S3](#).

.NET

L'esempio di codice #C seguente mostra come interrompere un caricamento in più parti. Per un esempio in C# completo che include il codice seguente, consulta [Utilizzo di AWS SDK \(API di basso livello\)](#).

```
AbortMultipartUploadRequest abortMPURequest = new AbortMultipartUploadRequest
{
    BucketName = existingBucketName,
    Key = keyName,
    UploadId = initResponse.UploadId
};
await AmazonS3Client.AbortMultipartUploadAsync(abortMPURequest);
```

Puoi anche interrompere tutti i caricamenti in più parti in corso che sono stati avviati prima di un determinato orario. Questa operazione di pulizia è utile per interrompere caricamenti in più parti che non sono stati completati o interrotti. Per ulteriori informazioni, consulta [Utilizzo di AWS SDK \(API di alto livello\)](#).

PHP

Questo esempio mostra come utilizzare una classe dalla versione 3 di AWS SDK per PHP per interrompere un caricamento in più parti in corso. Per ulteriori informazioni sull'API AWS SDK for Ruby, consulta SDK for Ruby - Version 2. [AWS](#) Nell'esempio il metodo `abortMultipartUpload()`.

Per ulteriori informazioni sull'API AWS SDK for Ruby, vai a SDK for Ruby - Version [AWS 2](#).

```
require 'vendor/autoload.php';
```

```
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$uploadId = '*** Upload ID of upload to Abort ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region' => 'us-east-1'
]);

// Abort the multipart upload.
$s3->abortMultipartUpload([
    'Bucket' => $bucket,
    'Key' => $keyname,
    'UploadId' => $uploadId,
]);
```

Copia di un oggetto utilizzando il caricamento in più parti

Il caricamento multipart consente di copiare oggetti su un insieme di parti. Gli esempi in questa sezione mostrano come copiare oggetti con dimensioni superiori a 5 GB utilizzando l'API per il caricamento in più parti. Per informazioni sui caricamenti multipart, consulta [Caricamento e copia di oggetti utilizzando il caricamento multipart in Amazon S3](#).

È possibile copiare oggetti inferiori a 5 GB in una singola operazione senza utilizzare l'API di caricamento multipart. Puoi copiare oggetti inferiori a 5 GB utilizzando l'API REST Console di gestione AWS AWS CLI, o gli SDK. AWS Per ulteriori informazioni, consulta [Copia, spostamento e denominazione di oggetti](#).

Per una procedura end-to-end che dimostra come caricare un oggetto utilizzando il caricamento multipart con un checksum aggiuntivo, consulta [Esercitazione: caricamento di un oggetto tramite caricamento multipart per verificarne l'integrità dei dati](#).

La sezione seguente mostra come copiare un oggetto con caricamento in più parti con l'API REST o AWS gli SDK.

Utilizzo della REST API

Le sezioni seguenti della Documentazione di riferimento delle API di Amazon Simple Storage Service descrivono REST API per il caricamento in più parti. Per copiare un oggetto esistente, utilizza l'API Upload Part (Copy) e specifica l'oggetto di origine aggiungendo l'intestazione `x-amz-copy-source` nella richiesta.

- [Avvio del caricamento in più parti](#)
- [Upload Part](#)
- [Upload Part \(Copy\)](#)
- [Completamento del caricamento in più parti](#)
- [Abort Multipart Upload](#)
- [List Parts](#)
- [Elenco dei caricamenti in più parti](#)

Si possono utilizzare queste API per effettuare richieste REST personalizzate oppure è possibile utilizzare uno degli SDK forniti da noi. Per ulteriori informazioni sull'utilizzo di Multipart Upload con, vedere. AWS CLI [Utilizzo di AWS CLI](#) Per ulteriori informazioni sugli SDK, consulta [AWS Supporto SDK per il caricamento in più parti](#).

Utilizzo di AWS SDK

Per copiare un oggetto utilizzando l'API di basso livello, effettua le seguenti operazioni:

- Avvia il caricamento in più parti chiamando il metodo `AmazonS3Client.initiateMultipartUpload()`.
- Salvare l'ID caricamento dall'oggetto della risposta restituito dal metodo `AmazonS3Client.initiateMultipartUpload()`. Si fornisce questo ID di caricamento per ciascuna operazione di caricamento di parte.
- Copia tutte le parti. Per ciascuna parte che è necessario copiare, creare una nuova istanza della classe `CopyPartRequest`. Fornisci le informazioni sulla parte, inclusi i nomi bucket di origine e destinazione, le chiavi dell'oggetto di origine e destinazione, l'ID di caricamento, le posizioni dei primi e degli ultimi byte della parte e il numero della parte.
- Salva le risposte che il metodo `AmazonS3Client.copyPart()` chiama. Ogni risposta include il valore ETag e il numero della parte per la parte caricata. Tali informazioni saranno necessarie per completare il caricamento in più parti.

- Chiama il metodo `AmazonS3Client.completeMultipartUpload()` per completare l'operazione di copia.

Java

Per esempi di come copiare oggetti utilizzando il caricamento in più parti con l' AWS SDK per Java, consulta [Copiare parte di un oggetto da un altro oggetto](#) nell'API Reference di Amazon S3.

.NET

Il seguente esempio in C# mostra come copiare un oggetto Amazon S3 di dimensioni superiori a 5 GB da una posizione di origine a un'altra, ad esempio da un bucket all'altro. Per copiare gli oggetti con dimensioni inferiori a 5 GB, utilizza la procedura di copia in una sola operazione come descritto in [Utilizzo di AWS SDK](#). Per ulteriori informazioni sui caricamenti in più parti di Amazon S3, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Questo esempio mostra come copiare un oggetto Amazon S3 di dimensioni superiori a 5 GB da un bucket S3 a un altro utilizzando l'API di caricamento in più parti. SDK per .NET

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CopyObjectUsingMPUapiTest
    {
        private const string sourceBucket = "*** provide the name of the bucket with source object ***";
        private const string targetBucket = "*** provide the name of the bucket to copy the object to ***";
        private const string sourceObjectKey = "*** provide the name of object to copy ***";
        private const string targetObjectKey = "*** provide the name of the object copy ***";
        // Specify your bucket region (an example region is shown).
```

```
private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
private static IAmazonS3 s3Client;

public static void Main()
{
    s3Client = new AmazonS3Client(bucketRegion);
    Console.WriteLine("Copying an object");
    MPUCopyObjectAsync().Wait();
}
private static async Task MPUCopyObjectAsync()
{
    // Create a list to store the upload part responses.
    List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();
    List<CopyPartResponse> copyResponses = new List<CopyPartResponse>();

    // Setup information required to initiate the multipart upload.
    InitiateMultipartUploadRequest initiateRequest =
        new InitiateMultipartUploadRequest
        {
            BucketName = targetBucket,
            Key = targetObjectKey
        };

    // Initiate the upload.
    InitiateMultipartUploadResponse initResponse =
        await s3Client.InitiateMultipartUploadAsync(initiateRequest);

    // Save the upload ID.
    String uploadId = initResponse.UploadId;

    try
    {
        // Get the size of the object.
        GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest
        {
            BucketName = sourceBucket,
            Key = sourceObjectKey
        };

        GetObjectMetadataResponse metadataResponse =
            await s3Client.GetObjectMetadataAsync(metadataRequest);
```

```
long objectSize = metadataResponse.ContentLength; // Length in
bytes.

// Copy the parts.
long partSize = 5 * (long)Math.Pow(2, 20); // Part size is 5 MB.

long bytePosition = 0;
for (int i = 1; bytePosition < objectSize; i++)
{
    CopyPartRequest copyRequest = new CopyPartRequest
    {
        DestinationBucket = targetBucket,
        DestinationKey = targetObjectKey,
        SourceBucket = sourceBucket,
        SourceKey = sourceObjectKey,
        UploadId = uploadId,
        FirstByte = bytePosition,
        LastByte = bytePosition + partSize - 1 >= objectSize ?
objectSize - 1 : bytePosition + partSize - 1,
        PartNumber = i
    };

    copyResponses.Add(await s3Client.CopyPartAsync(copyRequest));

    bytePosition += partSize;
}

// Set up to complete the copy.
CompleteMultipartUploadRequest completeRequest =
new CompleteMultipartUploadRequest
{
    BucketName = targetBucket,
    Key = targetObjectKey,
    UploadId = initResponse.UploadId
};
completeRequest.AddPartETags(copyResponses);

// Complete the copy.
CompleteMultipartUploadResponse completeUploadResponse =
    await s3Client.CompleteMultipartUploadAsync(completeRequest);
}
catch (AmazonS3Exception e)
{

```

```
        Console.WriteLine("Error encountered on server. Message:'{0}' when  
writing an object", e.Message);  
    }  
    catch (Exception e)  
    {  
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when  
writing an object", e.Message);  
    }  
}  
}
```

Esercitazione: caricamento di un oggetto tramite caricamento multiparte per verificarne l'integrità dei dati

Il caricamento in più parti consente di caricare un singolo oggetto come un insieme di parti. Ciascuna parte è una parte contigua dei dati dell'oggetto. È possibile caricare queste parti dell'oggetto in modo indipendente e in qualsiasi ordine. Se la trasmissione di una parte non riesce, è possibile ritrasmettere tale parte senza influire sulle altre. Una volta caricate tutte le parti dell'oggetto, Amazon S3 le assembla e crea l'oggetto. In generale, quando la dimensione dell'oggetto raggiunge i 100 MB, si consiglia di valutare la possibilità di eseguire caricamenti in più parti anziché caricare l'oggetto in una singola operazione. Per ulteriori informazioni sui caricamenti in più parti, consulta la sezione [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#). Per i limiti relativi ai caricamenti multiparte, consulta [Limiti del caricamenti in più parti di Amazon S3](#).

È possibile utilizzare i checksum per verificare che le risorse non vengano alterate quando vengono copiate. L'esecuzione di un checksum consiste nell'utilizzare un algoritmo per iterare sequenzialmente su ogni byte di un file. Amazon S3 offre diverse opzioni di checksum per verificare l'integrità dei dati. Si consiglia di eseguire questi controlli di integrità come best practice di durata e per confermare che ogni byte viene trasferito senza alterazioni. Amazon S3 supporta anche i seguenti algoritmi: SHA-1, SHA-256 CRC32 e CRC32C. Amazon S3 utilizza uno o più di questi algoritmi per calcolare un valore di checksum aggiuntivo e memorizzarlo come parte dei metadati dell'oggetto. Per ulteriori informazioni sui checksum, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Obiettivo

In questo tutorial, imparerai come caricare un oggetto su Amazon S3 utilizzando un caricamento in più parti e un SHA-256 checksum aggiuntivo tramite l'interfaccia a riga di comando (CLI). AWS AWS

Imparerai anche come verificare l'integrità dei dati dell'oggetto calcolando l'hash MD5 e il checksum dell'oggetto caricato. SHA-256

Argomenti

- [Prerequisiti](#)
- [Fase 1: creazione di un file di grandi dimensioni](#)
- [Fase 2: suddivisione del file in più file](#)
- [Fase 3: creazione del caricamento multiparte con checksum aggiuntivo](#)
- [Fase 4: caricamento delle parti del caricamento multiparte](#)
- [Fase 5: elenco di tutte le parti del caricamento multiparte](#)
- [Fase 6: completamento del caricamento multiparte](#)
- [Fase 7: conferma del fatto che l'oggetto è stato caricato nel proprio bucket](#)
- [Fase 8: verifica dell'integrità dell'oggetto con un checksum MD5](#)
- [Fase 9: verifica dell'integrità dell'oggetto con un checksum aggiuntivo](#)
- [Fase 10: eliminare le risorse](#)

Prerequisiti

- Prima di iniziare questa esercitazione, assicurati di avere accesso a un bucket Amazon S3 su cui effettuare l'upload. Per ulteriori informazioni, consulta [Creazione di un bucket per uso generico](#).
- È necessario che la AWS CLI sia installata e configurata. Se non hai installato la CLI AWS , consulta [Installazione o aggiornamento alla versione più recente di AWS CLI](#) nella Guida all'utente AWS Command Line Interface .
- In alternativa, è possibile eseguire i comandi AWS CLI dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da Console di gestione AWS. Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Fase 1: creazione di un file di grandi dimensioni

Se hai già un file pronto per il caricamento, puoi utilizzarlo per questa esercitazione. In caso contrario, crea un file di 15 MB utilizzando i seguenti passaggi. Per i limiti relativi ai caricamenti multiparte, consulta [Limiti del caricamenti in più parti di Amazon S3](#).

Creazione un file di grandi dimensioni

Per creare il file, utilizza uno dei seguenti comandi, a seconda del sistema operativo in uso.

Linux o macOS

Per creare un file da 15 MB, apri il terminale locale ed esegui il seguente comando:

```
dd if=/dev/urandom of=census-data.bin bs=1M count=15
```

Questo comando crea un file chiamato `census-data.bin` pieno di byte casuali, con una dimensione di 15 MB.

Windows

Per creare un file da 15 MB, apri il terminale locale ed esegui il seguente comando:

```
fsutil file createnew census-data.bin 15728640
```

Questo comando crea un file chiamato `census-data.bin` con una dimensione di 15 MB di dati arbitrari (15728640 byte).

Fase 2: suddivisione del file in più file

Per eseguire il caricamento multiparte, è necessario dividere il file di grandi dimensioni in parti più piccole. È quindi possibile caricare le parti più piccole utilizzando il processo di caricamento multiparte. Questo passaggio mostra come suddividere il file di grandi dimensioni creato nella [Fase 1](#) in parti più piccole. L'esempio seguente utilizza un file di 15 MB denominato `census-data.bin`.

Suddivisione di un file di grandi dimensioni in parti

Linux o macOS

Per dividere il file di grandi dimensioni in parti da 5 MB, utilizza il comando `split`. Apri il terminale ed esegui il seguente comando:

```
split -b 5M -d census-data.bin census-part
```

Questo comando divide `census-data.bin` in parti da 5 MB denominate `census-part**`, dove `**` è un suffisso numerico che parte da `00`.

Windows

Per dividere un file di grandi dimensioni, usa PowerShell. Apri [Powershell](#) ed esegui il seguente script:

```
$inputFile = "census-data.bin"
$outputFilePrefix = "census-part"
$chunkSize = 5MB

$fs = [System.IO.File]::OpenRead($inputFile)
$buffer = New-Object byte[] $chunkSize
$fileNumber = 0

while ($fs.Position -lt $fs.Length) {
    $bytesRead = $fs.Read($buffer, 0, $chunkSize)
    $outputFile = "{0}{1:D2}" -f $outputFilePrefix, $fileNumber
    $fileStream = [System.IO.File]::Create($outputFile)
    $fileStream.Write($buffer, 0, $bytesRead)
    $fileStream.Close()
    $fileNumber++
}

$fs.Close()
```

Questo PowerShell script legge il file di grandi dimensioni in blocchi di 5 MB e scrive ogni blocco in un nuovo file con un suffisso numerico.

Dopo aver eseguito il comando appropriato, si dovrebbero vedere le parti nella directory in cui è stato eseguito il comando. Ogni parte avrà un suffisso corrispondente al suo numero di parte, ad esempio:

```
census-part00 census-part01 census-part02
```

Fase 3: creazione del caricamento multiparte con checksum aggiuntivo

Per iniziare il processo di caricamento multiparte, è necessario creare la richiesta di caricamento multiparte. Questa fase prevede l'avvio del caricamento multiparte e la specifica di un checksum aggiuntivo per l'integrità dei dati. L'esempio seguente utilizza il checksum SHA-256. Se si desidera fornire metadati che descrivono l'oggetto da caricare, è necessario fornirli nella richiesta di avvio del caricamento multiparte.

 Note

In questo passaggio e nei passaggi successivi, questo tutorial utilizza l'algoritmo SHA-256 aggiuntivo. Facoltativamente, potresti utilizzare un altro checksum aggiuntivo per questi passaggi, come CRC32, CRC32C o. SHA-1. Se si utilizza un algoritmo diverso, è necessario utilizzarlo per tutte le fasi dell'esercitazione.

Per avviare il caricamento multipart

Nel terminale, utilizza il seguente comando `create-multipart-upload` per avviare un caricamento multipart per il bucket. Sostituisci `amzn-s3-demo-bucket1` con il nome effettivo del bucket. Inoltre, sostituisci `census_data_file` con il nome del file scelto. Questo nome di file diventa la chiave dell'oggetto al termine del caricamento.

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket1 --key  
'census_data_file' --checksum-algorithm sha256
```

Se la richiesta ha successo, si vedrà un output JSON come il seguente:

```
{  
  "ServerSideEncryption": "AES256",  
  "ChecksumAlgorithm": "SHA256",  
  "Bucket": "amzn-s3-demo-bucket1",  
  "Key": "census_data_file",  
  "UploadId":  
    "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sN0KPeMhpKQRrbT9k0ePmgo0TCj9K83T4e2Gb5hQvNoNpCKqyb8m3"  
}
```

 Note

Quando invii una richiesta di avvio di un caricamento in più parti, Amazon S3 restituisce una risposta con un ID di caricamento, che rappresenta un identificativo univoco per il caricamento in più parti. È necessario includere questo ID di caricamento ogni volta che si caricano o si elencano le parti oppure ogni volta che si completa o si interrompe un caricamento. I valori `UploadId`, `Key` e `Bucket` dovranno essere utilizzati per le fasi successive per assicurarsi di salvarli.

Inoltre, se si utilizza il caricamento multiparte con checksum aggiuntivi, i numeri di parte devono essere consecutivi. Se si utilizzano numeri di parte non consecutivi, la richiesta `complete-multipart-upload` può determinare un `HTTP 500 Internal Server Error`.

Fase 4: caricamento delle parti del caricamento multiparte

In questa fase, si caricheranno le parti del caricamento multiparte sul bucket S3. Usa il comando `upload-part` per caricare ogni parte singolarmente. Questo processo richiede di specificare l'ID di caricamento, il numero di parte e il file da caricare per ogni parte.

Per caricare le parti

1. Quando si carica una parte, è necessario specificare un numero di parte oltre all'ID di caricamento usando l'argomento `--part-number`. È possibile scegliere qualsiasi numero compreso tra 1 e 10.000. Il numero della parte identifica in modo univoco una parte e la relativa posizione nell'oggetto che si sta caricando. Il numero di parte scelto non deve necessariamente essere in sequenza (ad esempio, può essere 1, 2 e 3). Se si carica una nuova parte che utilizza lo stesso numero di una parte caricata in precedenza, quest'ultima viene sovrascritta.
2. Usa il comando `upload-part` per caricare ogni parte del caricamento multiparte. `--upload-id` è lo stesso che si trovava nell'output creato dal comando `create-multipart-upload` nella [Fase 3](#). Per caricare la prima parte dei dati, utilizza il seguente comando:

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key  
'census_data_file' --part-number 1 --body census-part00 --upload-id  
"cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sN0KPeMhpKQRrbT9k0ePmgo0TCj9K83T4e2Gb5hQvNoNpCKqy  
--checksum-algorithm SHA256
```

Al termine di ogni comando `upload-part`, si dovrebbe vedere un output come quello dell'esempio seguente:

```
{  
  "ServerSideEncryption": "AES256",  
  "ETag": "\"e611693805e812ef37f96c9937605e69\"",  
  "ChecksumSHA256": "QL18R4i4+SaJlrl8Zlcutc5TbZtw2NwB81TXkd3GH0="  
}
```

3. Per le parti successive, incrementa il numero di parte di conseguenza:

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --  
part-number <part-number> --body <file-path> --upload-id "<your-upload-id>" --  
checksum-algorithm SHA256
```

Ad esempio, utilizza il seguente comando per caricare la seconda parte:

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key  
'census_data_file' --part-number 2 --body census-part01 --upload-id  
"cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sN0KPeMhpKQRrbT9k0ePmgo0TCj9K83T4e2Gb5hQvNoNpCKqy  
--checksum-algorithm SHA256
```

Amazon S3 restituisce un tag entità (ETag) e checksum aggiuntivi per ogni parte caricata come intestazione della risposta.

4. Continua a usare il comando `upload-part` finché non si sono caricate tutte le parti dell'oggetto.

Fase 5: elenco di tutte le parti del caricamento multiparte

Per completare il caricamento multiparte, è necessario un elenco di tutte le parti che sono state caricate per quel determinato caricamento multiparte. L'output del comando `list-parts` fornisce informazioni quali il nome del bucket, la chiave, l'ID di caricamento, il numero di parte, l'ETag, i checksum aggiuntivi e altro ancora. È utile salvare questo risultato in un file, in modo da poterlo utilizzare per il passaggio successivo, quando si completa il processo di caricamento multiparte. È possibile creare un file di output JSON chiamato `parts.json` utilizzando il metodo seguente.

Per creare un file che elenchi tutte le parti

1. Per generare un file JSON con i dettagli di tutte le parti caricate, utilizza il seguente comando `list-parts`. Sostituisci **amzn-s3-demo-bucket1** con il nome effettivo del bucket e **<your-upload-id>** con l'ID di caricamento ricevuto nella [Fase 3](#). Per ulteriori informazioni sul comando `list-parts` consulta [list-parts](#) nella Guida all'utente AWS Command Line Interface .

```
aws s3api list-parts --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --  
upload-id <your-upload-id> --query '{Parts: Parts[*].{PartNumber: PartNumber, ETag:  
ETag, ChecksumSHA256: ChecksumSHA256}}' --output json > parts.json
```

Viene generato un nuovo file chiamato `parts.json`. Il file contiene le informazioni formattate in JSON di tutte le parti caricate. Il file `parts.json` contiene informazioni essenziali per ogni parte del caricamento multiparte, come i numeri di parte e i valori ETag corrispondenti, necessari per completare il processo di caricamento multiparte.

2. Apri `parts.json` utilizzando un qualsiasi editor di testo o tramite il terminale. Ecco l'esempio di output:

```
{
  "Parts": [
    {
      "PartNumber": 1,
      "ETag": "\"3c3097f89e2a2fece47ac54b243c9d97\"",
      "ChecksumSHA256": "fTPVHfyNHdv5VkR4S3EewdyioXECv7JBxN+d4FXYYTw="
    },
    {
      "PartNumber": 2,
      "ETag": "\"03c71cc160261b20ab74f6d2c476b450\"",
      "ChecksumSHA256": "VDWTa8enj0vULBA03W2a6C+5/7ZnNjrnLApa1QVc3FE="
    },
    {
      "PartNumber": 3,
      "ETag": "\"81ae0937404429a97967dffa7eb4affb\"",
      "ChecksumSHA256": "cVVkXehUlzcwrBrXgPIM+EKQXPUvWist8m1UTCs4bg8="
    }
  ]
}
```

Fase 6: completamento del caricamento multiparte

Dopo aver caricato tutte le parti del caricamento multiparte e averle elencate, il passaggio finale consiste nel completare il caricamento multiparte. Questo passaggio unisce tutte le parti caricate in un unico oggetto nel bucket S3.

Note

È possibile calcolare il checksum dell'oggetto prima di chiamare `complete-multipart-upload`, includendo `--checksum-sha256` nella richiesta. Se i checksum non

corrispondono, Amazon S3 rifiuta la richiesta. Per ulteriori informazioni, consulta [complete-multipart-upload](#) nella Guida per l'utente di AWS Command Line Interface .

Per completare il caricamento multiparte

Per finalizzare il caricamento multiparte, utilizza il comando `complete-multipart-upload`. Questo comando richiede il file `parts.json` creato nella [Fase 5](#), il nome del bucket e l'ID di caricamento. Sostituisci **<amzn-s3-demo-bucket1>** con il nome del bucket e **<your-upload-id>** con l'ID di caricamento di `parts.json`.

```
aws s3api complete-multipart-upload --multipart-upload file://parts.json --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --upload-id <your-upload-id>
```

Ecco l'esempio di output:

```
{
  "ServerSideEncryption": "AES256",
  "Location": "https://amzn-s3-demo-bucket1.s3.us-east-2.amazonaws.com/census_data_file",
  "Bucket": "amzn-s3-demo-bucket1",
  "Key": "census_data_file",
  "ETag": "\"f453c6dcca969c457efdf9b1361e291-3\"",
  "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3"
}
```

Note

Non eliminare ancora i file delle singole parti. È necessario disporre delle singole parti, in modo da poter eseguire checksum su di esse per verificare l'integrità dell'oggetto unito.

Fase 7: conferma del fatto che l'oggetto è stato caricato nel proprio bucket

Dopo aver completato il caricamento multiparte, è possibile verificare che l'oggetto sia stato caricato correttamente sul bucket S3. Per elencare gli oggetti nel bucket e confermare la presenza del file appena caricato, utilizza il comando `list-objects-v2`

Per elencare l'oggetto caricato

Per elencare gli oggetti presenti, utilizza il comando `list-objects-v2` del bucket. Sostituisci ***amzn-s3-demo-bucket1*** con il nome effettivo del bucket:

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket1
```

Questo comando restituisce un elenco di oggetti presenti nel bucket. Cerca il file caricato (ad esempio, `census_data_file`) nell'elenco degli oggetti.

Per ulteriori informazioni, consulta la sezione [Esempi](#) del comando `list-objects-v2` nella Guida all'utente AWS Command Line Interface .

Fase 8: verifica dell'integrità dell'oggetto con un checksum MD5

Quando si carica un oggetto, è possibile specificare un algoritmo di checksum da utilizzare per Amazon S3. Per impostazione predefinita, Amazon S3 memorizza il digest MD5 dei byte come ETag dell'oggetto. Per i caricamenti multiparte, l'ETag non è il checksum dell'intero oggetto, ma piuttosto un insieme di checksum per ogni singola parte.

Per verificare l'integrità dell'oggetto utilizzando un checksum MD5

1. Per recuperare l'ETag dell'oggetto caricato, esegui una richiesta `head-object`:

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file
```

Ecco l'esempio di output:

```
{
  "AcceptRanges": "bytes",
  "LastModified": "2024-07-26T19:04:13+00:00",
  "ContentLength": 16106127360,
  "ETag": "\"f453c6dcca969c457efdf9b1361e291-3\"",
  "ContentType": "binary/octet-stream",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}
```


Questo ETag ha "-3" aggiunto alla fine. Questo indica che l'oggetto è stato caricato in tre parti utilizzando il caricamento multiparte.

2. Quindi, calcola la somma di controllo MD5 di ogni parte utilizzando il comando `md5sum`. Assicurati di fornire il percorso corretto dei file delle parti:

```
md5sum census-part*
```

Ecco l'esempio di output:

```
e611693805e812ef37f96c9937605e69 census-part00
63d2d5da159178785bfd6b6a5c635854 census-part01
95b87c7db852451bb38b3b44a4e6d310 census-part02
```

3. Per questo passaggio, combina manualmente gli hash MD5 in un'unica stringa. Quindi, esegui il seguente comando per convertire la stringa in codice binario e calcolare il checksum MD5 del valore binario:

```
echo
  "e611693805e812ef37f96c9937605e6963d2d5da159178785bfd6b6a5c63585495b87c7db852451bb38b3b44a4e6d310"
  | xxd -r -p | md5sum
```

Ecco l'esempio di output:

```
f453c6dcccc969c457efdf9b1361e291 -
```

Questo valore di hash dovrebbe corrispondere al valore di hash del valore ETag originale nella [Fase 1](#), che convalida l'integrità dell'oggetto `census_data_file`.

Quando chiedi ad Amazon S3 di utilizzare checksum aggiuntivi, Amazon S3 calcola il valore del checksum per ogni parte e archivia i valori. Se si desidera recuperare i valori di checksum per le singole parti dei caricamenti multiparte mentre sono ancora in corso, si può usare `list-parts`.

Per ulteriori informazioni sul funzionamento dei checksum con gli oggetti di caricamento multiparte, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Fase 9: verifica dell'integrità dell'oggetto con un checksum aggiuntivo

In questo passaggio, questo tutorial utilizza SHA-256 come checksum aggiuntivo per convalidare l'integrità dell'oggetto. Se è stato utilizzato un checksum aggiuntivo diverso, utilizza invece quel valore di checksum.

Per verificare l'integrità dell'oggetto con SHA256

1. Esegui il seguente comando nel terminale, includendo l'argomento `--checksum-mode enabled`, per visualizzare il valore ChecksumSHA256 dell'oggetto:

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file --checksum-mode enabled
```

Ecco l'esempio di output:

```
{
  "AcceptRanges": "bytes",
  "LastModified": "2024-07-26T19:04:13+00:00",
  "ContentLength": 16106127360,
  "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3",
  "ETag": "\"f453c6dcca969c457efdf9b1361e291-3\"",
  "ContentType": "binary/octet-stream",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}
```

2. Usa i seguenti comandi per decodificare i valori ChecksumSHA256 delle singole parti in base64 e salvarli in un file binario chiamato `outfile`. Questi valori si trovano nel file `parts.json`. Sostituisci le stringhe base64 di esempio con i valori reali di ChecksumSHA256.

```
echo "QL18R4i4+SaJlr18ZICutc5TbZtw2NwB8lTXkd3GH0=" | base64 --decode >> outfile
echo "xCdgs1K5Bm4jWETYw/CmGYr+m602DcGfpckx5NVokvE=" | base64 --decode >> outfile
echo "f5wsf5a5bB+yXuwzqG1Bst91uYneqGD3CCidpb54mAo=" | base64 --decode >> outfile
```

3. Esegui il seguente comando per calcolare il checksum SHA256 di `outfile`:

```
sha256sum outfile
```

Ecco l'esempio di output:

```
688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9 outfile
```

Nella fase successiva, si prende il valore hash e lo si converte in un valore binario. Questo valore binario deve corrispondere al valore ChecksumSHA256 della [Fase 1](#).

4. Converti il checksum SHA256 della [Fase 3](#) in binario, quindi codificala in base64 per verificare che corrisponda al valore di ChecksumSHA256 della [Fase 1](#):

```
echo "688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9" | xxd -r -p  
| base64
```

Ecco l'esempio di output:

```
aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=
```

Questo risultato dovrebbe confermare che l'output base64 corrisponde al valore ChecksumSHA256 dall'output del comando `head-object`. Se l'output corrisponde al valore del checksum, l'oggetto è valido.

Important

- Quando si indica ad Amazon S3 di utilizzare checksum aggiuntivi, Amazon S3 calcola il valore di checksum per ogni parte e memorizza i valori.
- Se si desidera recuperare i valori di checksum per le singole parti dei caricamenti multiparte mentre sono ancora in corso, si può usare il comando `list-parts`.

Fase 10: eliminare le risorse

Se desideri ripulire i file creati in questa esercitazione, utilizza il metodo seguente. Per istruzioni sull'eliminazione dei file caricati sul bucket S3, consulta [Eliminazione di oggetti Amazon S3](#).

Elimina i file locali creati nella [Fase 1](#):

Per rimuovere i file creati per il caricamento multiparte, esegui il seguente comando dalla tua directory di lavoro:

```
rm census-data.bin census-part* outfile parts.json
```

Limiti del caricamenti in più parti di Amazon S3

Il caricamento in più parti consente di caricare un singolo oggetto come un insieme di parti. Ciascuna parte è una parte contigua dei dati dell'oggetto. Una volta caricate tutte le parti dell'oggetto, Amazon S3 le assembla e crea l'oggetto. In generale, quando la dimensione dell'oggetto raggiunge i 100 MB, si consiglia di valutare la possibilità di eseguire caricamenti in più parti anziché caricare l'oggetto in una singola operazione. Per ulteriori informazioni sui caricamenti in più parti, consulta la sezione [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

La tabella riportata di seguito fornisce le specifiche di base di un caricamento in più parti. Ciò include la dimensione massima dell'oggetto, il numero massimo di parti, la dimensione massima delle parti e altro. Non vi è alcun limite minimo di dimensione per l'ultima parte del caricamento in più parti.

Elemento	Specifica
Dimensione massima oggetto	48,8 TiB
Numero massimo di parti per caricamento	10.000
Numeri delle parti	Da 1 a 10.000 (inclusi)
Dimensione parte	Da 5 MiB a 5 GiB. Non vi è alcun limite minimo di dimensione per l'ultima parte del caricamento in più parti.
Numero massimo di parti restituite per una richiesta di elenco delle parti	1000
Numero massimo di caricamenti in più parti restituiti per una richiesta di elenco dei caricamenti in più parti	1000

Aggiunta di precondizioni alle operazioni S3 con richieste condizionali

È possibile utilizzare le richieste condizionali per aggiungere precondizioni alle operazioni S3. Per utilizzare le richieste condizionali, si aggiunge un'intestazione supplementare all'operazione API di Amazon S3. Questa intestazione specifica una condizione che, se non viene soddisfatta, comporta il fallimento dell'operazione S3.

Le letture condizionali sono supportate per le richieste GET, HEAD e COPY. È possibile aggiungere precondizioni per restituire o copiare un oggetto in base al suo tag entità (ETag) o alla data dell'ultima modifica. Questo può limitare un'operazione S3 agli oggetti aggiornati a partire da una data specifica. È anche possibile limitare un'operazione S3 a un ETag specifico. In questo modo si potrebbe garantire la restituzione o la copia solo di una versione specifica dell'oggetto. Per ulteriori informazioni sui metadata degli oggetti, consulta [Utilizzo dei metadata degli oggetti](#).

Le scritture condizionali possono garantire l'assenza di oggetti esistenti con lo stesso nome di chiave nel bucket durante operazioni PUT. Questo impedisce la sovrascrittura di oggetti esistenti con nomi di chiavi identici. Allo stesso modo, si possono usare le scritture condizionali per verificare se l'ETag di un oggetto è invariato prima di aggiornare l'oggetto. Ciò impedisce di sovrascrivere involontariamente un oggetto senza conoscere lo stato del suo contenuto. È possibile utilizzare scritture condizionali per [PutObject](#), [CompleteMultipartUpload](#), o richieste. [CopyObject](#). Per ulteriori informazioni sui nomi delle chiavi, consultare [Denominazione di oggetti Amazon S3](#).

Le eliminazioni condizionali valutano se l'oggetto esiste o è immutato prima di eliminarlo. È possibile eseguire eliminazioni condizionali utilizzando le API `DeleteObject` o `DeleteObjects` nei bucket per uso generico e di directory. Per ulteriori informazioni sulle eliminazioni condizionali, consulta [Come eseguire le eliminazioni condizionali](#). Non è previsto alcun costo aggiuntivo per le letture e le scritture condizionali, né per le eliminazioni condizionali. Vengono addebitate solo le tariffe esistenti per le richieste applicabili, comprese quelle non andate a buon fine. Per informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

Argomenti

- [Come recuperare o copiare gli oggetti in base ai metadata con letture condizionali](#)
- [Come prevenire la sovrascrittura degli oggetti con le scritture condizionali](#)
- [Come eseguire le eliminazioni condizionali](#)

Come recuperare o copiare gli oggetti in base ai metadati con letture condizionali

Con la lettura condizionale, è possibile aggiungere un'intestazione supplementare alla richiesta di lettura per aggiungere precondizioni all'operazione S3. Se queste precondizioni non sono soddisfatte, la richiesta di lettura fallisce.

È possibile usare la lettura condizionale sulle richieste GET, HEAD o COPY per restituire un oggetto solo in base ai suoi metadati.

Quando si carica un oggetto, Amazon S3 crea metadati controllati dal sistema che possono essere modificati solo da S3. I tag di entità (ETags) Last-Modified sono esempi di metadati controllati dal sistema. L'ETag di un oggetto è una stringa che rappresenta una versione specifica di un oggetto. Last-Modified la data è un metadato che rappresenta la data di creazione di un oggetto o la data dell'ultima modifica, a seconda di quale sia l'ultima.

Con le letture condizionali, puoi restituire un oggetto in base all'ETag o alla data dell'oggetto. Last-Modified È possibile specificare un valore ETag con la richiesta e restituire l'oggetto solo se il valore ETag corrisponde. In questo modo si potrebbe garantire la restituzione o la copia di una specifica versione di un oggetto. È possibile specificare un Last-Modified valore nella richiesta di lettura e restituire un oggetto solo se tale oggetto è stato modificato dopo una data fornita.

API supportate

Le seguenti API S3 supportano l'uso della lettura condizionale:

- [GetObject](#)
- [HeadObject](#)
- [CopyObject](#)

È possibile usare le seguenti intestazioni per restituire un oggetto in base al suo tag entità (ETag) o alla data di ultima modifica. Per ulteriori informazioni sui metadati degli oggetti come ETags e, vedete. Last-Modified [the section called “System-defined metadati degli oggetti”](#)

[GetObject](#)

- **If-Match** - Restituisce l'oggetto solo se il suo ETag corrisponde a quello fornito.

- **If-Modified-Since** - Restituisce l'oggetto solo se è stato modificato dal momento specificato.
- **If-None-Match** - Restituisce l'oggetto solo se il suo ETag non corrisponde a quello fornito.
- **If-Unmodified-Since** - Restituisce l'oggetto solo se non è stato modificato dal momento specificato.

Per ulteriori informazioni su queste intestazioni, sugli errori restituiti e sull'ordine con cui S3 gestisce più intestazioni condizionali in una singola richiesta, consulta [GetObject](#) nel Riferimento API di Amazon Simple Storage Service.

[HeadObject](#)

- **If-Match** - Restituisce l'oggetto solo se il suo ETag corrisponde a quello fornito.
- **If-Modified-Since** - Restituisce l'oggetto solo se è stato modificato dal momento specificato.
- **If-None-Match** - Restituisce l'oggetto solo se il suo ETag non corrisponde a quello fornito.
- **If-Unmodified-Since** - Restituisce l'oggetto solo se non è stato modificato dal momento specificato.

Per ulteriori informazioni su queste intestazioni, sugli errori restituiti e sull'ordine con cui S3 gestisce più intestazioni condizionali in una singola richiesta, consulta [HeadObject](#) nel Riferimento API di Amazon Simple Storage Service.

[CopyObject](#)

- **x-amz-copy-source-if-match** - Copia l'oggetto di origine solo se il suo ETag corrisponde a quello fornito.
- **x-amz-copy-source-if-modified-since** - Copia l'oggetto di origine solo se è stato modificato dal momento specificato.
- **x-amz-copy-source-if-none-match** - Copia l'oggetto di origine solo se il suo ETag non corrisponde a quello fornito.
- **x-amz-copy-source-if-unmodified-since** - Copia l'oggetto di origine solo se non è stato modificato dal momento specificato.
- **If-Match**— Copia l'oggetto solo se il relativo ETag corrisponde a quello fornito. **If-Matchsi** aspetta il valore ETag come stringa.

- **If-None-Match**— Copia l'oggetto solo se il relativo ETag non corrisponde a quello fornito. **If-None-Match** si aspetta il carattere '*' (asterisco).

Per ulteriori informazioni su queste intestazioni, sugli errori restituiti e sull'ordine con cui S3 gestisce più intestazioni condizionali in una singola richiesta, consulta [CopyObject](#) nel Riferimento API di Amazon Simple Storage Service.

Per informazioni sull'utilizzo delle intestazioni condizionali per evitare la sovrascrittura durante le operazioni di scrittura, vedere. [Come prevenire la sovrascrittura degli oggetti con le scritture condizionali](#)

Come prevenire la sovrascrittura degli oggetti con le scritture condizionali

Utilizzando le scritture condizionali, è possibile aggiungere un'ulteriore intestazione alle richieste **WRITE** per specificare le precondizioni per le operazioni su Amazon S3. Per scrivere oggetti in modo condizionato, aggiungi l'intestazione **HTTP If-None-Match** o **If-Match**.

L'intestazione **If-None-Match** impedisce la sovrascrittura dei dati esistenti, verificando che non vi sia già un oggetto con lo stesso nome di chiave nel bucket.

In alternativa, si può aggiungere l'intestazione **If-Match** per verificare il tag entità (ETag) di un oggetto prima di scrivere un oggetto. Con questa intestazione, Amazon S3 confronta il valore ETag fornito con il valore ETag dell'oggetto in S3. Se i valori ETag non corrispondono, l'operazione non riesce.

I proprietari dei bucket possono usare le policy di bucket per imporre la scrittura condizionale degli oggetti caricati. Per ulteriori informazioni, consulta [the section called "Applicazione delle scritture condizionali"](#).

Note

Per utilizzare le scritture condizionali, è necessario utilizzare la versione 4 di AWS Signature per firmare la richiesta.

Argomenti

- [Come impedire la sovrascrittura degli oggetti in base ai nomi delle chiavi](#)
- [Come impedire la sovrascrittura se l'oggetto è stato modificato](#)

- [Comportamento di scrittura condizionale](#)
- [Scenari di scrittura condizionati](#)
- [Applicazione delle scritture condizionali sui bucket Amazon S3](#)

Come impedire la sovrascrittura degli oggetti in base ai nomi delle chiavi

È possibile utilizzare l'intestazione `If-None-Match` condizionale HTTP per verificare se un oggetto esiste già nel bucket specificato in base al nome della chiave prima di crearlo o copiarlo nel bucket di destinazione.

Le scritture condizionali con l'intestazione HTTP `If-None-Match` controllano l'esistenza di un oggetto durante l'operazione `WRITE`. Se nel bucket viene trovato un nome di chiave identico, l'operazione fallisce. Senza l'`If-None-Match` intestazione HTTP, se carichi o copi un oggetto con un nome di chiave identico in un bucket senza versione o con versione sospesa, l'oggetto viene sovrascritto. Per ulteriori informazioni sull'uso dei nomi delle chiavi, consulta [the section called "Denominazione di oggetti"](#).

Note

L'`If-None-Match` intestazione HTTP si applica solo alla versione corrente di un oggetto in un bucket di versioni.

Per eseguire scritture condizionali con l'intestazione HTTP `If-None-Match` è necessario disporre dell'autorizzazione `s3:PutObject`. Ciò consente al chiamante di verificare la presenza di oggetti nel bucket. L'intestazione `If-None-Match` prevede il valore `*` (asterisco).

È possibile utilizzare l'intestazione `If-None-Match` con le seguenti API:

- [PutObject](#)
- [CompleteMultipartUpload](#)
- [CopyObject](#)

Put condizionale utilizzando il AWS CLI

Il seguente comando di esempio `put-object` tenta di eseguire una scrittura condizionale per un oggetto con il nome della chiave `dir-1/my_images.tar.bz2`.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body  
my_images.tar.bz2 --if-none-match "*"
```

Per ulteriori informazioni, consulta [put-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedi [Che cos'è il AWS Command Line Interface?](#) nella Guida AWS Command Line Interface per l'utente.

Copia condizionale utilizzando il AWS CLI

Il comando di `copy-object` esempio seguente tenta di copiare un oggetto in un bucket di destinazione con una scrittura condizionale per un oggetto con il nome della chiave. `dir-1/my_images.tar.bz2`

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket/key --key dir-1/  
my_images.tar.bz2 --bucket amzn-s3-demo-bucket2 --if-none-match "*"
```

Per ulteriori informazioni, consulta [copy-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedi [What is the? AWS Command Line Interface](#) nella Guida AWS Command Line Interface per l'utente.

Caricamento condizionale in più parti utilizzando il AWS CLI

Il comando di `complete-multipart-upload` esempio seguente tenta di completare un caricamento in più parti con una scrittura condizionale per un oggetto con il nome della chiave. `dir-1/my_images.tar.bz2` In questo esempio, il prefisso `file://` viene utilizzato per caricare la struttura JSON da un file nella cartella locale denominata con l'elenco di tutte le parti `mpustruct` che sono state caricate per questo specifico caricamento in più parti.

```
aws s3api complete-multipart-upload --multipart-upload file://mpustruct --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --upload-id upload-id --if-none-match "*"
```

Per ulteriori informazioni, consulta [complete-multipart-upload](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedi [What is the? AWS Command Line Interface](#) nella Guida AWS Command Line Interface per l'utente.

Come impedire la sovrascrittura se l'oggetto è stato modificato

L'ETag di un oggetto è una stringa univoca per l'oggetto e riflette una modifica al contenuto dell'oggetto. È possibile utilizzare l'intestazione If-Match per confrontare il valore ETag di un oggetto in un bucket Amazon S3 con quello fornito dall'utente durante l'operazione WRITE. Se i valori ETag non corrispondono, l'operazione non riesce. Per ulteriori informazioni sugli ETag, consulta [the section called "Utilizzo Content-MD5 e ETag per verificare gli oggetti caricati"](#).

Per eseguire scritture condizionali con l'intestazione HTTP If-Match è necessario disporre delle autorizzazioni `s3:PutObject` e `s3:GetObject`. Ciò consente al chiamante di verificare l'ETag e lo stato degli oggetti nel bucket. L'intestazione If-Match prevede il valore ETag come stringa.

È possibile utilizzare l'intestazione If-Match con le seguenti API:

- [PutObject](#)
- [CompleteMultipartUpload](#)
- [CopyObject](#)

Put condizionale utilizzando il AWS CLI

Il seguente comando di esempio `put-object` tenta di eseguire una scrittura condizionale per un oggetto con il valore ETag `6805f2cfc46c0f04559748bb039d69ae` fornito.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body  
my_images.tar.bz2 --if-match "6805f2cfc46c0f04559748bb039d69ae"
```

Per ulteriori informazioni, consulta [put-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedi [Che cos'è il AWS Command Line Interface?](#) nella Guida AWS Command Line Interface per l'utente.

Copia condizionale utilizzando il AWS CLI

Il seguente comando di esempio `copy-object` tenta di eseguire una scrittura condizionale per un oggetto con il valore ETag `6805f2cfc46c0f04559748bb039d69ae` fornito.

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket/key --key  
dir-1/my_images.tar.bz2 --bucket amzn-s3-demo-bucket2 --if-match  
"6805f2cfc46c0f04559748bb039d69ae"
```

Per ulteriori informazioni, consulta [copy-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedere [Che cos'è il AWS Command Line Interface?](#) nella Guida AWS Command Line Interface per l'utente.

Caricamento condizionale in più parti utilizzando il AWS CLI

Il seguente comando di `complete-multipart-upload` esempio tenta di completare un caricamento in più parti con una scrittura condizionale utilizzando il valore ETag fornito. `6805f2cfc46c0f04559748bb039d69ae` In questo esempio, il prefisso `file://` viene utilizzato per caricare la struttura JSON da un file nella cartella locale denominata con l'elenco di tutte le parti `mpustruct` che sono state caricate per questo specifico caricamento in più parti.

```
aws s3api complete-multipart-upload --multipart-upload file://mpustruct --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --upload-id upload-id --if-match  
"6805f2cfc46c0f04559748bb039d69ae"
```

Per ulteriori informazioni, consulta [complete-multipart-upload](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedi [What is the? AWS Command Line Interface](#) nella Guida AWS Command Line Interface per l'utente.

Comportamento di scrittura condizionale

Scritture o copie condizionali con **If-None-Match** intestazione

Le scritture condizionali con l'intestazione `If-None-Match` vengono valutate rispetto agli oggetti esistenti in un bucket. Se non c'è nessun oggetto esistente con lo stesso nome di chiave nel bucket, l'operazione di scrittura ha successo, con una risposta `200 OK`. Se c'è un oggetto esistente, l'operazione di scrittura fallisce e la risposta è `412 Precondition Failed`.

Per i bucket con controllo delle versioni abilitato, se non esiste una versione corrente dell'oggetto con lo stesso nome o se la versione corrente dell'oggetto è un marcatore di cancellazione,

l'operazione di scrittura va a buon fine. Altrimenti, si ottiene un'operazione di scrittura fallita con una risposta `412 Precondition Failed`.

Se si verificano più scritture o copie condizionali per lo stesso nome di oggetto, la prima operazione di scrittura completata ha esito positivo. Amazon S3 quindi non riesce a eseguire le scritture successive con una risposta `412 Precondition Failed`.

È inoltre possibile ricevere una risposta `409 Conflict` nel caso di richieste concorrenti, se una richiesta di cancellazione di un oggetto ha successo prima che un'operazione di scrittura condizionale su quell'oggetto sia completata. Quando si usano le scritture condizionali con `PutObject`, i caricamenti possono essere ritentati dopo aver ricevuto un errore `409 Conflict`. Quando si usa `CompleteMultipartUpload`, l'intero caricamento multipart deve essere riavviato con `CreateMultipartUpload` per caricare nuovamente l'oggetto dopo aver ricevuto un errore `409 Conflict`.

Scritture o copie condizionali con intestazione **If-Match**

L'intestazione `If-Match` viene valutata rispetto agli oggetti esistenti in un bucket. Se non c'è nessun oggetto esistente con lo stesso nome di chiave ed ETag corrispondente, l'operazione di scrittura ha successo, con una risposta `200 OK`. Se l'ETag non corrisponde, l'operazione di scrittura fallisce con una risposta `412 Precondition Failed`.

È anche possibile ricevere una risposta `409 Conflict` in caso di richieste simultanee.

Si riceverà una risposta `404 Not Found` se una richiesta di cancellazione concorrente di un oggetto riesce prima che un'operazione di scrittura condizionale su quell'oggetto sia completata, poiché la chiave dell'oggetto non esiste più. È necessario ricaricare l'oggetto quando si riceve una risposta `404 Not Found`.

Se non esiste una versione corrente dell'oggetto con lo stesso nome o se la versione corrente dell'oggetto è un marcatore di cancellazione, l'operazione fallisce con un errore `404 Not Found`.

Scenari di scrittura condizionati

Si considerino i seguenti scenari in cui due client eseguono operazioni sullo stesso bucket.

Scrittura condizionale durante il caricamento multipart

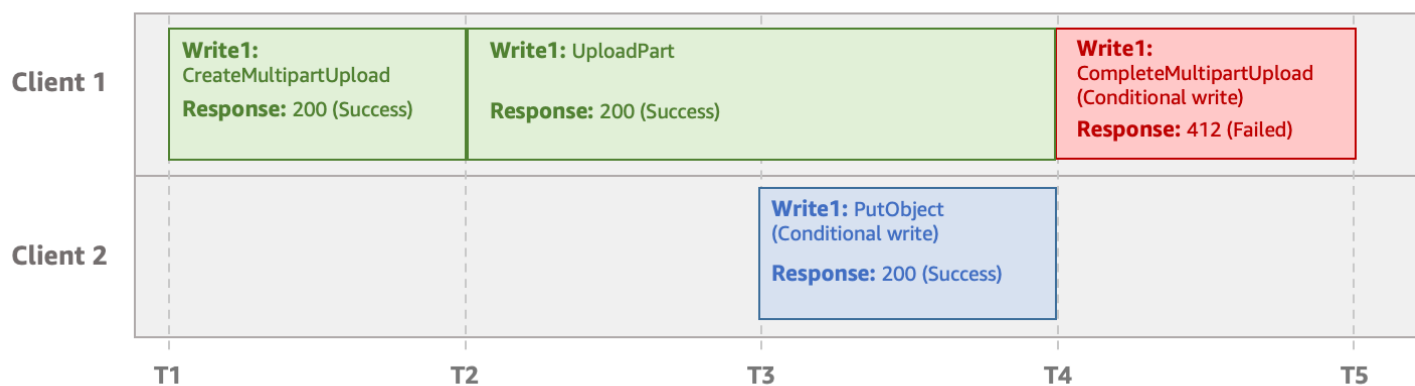
Le scritture condizionali non considerano le richieste di caricamento multipart in corso, poiché non sono ancora oggetti completamente scritti. Si consideri il seguente esempio in cui il client 1 sta

caricando un oggetto utilizzando il caricamento multipart. Durante il caricamento multipart, il client 2 è in grado di scrivere con successo lo stesso oggetto con l'operazione di scrittura condizionale. Successivamente, quando il client 1 tenta di completare il caricamento multipart utilizzando una scrittura condizionale, il caricamento non riesce.

Note

In questo caso si otterrà una risposta 412 `Precondition Failed` per entrambe le intestazioni `If-None-Match` e `If-Match`.

L'esempio seguente mostra due client che scrivono elementi con lo stesso nome di chiave. Uno con `UploadPart` per MPU e uno con `PutObject` e una scrittura condizionale. L' `CompleteMultipartUpload` operazione, che inizia dopo, non riesce.



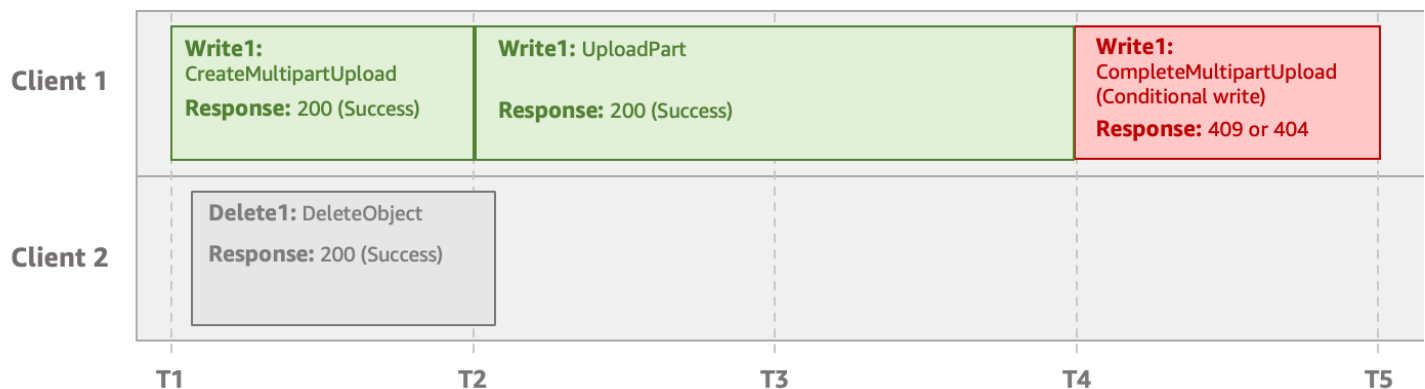
Cancellazioni simultanee durante il caricamento di più parti

Se una richiesta di cancellazione riesce prima che una richiesta di scrittura condizionale possa essere completata, Amazon S3 restituisce una risposta 409 `Conflict` o 404 `Not Found` per l'operazione di scrittura. Questo perché la richiesta di cancellazione avviata in precedenza ha la precedenza sull'operazione di scrittura condizionale. In questi casi, è necessario avviare un nuovo caricamento multipart.

Note

In questo caso si otterrà una risposta 409 `Conflict` per un'intestazione `If-None-Match` e una risposta 404 `Not Found` per un'intestazione `If-Match`.

L'esempio seguente mostra due client, uno che utilizza il caricamento in più parti e l'altro che invia una richiesta di eliminazione dopo l'avvio della MPU. La richiesta di cancellazione termina prima dell'inizio della scrittura condizionale.



Note

Per ridurre al minimo i costi di archiviazione, ti consigliamo di configurare una regola del ciclo di vita per eliminare i caricamenti in più parti incompleti dopo un numero di giorni specificato utilizzando l'operazione `AbortIncompleteMultipartUpload`. Per ulteriori informazioni sulla creazione di una regola del ciclo di vita per eliminare i caricamenti in più parti incompleti, consulta [Configurazione del ciclo di vita del bucket per l'eliminazione dei caricamenti in più parti incompleti](#).

Applicazione delle scritture condizionali sui bucket Amazon S3

Utilizzando le policy di bucket Amazon S3, è possibile imporre scritture condizionali per il caricamento di oggetti nei bucket per uso generico.

Una policy di bucket è una policy basata sulle risorse che può essere utilizzata per concedere le autorizzazioni di accesso al bucket Amazon S3 e agli oggetti in esso contenuti. Solo il proprietario del bucket può associare una policy a un bucket. Per ulteriori informazioni sulle policy di bucket, consulta [the section called "Policy di bucket"](#).

È possibile utilizzare le chiavi di condizione `s3:if-match` o `s3:if-none-match` come l'elemento opzionale `Condition` o il blocco `Condition` per specificare quando una policy è in vigore. Per i caricamenti multiparte è necessario specificare la chiave di condizione `s3:ObjectCreationOperation` per esentare le operazioni `CreateMultipartUpload`,

UploadPart e UploadPartCopy, poiché queste API non accettano intestazioni condizionali. Per ulteriori informazioni sull'uso delle condizioni nelle policy di bucket, consulta [the section called “Esempi di condizioni chiave”](#).

Note

Se si usa una policy di bucket per imporre scritture condizionali, non è possibile eseguire operazioni di copia sul bucket o sul prefisso specificato nella policy di bucket. Le richieste CopyObject senza un'intestazione HTTP If-None-Match o If-Match falliscono con un errore 403 Access Denied. Le richieste CopyObject fatte con queste intestazioni HTTP falliscono con una risposta 501 Not Implemented.

Gli esempi seguenti mostrano come utilizzare le condizioni in una policy di bucket per forzare i client a usare l'intestazione HTTP If-None-Match o If-Match.

Argomenti

- [Esempio 1: consenti solo il caricamento di oggetti utilizzando PutObject e le CompleteMultipartUpload richieste che includono l'intestazione if-none-match](#)
- [Esempio 2: consenti solo il caricamento di oggetti utilizzando PutObject e le richieste che includono l'intestazione if-match CompleteMultipartUpload](#)
- [Esempio 3: consenti solo le richieste di caricamento di oggetti che includono l'intestazione if-none-match o if-match](#)

Esempio 1: consenti solo il caricamento di oggetti utilizzando **PutObject** e le **CompleteMultipartUpload** richieste che includono l'intestazione if-none-match

Questa policy consente all'account 111122223333, utente Alice, di scrivere nel bucket **amzn-s3-demo-bucket1** se la richiesta include l'intestazione if-none-match, assicurando che la chiave dell'oggetto non sia già presente nel bucket. Tutte le richieste PutObject e CompleteMultipartUpload al bucket specificato devono includere l'intestazione if-none-match per avere successo. Utilizzando questa intestazione, i clienti possono scrivere su questo bucket solo se la chiave dell'oggetto non esiste nel bucket.

 Note

Questa policy imposta anche la chiave di condizione `s3:ObjectCreationOperation`, che consente di caricare più parti utilizzando le API `CreateMultipartUpload`, `UploadPart` e `UploadPartCopy`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConditionalPut",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "Condition": {
        "Null": {
          "s3:if-none-match": "false"
        }
      }
    },
    {
      "Sid": "AllowConditionalPutwithMPUs",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "Condition": {
        "Bool": {
          "s3:ObjectCreationOperation": "false"
        }
      }
    }
  ]
}
```

```
}
```

Esempio 2: consenti solo il caricamento di oggetti utilizzando **PutObject** e le richieste che includono l'intestazione if-match **CompleteMultipartUpload**

Questa policy consente all'account 111122223333, utente Alice, di scrivere su *amzn-s3-demo-bucket1* solo se la richiesta include l'intestazione if-match. Questa intestazione confronta il valore ETag di un oggetto in S3 con quello fornito dall'utente durante l'operazione WRITE. Se i valori ETag non corrispondono, l'operazione fallisce. Tutte le richieste PutObject e CompleteMultipartUpload al bucket specificato devono includere l'intestazione if-match per avere successo.

Note

Questa policy imposta anche la chiave di condizione s3:ObjectCreationOperation, che consente di caricare più parti utilizzando le API CreateMultipartUpload, UploadPart e UploadPartCopy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutObject",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
    },
    {
      "Sid": "BlockNonConditionalObjectCreation",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "Condition": {
```

```

        "Null": {
            "s3:if-match": "true"
        },
        "Bool": {
            "s3:ObjectCreationOperation": "true"
        }
    },
    {
        "Sid": "AllowGetObjectBecauseConditionalPutIfMatchETag",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:user/Alice"
        },
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
]
}

```

Esempio 3: consenti solo le richieste di caricamento di oggetti che includono l'intestazione if-none-match o if-match

Questa policy consente all'account 111122223333 e all'utente Alice di scrivere su *amzn-s3-demo-bucket1* se le richieste includono l'intestazione if-none-match o if-match. Questo permette ad Alice di caricare un oggetto se il nome della chiave non esiste nel bucket, oppure, se il nome della chiave esiste, Alice può sovrascrivere l'oggetto se l'ETag dell'oggetto corrisponde all'ETag fornito nella richiesta PUT.

Note

Questa policy imposta anche la chiave di condizione `s3:ObjectCreationOperation`, che consente di caricare più parti utilizzando le API `CreateMultipartUpload`, `UploadPart` e `UploadPartCopy`.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [

```

```

{
  "Sid": " AllowConditionalPutifAbsent",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Alice"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
  "Condition": {
    "Null": {
      "s3:if-none-match": "false"
    }
  }
},
{
  "Sid": "AllowConditionalPutIfMatchEtag",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Alice"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
  "Condition": {
    "Null": {
      "s3:if-match": "false"
    }
  }
},
{
  "Sid": "AllowConditionalObjectCreation",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Alice"
  },
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
  "Condition": {
    "Bool": {
      "s3:ObjectCreationOperation": "false"
    }
  }
},
{
  "Sid": " AllowGetObjectBecauseConditionalPutIfMatchETag",

```

```
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
  }
]
```

Come eseguire le eliminazioni condizionali

È possibile utilizzare le eliminazioni condizionali per valutare se l'oggetto esiste o è immutato prima di eliminarlo. È possibile eseguire le eliminazioni condizionali utilizzando le operazioni API `DeleteObject` o `DeleteObjects` nei bucket di directory e per uso generico S3. Per effettuare una richiesta di eliminazione condizionale, è possibile utilizzare l'intestazione HTTP `If-Match` con il valore di preconditione `*` per verificare se l'oggetto esiste o l'intestazione `If-Match` con il valore fornito `ETag` per verificare se l'oggetto è stato modificato.

Puoi applicare le eliminazioni condizionali a livello di bucket per uso generico utilizzando i bucket S3 o le policy Identity and Access Management (IAM). Per ulteriori informazioni, consulta [Applicazione delle eliminazioni condizionali sui bucket Amazon S3](#).

Note

Le valutazioni delle eliminazioni condizionali si applicano solo alla versione corrente dell'oggetto.

Argomenti

- [Come verificare se l'oggetto è stato modificato prima di eliminarlo](#)
- [Come verificare se l'oggetto esiste prima di eliminarlo](#)
- [Applicazione delle eliminazioni condizionali sui bucket Amazon S3](#)

Come verificare se l'oggetto è stato modificato prima di eliminarlo

Con le eliminazioni condizionali, è possibile proteggere l'applicazione dall'eliminazione accidentale di oggetti. È possibile utilizzare l'intestazione HTTP `If-Match` con il valore `ETag` per verificare se un

oggetto è stato modificato. Se il valore ETag di un oggetto in un bucket S3 non corrisponde al valore ETag fornito durante l'operazione di eliminazione, l'operazione non riesce. Per eliminare in modo condizionale più oggetti utilizzando l'operazione `DeleteObjects`, è necessario fornire il valore ETag nell'elemento ETag dell'oggetto nel corpo della richiesta XML. Per ulteriori informazioni, consulta [the section called “Utilizzo Content-MD5 e ETag per verificare gli oggetti caricati”](#).

Note

Per eseguire eliminazioni condizionali con l'intestazione `If-Match` con il valore ETag, è necessario disporre delle autorizzazioni `s3:DeleteObject` e `s3:GetObject`.

L'intestazione `If-Match` con il valore ETag viene valutata rispetto agli oggetti esistenti in un bucket. Se non è presente un oggetto con lo stesso nome di chiave ed ETag corrispondente, la richiesta `DeleteObject` ha esito positivo e restituisce una risposta `204 No content`. Se ETag non corrisponde, l'operazione di eliminazione non riesce con una risposta `412 Precondition Failed`. Per eliminare in modo condizionale più oggetti utilizzando l'operazione `DeleteObjects`, è possibile fornire il ETag valore nell'ETagelemento dell'oggetto nel corpo della richiesta XML. Se la richiesta ha esito positivo, l'operazione `DeleteObjects` risponde con un `200 OK` e fornisce lo stato di ogni oggetto nel corpo della risposta. Se la precondizione ha esito positivo, la risposta per l'oggetto verrà acquisita nell'elemento `<Deleted>` del corpo della risposta. Se la precondizione non riesce, la risposta per l'oggetto verrà acquisita nell'elemento `<Error>` del corpo della risposta.

È inoltre possibile ricevere una risposta di errore `409 Conflict` nel caso di richieste concorrenti, se una richiesta `DELETE` o `PUT` per un oggetto ha esito positivo prima che un'operazione di eliminazione condizionale sia stata completata su quell'oggetto. Si riceverà una risposta `404 Not Found` se una richiesta di cancellazione concorrente di un oggetto riesce prima che un'operazione di scrittura condizionale su quell'oggetto sia completata, poiché la chiave dell'oggetto non esiste più.

È possibile utilizzare l'intestazione `If-Match` con il valore ETag per le seguenti API:

- [DeleteObject](#)
- [DeleteObjects](#)

Utilizzo di AWS CLI

Il seguente comando di esempio `delete-object` tenta di eseguire un'eliminazione condizionale per un oggetto con il valore ETag `6805f2cfc46c0f04559748bb039d69a1` fornito.

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --if-match "6805f2cfc46c0f04559748bb039d69a1"
```

Per ulteriori informazioni, consulta [delete-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Il seguente comando di esempio `delete-objects` tenta di eseguire un'eliminazione condizionale per un oggetto con il valore ETag `6805f2cfc46c0f04559748bb039d69a1` fornito.

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete '{"Objects": [{"Key": "my_images.tar.bz2", "ETag": "6805f2cfc46c0f04559748bb039d69a1"}]}'
```

Per ulteriori informazioni, consulta [delete-objects](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedi [What is the? AWS Command Line Interface](#) nella Guida AWS Command Line Interface per l'utente.

Come verificare se l'oggetto esiste prima di eliminarlo

È possibile utilizzare l'intestazione `If-Match` con il valore `*` per verificare se l'oggetto esiste prima di tentare di eliminarlo. Il valore `*` indica che l'operazione deve procedere solo se l'oggetto esiste, indipendentemente dal fatto che sia stato modificato o meno.

Gli indicatori di eliminazione sono oggetti speciali contenuti nei bucket per uso generico S3 con controllo delle versioni che indicano che un oggetto è stato eliminato. Sono segnaposto che fanno apparire l'oggetto eliminato, conservando le versioni precedenti. Pertanto, quando si utilizza `If-Match: *` con un'API `DeleteObject`, l'operazione avrà esito positivo con `204 No Content` solo se l'oggetto esiste. Se l'ultima versione dell'oggetto è un indicatore di eliminazione, l'oggetto non esiste e l'API `DeleteObject` non riesce e restituisce una risposta `412 Precondition Failed`. Per ulteriori informazioni sui contrassegni di eliminazione, consulta [the section called "Utilizzo dei contrassegni di eliminazione"](#).

Per eliminare in modo condizionale più oggetti utilizzando l'operazione `DeleteObjects`, è possibile fornire `*` nell'elemento `ETag` dell'oggetto nel corpo della richiesta XML. Se la preconditione ha esito positivo, l'operazione `DeleteObjects` risponde con `200 OK` e fornisce lo stato di ogni oggetto nel corpo della risposta. Se la preconditione ha esito positivo, la risposta per l'oggetto verrà acquisita nell'elemento `<Deleted>` del corpo della risposta. Se la preconditione non riesce, la risposta per l'oggetto verrà acquisita nell'elemento `<Error>` del corpo della risposta. Se l'oggetto non esiste

durante la valutazione delle precondizioni, S3 rifiuta la richiesta e restituisce una risposta di errore `Not Found`.

Note

Per eseguire eliminazioni condizionali con `If-Match: *`, è necessario disporre delle autorizzazioni `s3:DeleteObject`.

È possibile utilizzare l'intestazione `If-Match` con il valore `*` per le seguenti API:

- [DeleteObject](#)
- [DeleteObjects](#)

Utilizzo di AWS CLI

Il comando di esempio `delete-object` seguente tenta di eseguire un'eliminazione condizionale per un oggetto con il nome della chiave `my_images.tar.bz2` con il valore `*` che rappresenta qualsiasi ETag.

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --if-match "*" 
```

Per ulteriori informazioni, consulta [delete-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Il comando di esempio `delete-objects` seguente tenta di eseguire un'eliminazione condizionale per un oggetto con il nome della chiave `my_images.tar.bz2` con il valore `*` che rappresenta qualsiasi ETag.

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete '{"Objects": [{"Key": "my_images.tar.bz2", "ETag": "*"}]}' 
```

Per ulteriori informazioni, consulta [delete-objects](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedi [Cos'è il AWS Command Line Interface?](#) nella Guida AWS Command Line Interface per l'utente.

Applicazione delle eliminazioni condizionali sui bucket Amazon S3

Utilizzando le policy di bucket Amazon S3, è possibile applicare l'intestazione If-Match con le eliminazioni condizionali per gli oggetti nei bucket per uso generico. Se l'intestazione If-Match non esiste, la richiesta verrà rifiutata con un errore 403 Access Denied. Una policy di bucket è una policy basata su risorse che puoi utilizzare per concedere autorizzazioni di accesso al bucket e agli oggetti che contiene. Solo il proprietario del bucket può associare una policy a un bucket. Per ulteriori informazioni sulle policy di bucket, consulta [the section called "Policy di bucket"](#).

Gli esempi seguenti mostrano come utilizzare le condizioni in una policy di bucket per forzare i client a utilizzare l'intestazione HTTP If-Match.

Argomenti

- [Esempio 1: consenti solo le eliminazioni condizionali utilizzando l'If-Matchintestazione con il valore ETag](#)
- [Esempio 2: consenti solo le eliminazioni condizionali utilizzando l'intestazione con il valore * If-Match](#)

Esempio 1: consenti solo le eliminazioni condizionali utilizzando l'**If-Match**intestazione con il valore ETag

Puoi utilizzare questa policy di bucket per consentire solo le eliminazioni condizionali con le richieste DeleteObject e DeleteObjects che includono l'intestazione If-Match con il valore ETag. La Null condizione garantisce la presenza dell'If-Matchintestazione e l's3:GetObjectautorizzazione viene concessa perché le eliminazioni condizionali con un valore ETag specifico richiedono entrambe le autorizzazioni. s3:DeleteObject s3:GetObject Tutte le eliminazioni non condizionali vengono negate e le eliminazioni condizionali vengono autorizzate.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConditionalDeletes",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
      },
      "Action": "s3:DeleteObject",
      "Resource": "arn:aws:s3::amzn-s3-demo-bucket/*",
```

```

        "Condition": {
            "Null": {
                "s3:if-match": "false"
            }
        },
        {
            "Sid": "AllowGetObjectBecauseConditionalDeleteIfMatchETag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3::amzn-s3-demo-bucket/*"
        }
    ]
}

```

Esempio 2: consenti solo le eliminazioni condizionali utilizzando l'intestazione con il valore * **If-Match**

Puoi utilizzare questa policy di bucket per consentire solo le eliminazioni condizionali con le richieste `DeleteObject` e `DeleteObjects` che includono l'intestazione `If-Match` con il valore `*`. La `Null` condizione garantisce la presenza dell'`If-Match` intestazione. Poiché non `s3:GetObject` è concesso, le eliminazioni condizionali con un valore `ETag` specifico falliranno: solo `If-Match: *` (che verifica l'esistenza dell'oggetto e richiede solo l'`s3:DeleteObject` autorizzazione) avranno esito positivo. Tutte le eliminazioni non condizionali verrebbero negate e solo le eliminazioni condizionali avrebbero esito positivo. `If-Match: *`

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowConditionalDeletes",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:DeleteObject",
            "Resource": "arn:aws:s3::amzn-s3-demo-bucket/*",
            "Condition": {
                "Null": {

```

```
        "s3:if-match": "false"
      }
    }
  }
}
```

Copia, spostamento e denominazione di oggetti

L'operazione `CopyObject` crea una copia di un oggetto già archiviato in Amazon S3.

È possibile creare una copia di un oggetto fino a 5 GB in una singola operazione atomica. Tuttavia, per copiare un oggetto di dimensioni superiori a 5 GB, è necessario utilizzare un caricamento in più parti utilizzando gli o SDK. AWS CLI AWS Per ulteriori informazioni, consulta [Copia di un oggetto utilizzando il caricamento in più parti](#).

Note

Per mantenere i vantaggi in termini di prestazioni di un oggetto caricato utilizzando il caricamento in più parti, devi copiare l'oggetto utilizzando il caricamento in più parti utilizzando l' AWS SDK AWS CLI or anziché la console S3. Per ulteriori informazioni, consulta [Copia di un oggetto utilizzando il caricamento in più parti](#).

L'operazione `CopyObject` consente di effettuare le seguenti operazioni:

- Creare copie aggiuntive di oggetti.
- Rinominare gli oggetti copiandoli e cancellando quelli originali.
- Copiare o spostare gli oggetti da un bucket all'altro, anche attraverso Regioni AWS (ad esempio, da `us-west-1` a `eu-west-2`). Quando si sposta un oggetto, Amazon S3 copia l'oggetto nella destinazione specificata, quindi elimina l'oggetto di origine.

Note

La copia o lo spostamento di oggetti comporta costi relativi alla larghezza di banda. Regioni AWS Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

- Modifica i metadati dell'oggetto. Ogni oggetto Amazon S3 ha metadati. Questi metadati sono un insieme di coppie nome-valore. È possibile impostare i metadati dell'oggetto al momento del

caricamento. Dopo aver caricato l'oggetto, non è possibile modificare i metadati dell'oggetto. L'unico modo per modificarli è eseguire una copia dell'oggetto e impostare i metadati. A tal fine, nell'operazione di copia, imposta lo stesso oggetto come origine e destinazione.

Alcuni metadati degli oggetti sono metadati di sistema e altri sono definiti dall'utente. È possibile controllare alcuni metadati del sistema. Ad esempio, è possibile controllare la classe di storage e il tipo di crittografia lato server da utilizzare per l'oggetto. Quando si copia un oggetto, vengono copiati anche i metadati di sistema controllati dall'utente e i metadati definiti dall'utente. Amazon S3 reimposta i metadati controllati dal sistema. Ad esempio, quando copi un oggetto, Amazon S3 reimposta la data di creazione dell'oggetto copiato. Non è necessario impostare nessuno di questi valori di metadati controllati dal sistema nella richiesta di copia.

Quando si copia un oggetto, si potrebbe decidere di aggiornare alcuni dei valori dei metadati. Ad esempio, se l'oggetto sorgente è configurato per utilizzare lo storage S3 Standard, è possibile scegliere di utilizzare S3 Intelligent-Tiering per la copia dell'oggetto. È anche possibile decidere di modificare alcuni dei valori dei metadati definiti dall'utente presenti nell'oggetto di origine. Se scegli di aggiornare uno qualsiasi dei metadati configurabili dall'utente (metadati di sistema o definiti dall'utente) dell'oggetto durante la copia, devi specificare in modo esplicito nella richiesta tutti i metadati configurabili dall'utente presenti nell'oggetto di origine, anche se stai modificando solo uno dei valori dei metadati.

Note

Quando si copia un oggetto tramite la console Amazon S3, è possibile ricevere il messaggio di errore “Copied metadata can't be verified”. La console utilizza le intestazioni per recuperare e impostare i metadati per l'oggetto. Se la configurazione della rete o del browser modifica le richieste di rete, questo comportamento potrebbe causare la scrittura non intenzionale di metadati (come intestazioni `Cache-Control` modificate) nell'oggetto copiato. Amazon S3 non può verificare questi metadati non intenzionali. Per risolvere questo problema, controlla la configurazione della rete e del browser per assicurarti che non modifichino le intestazioni, ad esempio `Cache-Control`. Per ulteriori informazioni, consulta [Il modello di responsabilità condivisa](#).

Per ulteriori informazioni sui metadati degli oggetti, consulta [Utilizzo dei metadati degli oggetti](#).

Copia di oggetti archiviati e ripristinati

Se l'oggetto di origine viene archiviato in Recupero flessibile Amazon S3 Glacier o Deep Archive Amazon S3 Glacier, è necessario ripristinare una copia temporanea prima di poter copiare l'oggetto in un altro bucket. Per ulteriori informazioni sull'archiviazione degli oggetti, consulta la sezione [Utilizzo di oggetti archiviati](#).

L'operazione di copia nella console Amazon S3 non è supportata per gli oggetti ripristinati nelle classi di storage Recupero flessibile S3 Glacier o S3 Glacier Deep Archive. Per copiare questi oggetti ripristinati, usa AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Copia di oggetti criptati

Amazon S3 esegue automaticamente la crittografia di tutti i nuovi oggetti copiati in un bucket S3. Se non si specificano le informazioni di crittografia nella richiesta di copia, la crittografia dell'oggetto di destinazione viene impostata sulla configurazione di crittografia predefinita del bucket di destinazione. Per impostazione predefinita, tutti i bucket hanno un livello di configurazione di crittografia di base che utilizza la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Se il bucket di destinazione ha una configurazione di crittografia predefinita che utilizza la crittografia lato server con una chiave AWS Key Management Service (AWS KMS) () o una chiave di crittografia fornita dal cliente (SSE-KMSSE-C), Amazon S3 utilizza la chiave KMS corrispondente o una chiave fornita dal cliente per crittografare la copia dell'oggetto di destinazione.

Quando si copia un oggetto, se si desidera utilizzare un tipo diverso di impostazione di crittografia per l'oggetto di destinazione, è possibile richiedere ad Amazon S3 di crittografare l'oggetto di destinazione con una chiave KMS, una chiave gestita da Amazon S3 o una chiave fornita dal cliente. Se l'impostazione di crittografia nella richiesta è diversa dalla configurazione di crittografia predefinita del bucket di destinazione, l'impostazione di crittografia nella richiesta ha la priorità. Se l'oggetto sorgente della copia è crittografato con SSE-C, devi fornire le informazioni di crittografia necessarie nella richiesta in modo che Amazon S3 possa decrittografare l'oggetto da copiare. Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia](#).

Utilizzo di checksum durante la copia degli oggetti

Durante la copia di oggetti puoi scegliere di utilizzare un algoritmo di checksum diverso per l'oggetto. Sia che si scelga di utilizzare lo stesso algoritmo o uno nuovo, Amazon S3 calcola un nuovo valore di checksum dopo la copia dell'oggetto. Amazon S3 non copia direttamente il valore del checksum. Tutti gli oggetti copiati senza checksum e senza algoritmi di checksum di destinazione specificati ottengono automaticamente un algoritmo di checksum CRC-64NVME. Per ulteriori informazioni sul calcolo del checksum, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Copia di più oggetti in un'unica richiesta

Per copiare più di un oggetto Amazon S3 con una singola richiesta, è possibile utilizzare anche le operazioni in batch S3. Fornisci alle operazioni in batch S3 un elenco di oggetti su cui operare. Le operazioni in batch S3 richiamano la rispettiva API per eseguire l'operazione specificata. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti contenenti esabyte di dati.

La funzionalità Operazioni in batch S3 tiene traccia dei progressi, invia notifiche e memorizza un report dettagliato sul completamento di tutte le azioni, offrendo un'esperienza serverless completamente gestita e verificabile. Puoi utilizzare S3 Batch Operations tramite la console Amazon S3, AWS CLI gli SDK o l'API REST. AWS Per ulteriori informazioni, consulta [the section called “Nozioni di base sulle operazioni in batch”](#).

Copia di oggetti nei bucket della directory

Per informazioni sulla copia di un oggetto in un bucket di directory, consulta [Copia di oggetti da o verso un bucket di directory](#). Per informazioni sull'uso della classe di storage Amazon S3 Express One Zone con i bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Copiare le annotazioni

Quando copi un oggetto utilizzando l'CopyObjectAPI, Amazon S3 copia le annotazioni dell'oggetto nella destinazione per impostazione predefinita. È possibile escludere le annotazioni dalla copia specificando l'`x-amz-annotation-directive: EXCLUDE` intestazione nella richiesta di copia.

Quando si copiano oggetti utilizzando il caricamento in più parti (ad esempio, con il AWS CLI `aws s3 cp` comando per oggetti di dimensioni superiori a circa 8 MB), le annotazioni non vengono copiate per impostazione predefinita. Per includere annotazioni quando si copiano oggetti con caricamento in più parti, specificare. `--copy-props all`

Per ulteriori informazioni sulle annotazioni, vedere. [Annotazione degli oggetti](#)

Per copiare un oggetto

Per copiare un oggetto utilizza i metodi riportati di seguito.

Utilizzo della console S3

Note

Le restrizioni e le limitazioni quando si copia un oggetto con la console sono le seguenti:

- È possibile copiare un oggetto se il suo oggetto è inferiore a 5 GB. Se l'oggetto è superiore a 5 GB, è necessario utilizzare gli SDK [AWS CLI](#) o [AWS per copiare un oggetto](#).
- Per un elenco delle autorizzazioni aggiuntive necessarie per copiare gli oggetti, consulta [the section called “Autorizzazioni necessarie per le operazioni API S3”](#). Per esempi di policy che concedono questa autorizzazione, consulta [the section called “Identity-based esempi di policy”](#).
- L'azione Copy si applica a tutti gli oggetti all'interno delle cartelle (prefissi) specificate. Gli oggetti aggiunti a queste cartelle mentre l'azione è in corso potrebbero essere interessati.
- Cross-Region la copia di oggetti crittografati con non SSE-KMS è supportata dalla console Amazon S3. Per copiare oggetti crittografati con SSE-KMS più regioni, utilizza l' AWS CLI AWS SDK o l'API REST di Amazon S3.
- Gli oggetti crittografati con chiavi di crittografia fornite dal cliente (SSE-C) non possono essere copiati utilizzando la console S3. Per copiare oggetti crittografati con SSE-C, utilizza l' AWS SDK o l' AWS CLI API REST di Amazon S3.
- Gli oggetti copiati non manterranno le impostazioni di Object Lock dagli oggetti originali.
- Se il bucket da cui si stanno copiando gli oggetti utilizza l'impostazione del proprietario del bucket per la proprietà degli oggetti S3, le ACL degli oggetti non verranno copiate nella destinazione specificata.
- Se desideri copiare oggetti in un bucket che utilizza l'impostazione imposta dal proprietario del bucket per S3 Object Ownership, assicurati che anche il bucket di origine utilizzi l'impostazione imposta dal proprietario del bucket o rimuovi qualsiasi oggetto che ACL concede ad altri account e gruppi. AWS

Per copiare un oggetto

1. Accedi e apri la console Amazon S3 all'indirizzo. Console di gestione AWS <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.
3. Nell'elenco dei bucket scegli il nome del bucket che contiene gli oggetti da copiare.

4. Selezionare la casella di controllo a sinistra dei nomi degli oggetti da copiare.
5. Nel menu Azioni, scegli Copia dall'elenco delle opzioni visualizzate.
6. Selezionare il tipo di destinazione e l'account di destinazione. Per specificare il percorso di destinazione, scegliere Browse S3 (Sfoglia S3), passare alla destinazione e selezionare la casella di controllo a sinistra della destinazione. Scegliere Choose destination (Scegli destinazione).

In alternativa, immettere il percorso di destinazione.

7. Se non è abilitato il controllo delle versioni del bucket, viene visualizzato un avviso che consiglia di abilitarlo per evitare la sovrascrittura o l'eliminazione involontaria di oggetti. Se si desidera mantenere tutte le versioni degli oggetti in questo bucket, seleziona Abilita versioni multiple per il bucket. È inoltre possibile visualizzare la crittografia predefinita e le proprietà di S3 Object Lock in Dettagli destinazione.
8. In Impostazioni di copia aggiuntive, scegli se eseguire Copia impostazioni dell'origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni dell'origine, scegli Non specificare le impostazioni. Scegli Specifica le impostazioni per specificare le impostazioni per la classe di archiviazione, gli ACL, i tag degli oggetti, le annotazioni, i metadati, la crittografia lato server e i checksum aggiuntivi.
9. Scegli Copia. Amazon S3 copia gli oggetti nella destinazione.

Utilizzo di AWS SDK

Gli esempi in questa sezione mostrano come copiare gli oggetti con dimensioni superiori a 5 GB in una singola operazione. Per copiare oggetti di dimensioni superiori a 5 GB, è necessario utilizzare un caricamento multipart. Per ulteriori informazioni, consulta [Copia di un oggetto utilizzando il caricamento in più parti](#).

Java

Per esempi di come copiare oggetti con l' AWS SDK per Java, consulta [Copiare un oggetto da un bucket all'altro nell'Amazon S3 API Reference](#).

.NET

Il seguente esempio in C# utilizza l'alto livello SDK per .NET per copiare oggetti di dimensioni fino a 5 GB in una singola operazione. Per gli oggetti con una dimensione superiore a 5 GB, utilizza

l'esempio di copia di un caricamento in più parti descritto in [Copia di un oggetto utilizzando il caricamento in più parti](#).

Questo esempio crea una copia di un oggetto con dimensione massima di 5 GB. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CopyObjectTest
    {
        private const string sourceBucket = "**** provide the name of the bucket with
source object ****";
        private const string destinationBucket = "**** provide the name of the bucket
to copy the object to ****";
        private const string objectKey = "**** provide the name of object to copy
****";
        private const string destObjectKey = "**** provide the destination object key
name ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Copying an object");
            CopyingObjectAsync().Wait();
        }

        private static async Task CopyingObjectAsync()
        {
            try
            {
                CopyObjectRequest request = new CopyObjectRequest
                {
```

```

        SourceBucket = sourceBucket,
        SourceKey = objectKey,
        DestinationBucket = destinationBucket,
        DestinationKey = destObjectKey
    };
    CopyObjectResponse response = await
s3Client.CopyObjectAsync(request);
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
    }
}
}

```

PHP

Questo argomento illustra l'utilizzo delle classi della versione 3 AWS SDK per PHP per copiare uno o più oggetti all'interno di Amazon S3, da un bucket all'altro o all'interno dello stesso bucket.

Per ulteriori informazioni sull'API AWS SDK for Ruby, consulta SDK for Ruby - [AWS Version 2](#).

Il seguente esempio PHP illustra l'uso del metodo `copyObject()` per copiare un singolo oggetto all'interno di Amazon S3. Dimostra inoltre come creare copie multiple di un oggetto utilizzando un gruppo di chiamate a `CopyObject` con il metodo `getCommand()`.

Copia di oggetti

1	Crea un'istanza di un client Amazon S3 utilizzando il costruttore della classe <code>Aws\S3\S3Client</code> .
2	Per creare più copie di un oggetto, si esegue una serie di chiamate al metodo del client Amazon S3 getCommand() che è ereditato dalla classe Aws\CommandInterface . Specificare il comando <code>CopyObject</code> come primo argomento e un

array contenente il bucket di origine, il nome della chiave di origine, il bucket di destinazione e il nome della chiave di destinazione come secondo argomento.

```
require 'vendor/autoload.php';

use Aws\CommandPool;
use Aws\Exception\AwsException;
use Aws\ResultInterface;
use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';
$targetBucket = '*** Your Target Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region' => 'us-east-1'
]);

// Copy an object.
$s3->copyObject([
    'Bucket' => $targetBucket,
    'Key' => "$sourceKeyname-copy",
    'CopySource' => "$sourceBucket/$sourceKeyname",
]);

// Perform a batch of CopyObject operations.
$batch = array();
for ($i = 1; $i <= 3; $i++) {
    $batch[] = $s3->getCommand('CopyObject', [
        'Bucket' => $targetBucket,
        'Key' => "{targetKeyname}-$i",
        'CopySource' => "$sourceBucket/$sourceKeyname",
    ]);
}
try {
    $results = CommandPool::batch($s3, $batch);
    foreach ($results as $result) {
        if ($result instanceof ResultInterface) {
            // Result handling here
        }
        if ($result instanceof AwsException) {

```

```

        // AwsException handling here
    }
}
} catch (Exception $e) {
    // General error handling here
}

```

Python

```

class ObjectWrapper:
    """Encapsulates S3 object actions."""

    def __init__(self, s3_object):
        """
        :param s3_object: A Boto3 Object resource. This is a high-level resource in
        Boto3
                           that wraps object actions in a class-like structure.
        """
        self.object = s3_object
        self.key = self.object.key

```

```

    def copy(self, dest_object):
        """
        Copies the object to another bucket.

        :param dest_object: The destination object initialized with a bucket and
        key.
                           This is a Boto3 Object resource.
        """
        try:
            dest_object.copy_from(
                CopySource={"Bucket": self.object.bucket_name, "Key":
                self.object.key}
            )
            dest_object.wait_until_exists()
            logger.info(
                "Copied object from %s:%s to %s:%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,

```

```
)
except ClientError:
    logger.exception(
        "Couldn't copy object from %s/%s to %s/%s.",
        self.object.bucket_name,
        self.object.key,
        dest_object.bucket_name,
        dest_object.key,
    )
    raise
```

Ruby

Le seguenti operazioni guidano all'uso delle classi Ruby per copiare un oggetto in Amazon S3 da un bucket a un altro o all'interno dello stesso bucket.

Copia di oggetti

- 1 Usa la gemma modularizzata Amazon S3 per la versione 3 di, richiedi e fornisci le AWS SDK per Ruby tue credenziali. `aws-sdk-s3` AWS Per ulteriori informazioni su come fornire le credenziali, consulta [Effettuare richieste utilizzando le credenziali dell' AWS account o dell'utente IAM nell'API Reference di Amazon S3](#).
- 2 Fornisci le informazioni sulla richiesta, come il nome del bucket di origine, il nome della chiave di origine, il nome del bucket di destinazione e la chiave di destinazione.

Il seguente esempio di codice Ruby dimostra le operazioni precedenti utilizzando il metodo `#copy_object` per copiare un oggetto da un bucket a un altro.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
  # used as the source object for
  # copy actions.
  def initialize(source_object)
```

```

    @source_object = source_object
  end

  # Copy the source object to the specified target bucket and rename it with the
  # target key.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
  # object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
  # nil.
  def copy_object(target_bucket, target_object_key)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
    #{e.message}"
  end
end

# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
  target_key = "my-target-file.txt"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
  target_object = wrapper.copy_object(target_bucket, target_key)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
  #{target_object.bucket_name}:#{target_object.key}."
end

run_demo if $PROGRAM_NAME == __FILE__

```

Utilizzo della REST API

Questo esempio descrive come copiare un oggetto utilizzando la REST API di Amazon S3. Per ulteriori informazioni su REST API, consulta [CopyObject](#).

In questo esempio viene copiato l'oggetto `flotsam` dal bucket `amzn-s3-demo-bucket1` all'oggetto `jetsam` del bucket `amzn-s3-demo-bucket2` conservandone i metadata.

```
PUT /jetsam HTTP/1.1
Host: amzn-s3-demo-bucket2.s3.amazonaws.com
x-amz-copy-source: /amzn-s3-demo-bucket1/flotsam
Authorization: AWS AKIAIOSFODNN7EXAMPLE:ENoSbxYByFA0UGLZUqJN5EUUnLDg=
Date: Wed, 20 Feb 2008 22:12:21 +0000
```

La firma viene generata dalle seguenti informazioni.

```
PUT\r\n
\r\n
\r\n
Wed, 20 Feb 2008 22:12:21 +0000\r\n

x-amz-copy-source:/amzn-s3-demo-bucket1/flotsam\r\n
/amzn-s3-demo-bucket2/jetsam
```

Amazon S3 restituisce la risposta riportata di seguito che specifica l'ETag dell'oggetto e la data dell'ultima modifica.

```
HTTP/1.1 200 OK
x-amz-id-2: Vyaxt7qEbzv34BnSu5hctyyNSlHTYZFMWK4Ftz0+iX8JQNyaLdTshL0Kxatba0Zt
x-amz-request-id: 6B13C3C5B34AF333
Date: Wed, 20 Feb 2008 22:13:01 +0000

Content-Type: application/xml
Transfer-Encoding: chunked
Connection: close
Server: AmazonS3
<?xml version="1.0" encoding="UTF-8"?>

<CopyObjectResult>
  <LastModified>2008-02-20T22:13:01</LastModified>
  <ETag>"7e9c608af58950deeb370c98608ed097"</ETag>
```

```
</CopyObjectResult>
```

Utilizzo di AWS CLI

Puoi anche usare AWS Command Line Interface (AWS CLI) per copiare un oggetto S3. Per ulteriori informazioni, consulta [copy-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedete [What is the AWS Command Line Interface?](#) nella Guida AWS Command Line Interface per l'utente.

Spostare un oggetto.

Per spostare un oggetto, utilizza i seguenti metodi.

Utilizzo della console S3

Note

- È possibile spostare un oggetto se la dimensione dell'oggetto è inferiore a 5 GB. Se l'oggetto è superiore a 5 GB, è necessario utilizzare gli SDK [AWS CLI](#) o [AWS per spostare un oggetto](#).
- Per un elenco delle autorizzazioni aggiuntive necessarie per spostare gli oggetti, consulta [the section called “Autorizzazioni necessarie per le operazioni API S3”](#). Per esempi di policy che concedono questa autorizzazione, consulta [the section called “Identity-based esempi di policy”](#).
- Gli oggetti crittografati con chiavi di crittografia fornite dal cliente (SSE-C) non possono essere spostati utilizzando la console Amazon S3. Per spostare oggetti crittografati con SSE-C, utilizza gli AWS SDK o l' AWS CLI API REST di Amazon S3.
- Quando si spostano le cartelle, attendi il termine dell'operazione di spostamento prima di apportare ulteriori modifiche alle cartelle.
- Non è possibile utilizzare gli alias dei punti di accesso S3 come origine o destinazione per le operazioni di spostamento nella console Amazon S3.

Spostare un oggetto.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket). Passare al bucket o alla cartella Amazon S3 che contiene gli oggetti che si desidera spostare.
3. Seleziona la casella di controllo degli oggetti da spostare.
4. Nel menu Azioni, scegli Sposta.
5. Per specificare il percorso di destinazione, scegli Sfoglia S3, naviga fino alla destinazione e seleziona la casella di controllo della destinazione. Scegliere Choose destination (Scegli destinazione).

In alternativa, immettere il percorso di destinazione.

6. Se non è abilitato il controllo delle versioni del bucket, viene visualizzato un avviso che consiglia di abilitarlo per evitare la sovrascrittura o l'eliminazione involontaria di oggetti. Se si desidera mantenere tutte le versioni degli oggetti in questo bucket, seleziona Abilita versioni multiple per il bucket. È inoltre possibile visualizzare le proprietà di crittografia e Object Lock predefinite in Dettagli destinazione.
7. In Impostazioni di copia aggiuntive, scegli se vuoi copiare le impostazioni di origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni di origine, scegli Non specificare le impostazioni. Scegli Specifica le impostazioni per specificare le impostazioni per la classe di storage, le ACL, i tag degli oggetti, i metadati, la crittografia lato server e i checksum aggiuntivi.
8. Scegliete Sposta. Amazon S3 sposta i tuoi oggetti nella destinazione.

Utilizzo di AWS CLI

Potete anche usare il pulsante AWS Command Line Interface (AWS CLI) per spostare un oggetto S3. Per ulteriori informazioni, consulta [mv](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per informazioni su AWS CLI, vedete [What is the AWS Command Line Interface?](#) nella Guida AWS Command Line Interface per l'utente.

Per rinominare un oggetto

Per rinominare un oggetto, utilizza la procedura seguente.

 Note

- È possibile rinominare un oggetto se l'oggetto è inferiore a 5 GB. Per rinominare oggetti di dimensioni superiori a 5 GB, è necessario utilizzare gli SDK [AWS CLI](#) o [AWS per copiare l'oggetto con un nuovo nome ed eliminare l'oggetto originale](#).
- Per un elenco delle autorizzazioni aggiuntive necessarie per copiare gli oggetti, consulta [the section called “Autorizzazioni necessarie per le operazioni API S3”](#). Per esempi di policy che concedono questa autorizzazione, consulta [the section called “Identity-based esempi di policy”](#).
- La ridenominazione di un oggetto crea una copia dell'oggetto con una nuova data di ultima modifica e aggiunge un indicatore di cancellazione all'oggetto originale.
- Le impostazioni del bucket per la crittografia predefinita vengono applicate automaticamente a qualsiasi oggetto specificato non crittografato.
- Non è possibile utilizzare la console Amazon S3 per rinominare oggetti con chiavi di crittografia fornite dal cliente (). SSE-C Per rinominare gli oggetti crittografati con SSE-C, utilizza gli AWS SDK o l' AWS CLI API REST di Amazon S3 per copiare tali oggetti con nuovi nomi.
- Se questo bucket utilizza l'impostazione del proprietario del bucket per la proprietà degli oggetti S3, le liste di controllo degli accessi (ACL) per gli oggetti non verranno copiate.

Per rinominare un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket, quindi scegli la scheda Bucket per uso generico. Naviga al bucket o alla cartella Amazon S3 che contiene l'oggetto da rinominare.
3. Seleziona la casella di controllo dell'oggetto da rinominare.
4. Nel menu Azioni, scegli Rinomina oggetto.
5. Nella casella Nuovo nome oggetto, inserisci il nuovo nome dell'oggetto.
6. In Impostazioni di copia aggiuntive, scegli se vuoi copiare le impostazioni di origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni di origine, scegli Non specificare le impostazioni. Scegli Specifica le impostazioni per specificare

le impostazioni per la classe di storage, le ACL, i tag degli oggetti, i metadati, la crittografia lato server e i checksum aggiuntivi.

7. Scegli Save changes (Salva modifiche). Amazon S3 rinomina l'oggetto.

Download di oggetti

In questa sezione viene illustrato come scaricare oggetti da un bucket Amazon S3. Con Amazon S3, puoi archiviare oggetti in uno o più bucket e ogni singolo oggetto può avere una dimensione massima di 50 TB. Qualsiasi oggetto Amazon S3 non archiviato è accessibile in tempo reale. Gli oggetti archiviati, tuttavia, devono essere ripristinati prima di poter essere scaricati. Per ulteriori informazioni sul download di oggetti archiviati, consulta [the section called “Download di oggetti archiviati”](#).

Puoi scaricare un singolo oggetto utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3. Per scaricare un oggetto fino a 5 TB da S3 senza scrivere codice o eseguire comandi, utilizza la console S3. Per ulteriori informazioni, consulta [the section called “Download di un oggetto”](#).

Per scaricare oggetti di dimensioni superiori a 5 TB, utilizza `GetObject` le richieste simultanee con intestazione `Range HTTP` per leggere intervalli di byte specifici o per `partNumber` scaricare una parte specifica di un oggetto. Le richieste GET singole sono limitate a 5 TB e riceverai un `405 - Method Not Allowed` errore per le richieste GET superiori a 5 TB.

Per il download di oggetti di grandi dimensioni, utilizzate S3 Transfer Manager in Java v1/v2, Python o AWS CLI SDK. Per ottenere prestazioni ottimali, utilizzate la versione più recente di AWS Common Runtime (CRT) con questi SDK, che è stata ottimizzata per un migliore utilizzo delle risorse. Il CRT ridimensiona automaticamente le dimensioni dei singoli GET per ottimizzare la produttività. È possibile migliorare la velocità di trasferimento complessiva allocando più memoria utilizzando parametri di limite di memoria come per Java SDK. `maxNativeMemoryLimitInBytes` È possibile disattivare questo comportamento impostando una dimensione esplicita della parte utilizzando parametri di richiesta come `multipart_chunksize` for AWS CLI e `minimumPartSizeInBytes` per Java SDK nella richiesta di download.

Per scaricare più oggetti, usa AWS CloudShell AWS CLI, o gli AWS SDK. Per ulteriori informazioni, consulta [the section called “Download di più oggetti”](#).

Se devi scaricare parte di un oggetto, utilizza parametri aggiuntivi con l'API AWS CLI o REST per specificare solo i byte che desideri scaricare. Per ulteriori informazioni, consulta [the section called “Download di parte di un oggetto”](#).

Se devi scaricare un oggetto di cui non sei il proprietario, chiedi al proprietario dell'oggetto di generare un URL prefirmato che ti consenta di scaricare l'oggetto. Per ulteriori informazioni, consulta [the section called “Scaricamento di un oggetto da un altro Account AWS”](#).

Quando scarichi oggetti al di fuori della AWS rete, si applicano le tariffe per il trasferimento dei dati. Il trasferimento dei dati all'interno della AWS rete è gratuito all'interno della stessa Regione AWS, ma eventuali GET richieste ti verranno addebitate. Per ulteriori informazioni sui costi del trasferimento dei dati e le tariffe di recupero dei dati, consulta [Prezzi di Amazon S3](#).

Argomenti

- [Download di un oggetto](#)
- [Download di più oggetti](#)
- [Download di parte di un oggetto](#)
- [Scaricamento di un oggetto da un altro Account AWS](#)
- [Download di oggetti archiviati](#)
- [Download di oggetti in base ai metadati](#)
- [Risoluzione dei problemi di download degli oggetti](#)

Download di un oggetto

Puoi scaricare un oggetto utilizzando la console Amazon S3 AWS CLI, gli AWS SDK o l'API REST.

Utilizzo della console S3

In questa sezione viene illustrato come utilizzare la console Amazon S3 per scaricare un oggetto da un bucket S3.

Note

- Puoi scaricare un solo oggetto alla volta.
- Se utilizzi la console di Amazon S3 per scaricare un oggetto il cui nome della chiave termina con un punto (.), il punto viene rimosso dal nome della chiave dell'oggetto scaricato. Per mantenere il punto alla fine del nome dell'oggetto scaricato, devi utilizzare AWS Command Line Interface (AWS CLI), AWS SDK o l'API REST di Amazon S3.

Per scaricare un oggetto da un bucket S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.
3. Nell'elenco dei bucket scegli il nome del bucket dal quale desideri scaricare un oggetto.
4. È possibile scaricare un oggetto da un bucket S3 in uno qualsiasi dei modi seguenti:
 - Seleziona la casella di controllo accanto all'oggetto e scegli Scarica. Se desideri scaricare l'oggetto in una cartella specifica, nel menu Azioni, scegli Scarica come.
 - Se desideri scaricare una versione specifica dell'oggetto, attiva Mostra versioni (che si trova accanto alla casella di ricerca). Seleziona la casella di controllo accanto alla versione dell'oggetto desiderato e scegli Scarica. Se desideri scaricare l'oggetto in una cartella specifica, nel menu Azioni, scegli Scarica come.

Utilizzo di AWS CLI

L'esempio `get-object` seguente mostra come utilizzare la AWS CLI per scaricare un oggetto da Amazon S3. Questo comando recupera l'oggetto *folder/my_image* dal bucket *amzn-s3-demo-bucket1*. È necessario includere un outfile, che è un nome di file per l'oggetto scaricato, ad esempio *my_downloaded_image.jpg*.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/  
my_image my_downloaded_image.jpg
```

Per ulteriori informazioni ed esempi, consulta [get-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo di AWS SDK

Per esempi su come scaricare un oggetto con gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Utilizzo della REST API

Puoi utilizzare REST API per recuperare oggetti da Amazon S3. Per ulteriori informazioni, consulta [GetObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Download di più oggetti

Puoi scaricare più oggetti utilizzando AWS CloudShell, gli o gli SDK AWS CLI. AWS

Utilizzo AWS CloudShell nel Console di gestione AWS

AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da Console di gestione AWS

Per ulteriori informazioni, consulta What is AWS CloudShell? [CloudShell](#) nella Guida AWS CloudShell per l'utente.

Important

Con AWS CloudShell, la tua home directory ha uno spazio di archiviazione fino a 1 GB per Regione AWS. Pertanto non puoi sincronizzare i bucket con oggetti per un totale superiore a tale quantità. Per ulteriori limitazioni, consulta [Service quotas e restrizioni](#) nella Guida per l'utente di AWS CloudShell.

Per scaricare oggetti utilizzando AWS CloudShell

1. Accedi a Console di gestione AWS e apri la CloudShell console all'indirizzo <https://console.aws.amazon.com/cloudshell/>.
2. Esegui il seguente comando per sincronizzare gli oggetti nel bucket con CloudShell. Il comando seguente sincronizza gli oggetti dal bucket denominato *amzn-s3-demo-bucket1* e crea una cartella denominata in *temp*. CloudShell sincronizza i tuoi oggetti in questa cartella. Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3 sync s3://amzn-s3-demo-bucket1 ./temp
```

 Note

Il comando `sync` non è compatibile con i bucket di directory.
Per eseguire la corrispondenza del modello per escludere o includere oggetti particolari, puoi utilizzare i parametri `--exclude "value"` e `--include "value"` con il comando `sync`.

3. Esegui il comando seguente per comprimere gli oggetti nella cartella denominata `temp` in un file denominato `temp.zip`.

```
zip temp.zip -r temp/
```

4. Scegli Azioni, quindi seleziona Scarica file.
5. Immetti un nome file `temp.zip`, quindi scegli Scarica.
6. (Facoltativo) Elimina il `temp.zip` file e gli oggetti sincronizzati con la `temp` cartella in CloudShell. Con AWS CloudShell, disponi di un'archiviazione persistente fino a 1 GB per ciascuna Regione AWS.

Puoi utilizzare il seguente comando di esempio per eliminare il file `.zip` e la cartella. Per utilizzare questo comando di esempio, sostituisci `user input placeholders` con le tue informazioni.

```
rm temp.zip && rm -rf temp/
```

Utilizzo di AWS CLI

L'esempio seguente mostra come è possibile utilizzare il AWS CLI per scaricare tutti i file o gli oggetti nella directory o nel prefisso specificato. Questo comando copia tutti gli oggetti dal bucket `amzn-s3-demo-bucket1` nella directory corrente. Per utilizzare questo comando di esempio, usa il nome del bucket al posto di `amzn-s3-demo-bucket1`.

```
aws s3 cp s3://amzn-s3-demo-bucket1 . --recursive
```

Il comando seguente scarica tutti gli oggetti sotto il prefisso `logs` nel bucket `amzn-s3-demo-bucket1` nella directory corrente. Inoltre, utilizza i parametri `--exclude` e `--include` per copiare

solo gli oggetti con il suffisso `.log`. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3 cp s3://amzn-s3-demo-bucket1/logs/ . --recursive --exclude "*" --include "*.log"
```

Per ulteriori informazioni ed esempi, consulta [cp](#) nel Riferimento ai comandi AWS CLI .

Utilizzo di AWS SDK

Per esempi su come scaricare tutti gli oggetti in un bucket Amazon S3 con gli AWS SDK, consulta Esempi di [codice](#) nell'Amazon S3 API Reference.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK nell'API Reference di Amazon S3](#).

Download di parte di un oggetto

Puoi scaricare parte di un oggetto utilizzando l'API o REST. AWS CLI A tale scopo, utilizza parametri aggiuntivi per specificare la parte di un oggetto da scaricare.

Utilizzo di AWS CLI

Il comando di esempio seguente esegue una richiesta GET per un intervallo di byte nell'oggetto denominato `folder/my_data` nel bucket denominato `amzn-s3-demo-bucket1`. Nella richiesta, l'intervallo di byte deve essere preceduto da `bytes=`. L'oggetto parziale viene scaricato nel file di output denominato `my_data_range`. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/my_data --range  
bytes=0-500 my_data_range
```

Per ulteriori informazioni ed esempi, consulta [get-object](#) nel Riferimento ai comandi AWS CLI .

Per ulteriori informazioni sull'intestazione Range HTTP, consulta [RFC 9110](#) nel sito Web RFC Editor.

Note

Amazon S3 non supporta il recupero di più intervalli di dati in una singola richiesta GET.

Utilizzo della REST API

Puoi utilizzare i parametri `partNumber` e `Range` nella REST API per recuperare parti di oggetti da Amazon S3. Per ulteriori informazioni, consulta [GetObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Scaricamento di un oggetto da un altro Account AWS

Per concedere un accesso limitato nel tempo agli oggetti senza aggiornare la policy del bucket, puoi utilizzare un URL prefirmato.

Un URL prefirmato può essere inserito in un browser o utilizzato da un programma per scaricare un oggetto. Le credenziali utilizzate dall'URL sono quelle dell'AWS utente che ha generato l'URL. Dopo che l'URL viene creato, chiunque disponga dell'URL prefirmato può scaricare l'oggetto corrispondente fino alla scadenza dell'URL.

Utilizzo di un URL prefirmato nella console S3

Le seguenti fasi consentono di utilizzare la console Amazon S3 per generare un URL prefirmato per la condivisione di un oggetto in un bucket per uso generico. Quando si utilizza la console, il tempo massimo di scadenza per un URL prefirmato è di 12 ore dal momento della creazione.

Generazione di un URL prefirmato utilizzando la console di Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket contenente l'oggetto per cui desideri ottenere l'URL prefirmato.
4. Nell'elenco Objects (Oggetti), seleziona l'oggetto per cui desideri creare un URL prefirmato.
5. Nel menu Operazioni oggetti, scegli Crea URL prefirmato.
6. Specifica per quanto tempo desideri che l'URL prefirmato sia valido.
7. Scegli Create presigned URL (Crea URL prefirmato).
8. Quando viene visualizzato un messaggio di conferma, l'URL viene automaticamente copiato negli appunti. Verrà visualizzato un pulsante per copiare l'URL preimpostato qualora fosse necessario copiarlo di nuovo.
9. Per scaricare l'oggetto, incolla l'URL in qualsiasi browser; l'oggetto tenderà di scaricarlo.

Per ulteriori informazioni sugli URL prefissati e altri metodi per crearli, consulta [Download e caricamento di oggetti con URL predefiniti](#).

Download di oggetti archiviati

Per ridurre i costi di archiviazione degli oggetti a cui si accede raramente, è possibile archiviare tali oggetti. Quando si archivia un oggetto, questo viene spostato in una archiviazione a basso costo, il che significa che non è possibile accedervi in tempo reale. Per scaricare un oggetto archiviato, occorre prima ripristinarlo.

Puoi ripristinare oggetti archiviati in pochi minuti o ore, a seconda della classe di storage. Puoi ripristinare un oggetto archiviato utilizzando la console Amazon S3, S3 Batch Operations, l'API REST di Amazon S3, AWS gli SDK e (). AWS Command Line Interface AWS CLI

Per istruzioni, consulta l'argomento [Ripristino di un oggetto archiviato](#). Dopo aver ripristinato l'oggetto archiviato, puoi scaricarlo.

Download di oggetti in base ai metadati

È possibile aggiungere precondizioni per scaricare un oggetto in base ai suoi metadati, utilizzando una richiesta di lettura condizionale. È possibile restituire un oggetto in base al suo tag entità (ETag) o alla data dell'ultima modifica. Questo può limitare un'operazione S3 agli oggetti aggiornati da una data specifica o restituire solo una versione specifica dell'oggetto.

Si possono usare le scritture condizionali per richieste [GetObject](#) o [HeadObject](#).

Per ulteriori informazioni sulle richieste condizionali, consulta [Aggiunta di precondizioni alle operazioni S3 con richieste condizionali](#).

Risoluzione dei problemi di download degli oggetti

Autorizzazioni insufficienti o policy utente errate per bucket o AWS Identity and Access Management (IAM) possono causare errori quando si tenta di scaricare oggetti da Amazon S3. Questi problemi possono spesso causare errori di accesso negato (403 Forbidden), in cui Amazon S3 non è in grado di consentire l'accesso a una risorsa.

Per cause comuni di errori di accesso negato (403 Forbidden), consulta [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#).

Se ricevi un NoSuchKey errore 404 quando provi ad accedere a un oggetto, vedi [Come posso risolvere l'errore 404 NoSuchKey da Amazon S3?](#) nel Knowledge Center. AWS re:Post

Verifica dell'integrità degli oggetti in Amazon S3

Amazon S3 offre una serie di funzionalità di protezione dei dati durante l'intero ciclo di vita dell'archiviazione di un oggetto. Con Amazon S3 puoi utilizzare i valori di checksum per verificare l'integrità dei dati caricati o scaricati. Inoltre, puoi richiedere il calcolo di un altro valore di checksum per qualsiasi oggetto da archiviare in S3.

Durante il caricamento, la copia o la gestione dei dati, puoi scegliere tra diversi algoritmi di checksum supportati:

- CRC-64/NVME (CRC64NVME)

Note

L'algoritmo di checksum CRC64NVME è l'algoritmo di checksum predefinito utilizzato per i calcoli di checksum.

- CRC-32 (CRC32)
- CRC-32C (CRC32C)
- SHA-1 (SHA1)
- SHA-256 (SHA256)
- MD5 () MD5
- XXHash 64 () XXHASH64
- Hash XX (3) XXHASH3
- XXHash 128 () XXHASH128
- SHA-512 (SHA512)

Note

Puoi fornire un checksum MD5 precalcolato utilizzando l'intestazione. `x-amz-checksum-md5` AWS Gli SDK non calcolano automaticamente i checksum MD5. Per i caricamenti in più parti, l'operazione `Compute checksum` in `S3 Batch Operations` può calcolare i checksum MD5 completi degli oggetti per gli oggetti inattivi. L'intestazione precedente rimane disponibile per i `Content-MD5` caricamenti di singole parti mediante crittografia. `SSE-S3`

Quando carichi un oggetto su S3, puoi specificare l'utilizzo di uno di questi algoritmi di checksum. Per i caricamenti, tutti i AWS client di proprietà calcolano un checksum dell'oggetto e lo inviano insieme alla richiesta di caricamento. Quindi, S3 calcola indipendentemente un valore di checksum dell'oggetto sul lato server e lo convalida con il valore fornito prima di archiviare l'oggetto e il valore di checksum. Puoi anche fornire valori precalcolati per questi algoritmi di checksum quando esegui un caricamento di una singola parte o in più parti (utilizzando il tipo di checksum dell'oggetto completo per i caricamenti in più parti). Per utilizzare valori precalcolati con più oggetti, usa gli SDK o. AWS CLI AWS

In alternativa, se desideri verificare i set di dati in S3 senza dover ripristinare o scaricare dati, puoi utilizzare l'operazione Calcola il checksum con Operazioni in batch S3. L'operazione Calcola il checksum consente di verificare in modo efficiente miliardi di oggetti in un'unica richiesta di processo. Quando viene eseguita l'operazione Calcola il checksum, S3 calcola i valori di checksum per un elenco di oggetti, a riposo. Al termine della richiesta di processo, viene generato automaticamente un report sull'integrità (noto anche come report di completamento) che puoi utilizzare per confermare che il set di dati rimanga intatto.

Argomenti

- [Verifica dell'integrità degli oggetti per caricamenti dei dati in Amazon S3](#)
- [Verifica dell'integrità degli oggetti per i dati a riposo in Amazon S3](#)

Verifica dell'integrità degli oggetti per caricamenti dei dati in Amazon S3

Amazon S3 utilizza valori di checksum per verificare l'integrità dei dati durante le operazioni di caricamento e download. Quando carichi i dati, AWS SDK Console di gestione AWS utilizza l'algoritmo di checksum scelto per calcolare un valore di checksum prima della trasmissione dei dati. S3 calcola quindi in modo indipendente un checksum dei dati e lo convalida rispetto al valore di checksum fornito. Gli oggetti vengono accettati solo dopo aver confermato che l'integrità dei dati è stata mantenuta durante il transito. S3 archivia il valore di checksum come metadati dell'oggetto e l'oggetto stesso.

Per verificare l'integrità dell'oggetto, è possibile richiedere il valore di checksum durante i download. Questa convalida funziona in modo coerente in tutte le modalità di crittografia, dimensioni degli oggetti, classi di archiviazione e in tutti i caricamenti sia di singole parti sia in più parti. Per modificare l'algoritmo di checksum per un caricamento, puoi copiare un singolo oggetto o utilizzare la copia in batch per più oggetti.

Per i caricamenti di singole parti, puoi fornire valori di checksum come intestazioni. Puoi fornire un valore precalcolato o lasciare che l' AWS SDK ne calcoli uno durante il caricamento. Se il valore di checksum calcolato da S3 corrisponde al valore fornito, la richiesta viene accettata. Se i valori non corrispondono, la richiesta viene rifiutata.

Per i caricamenti in più parti, gli AWS SDK possono creare automaticamente checksum finali per i caricamenti in blocchi. Quando usi un checksum finale, Amazon S3 genera valori di checksum per ogni parte utilizzando l'algoritmo specificato e aggiunge il valore di checksum alla fine della richiesta di caricamento in blocchi. S3 esegue la verifica e il caricamento in un unico passaggio, migliorando l'efficienza. Per ulteriori informazioni, consultare le [Utilizzo dei checksum finali](#).

Utilizzo di algoritmi di checksum supportati

Con Amazon S3, è possibile scegliere un algoritmo di checksum per convalidare i valori di checksum durante i caricamenti. L'algoritmo di checksum specificato viene quindi memorizzato con l'oggetto e può essere usato per convalidare l'integrità dei dati durante i download. È possibile scegliere uno dei seguenti algoritmi di checksum Secure Hash Algorithms (SHA) o Cyclic Redundancy Check (CRC) per calcolare il valore di checksum:

- CRC-64/NVME (CRC64NVME)
- CRC-32 (CRC32)
- CRC-32C (CRC32C)
- SHA-1 (SHA1)
- SHA-256 (SHA256)
- MD5MD5 ()
- XXHash 64 () XXHASH64
- Hash XX (3) XXHASH3
- Hash XX (128) XXHASH128
- SHA-512 (SHA512)

Note

L'content-MD5intestazione è disponibile solo utilizzando l'ETag S3 per gli oggetti caricati in un caricamento (PUToperazione) di una singola parte che utilizza la crittografia. SSE-S3

Inoltre, puoi fornire un checksum per ogni richiesta utilizzando l'intestazione. Content-MD5

Quando si [carica un oggetto](#), si specifica l'algoritmo che si desidera utilizzare:

- Quando usi il Console di gestione AWS, scegli l'algoritmo di checksum che desideri utilizzare. È possibile specificare facoltativamente il valore di checksum dell'oggetto. Quando Amazon S3 riceve l'oggetto, calcola il checksum utilizzando l'algoritmo specificato. Se i due valori di checksum non corrispondono, Amazon S3 genera un errore.
- Quando si utilizza un SDK, tieni presente quanto segue:
 - Imposta il parametro `ChecksumAlgorithm` sull'algoritmo da utilizzare per Amazon S3. Se hai già un checksum precalcolato, passi il valore di checksum all'SDK e l' AWS SDK include il valore nella richiesta. Se non si trasmette un valore di checksum o non si specifica un algoritmo di checksum, l'SDK calcola automaticamente un valore di checksum per l'utente e lo include nella richiesta per garantire la protezione dell'integrità. Se il valore del checksum individuale non corrisponde al valore impostato dell'algoritmo di checksum, Amazon S3 respinge la richiesta con un errore `BadDigest`.
 - Se stai utilizzando un SDK aggiornato, l' AWS SDK sceglie un algoritmo di checksum per te. Tuttavia, è possibile ignorare questo algoritmo di checksum.
 - Se non specifichi un algoritmo di checksum e l'SDK inoltre non calcola un checksum per te, S3 sceglie automaticamente l'algoritmo di checksum (). CRC-64/NVME CRC64NVME
- Quando utilizzi la REST API, non utilizzare il parametro `x-amz-sdk-checksum-algorithm`. Utilizza invece una delle intestazioni specifiche dell'algoritmo (ad esempio, `x-amz-checksum-crc32`).

Per applicare uno di questi valori di checksum a oggetti già caricati su Amazon S3, è possibile copiare l'oggetto e specificare se si desidera utilizzare l'algoritmo di checksum esistente o uno nuovo. Se non si specifica un algoritmo, S3 utilizza l'algoritmo esistente. Se l'oggetto sorgente non ha un algoritmo di checksum o un valore di checksum specificato, Amazon S3 utilizza l'algoritmo per calcolare il valore di checksum per l'oggetto di CRC-64/NVME destinazione. È inoltre possibile specificare un algoritmo di checksum quando si copiano gli oggetti utilizzando le [Operazioni in batch S3](#).

Important

Se si utilizza un caricamento in più parti con Checksum per checksum compositi (o a livello di parte), i numeri di parte del caricamento in più parti devono essere consecutivi e iniziare con

1. Se si tenta di completare una richiesta di caricamento multiparte con numeri di parte non consecutivi, Amazon S3 genera un errore HTTP 500 Internal Server.

Tipi di checksum di oggetti completi e compositi

In Amazon S3, esistono due tipi di checksum supportati:

- **Checksum di oggetti completi:** un checksum dell'oggetto completo viene calcolato sulla base di tutto il contenuto di un caricamento multiparte, coprendo tutti i dati dal primo byte della prima parte all'ultimo byte dell'ultima parte. Tieni presente che se stai utilizzando Console di gestione AWS per caricare oggetti di dimensioni inferiori a 16 MB, è supportato solo il tipo di checksum completo degli oggetti.

Note

Gli oggetti caricati [PutObject](#) utilizzando il tipo di checksum completo degli oggetti. Non è necessario specificare un tipo di checksum.

- **Checksum compositi:** un checksum composito viene calcolato in base ai singoli checksum di ciascuna parte di un caricamento multiparte. Invece di calcolare un checksum basato su tutto il contenuto dei dati, questo approccio aggrega i checksum a livello di parte (dalla prima all'ultima parte) per produrre un singolo checksum combinato per l'oggetto completo. È possibile utilizzare il tipo di checksum composito solo con determinati algoritmi di checksum e solo quando si utilizza un caricamento in più parti per caricare l'oggetto. Per gli algoritmi che supportano ogni tipo di checksum, consulta la sezione. [Caricamenti in più parti](#)

Note

Quando un oggetto viene caricato come caricamento multiparte, il tag entità (ETag) per l'oggetto non è un digest MD5 dell'intero oggetto. Invece, Amazon S3 calcola il digest MD5 di ogni singola parte mentre viene caricata. I digest MD5 vengono utilizzati per determinare l'ETag dell'oggetto finale. Amazon S3 concatena i byte per i digest MD5 e quindi calcola il digest MD5 di questi valori concatenati. Durante la fase finale di creazione dell'ETag, Amazon S3 aggiunge un trattino con il numero totale di parti alla fine.

Caricamenti di una singola parte

I checksum degli oggetti caricati in una singola parte (usando il metodo [PutObject](#)) sono trattati come checksum completi dell'oggetto. Quando si carica un oggetto nella console di Amazon S3, è possibile scegliere l'algoritmo di checksum che si desidera che S3 utilizzi e anche (facoltativamente) fornire un valore precompilato. Amazon S3 convalida quindi il valore di checksum precalcolato prima di archiviare l'oggetto e il relativo valore di checksum. È possibile verificare l'integrità dei dati di un oggetto quando si richiede il valore di checksum durante il download degli oggetti.

Caricamenti in più parti

Quando si carica l'oggetto in più parti utilizzando l'API [MultipartUpload](#) è possibile specificare l'algoritmo di checksum che si desidera utilizzare su Amazon S3 e il tipo di checksum (oggetto completo o composito).

La tabella seguente indica quale tipo di algoritmo di checksum è supportato per ogni algoritmo di checksum in un caricamento multiparte:

Algoritmo di checksum	Oggetto completo	Composita
CRC-64/NVME (CRC64NVME)	Sì	No
CRC-32 (CRC32)	Sì	Sì
CRC-32C (CRC32C)	Sì	Sì
SHA-1 (SHA1)	No	Sì
SHA-256 (SHA256)	No	Sì
MD5 () MD5	No	Sì
XXHash 64 () XXHASH64	No	Sì
Hash XX (3) XXHASH3	No	Sì
Hash XX (128) XXHASH128	No	Sì
SHA-512 (SHA512)	No	Sì

Utilizzo di checksum completi degli oggetti per il caricamento multiparte

Quando si crea o si esegue un caricamento multiparte, è possibile utilizzare checksum completi degli oggetti per la convalida del caricamento. Ciò significa che è possibile fornire l'algoritmo di checksum per l'API [MultipartUpload](#) semplificando gli strumenti di validazione dell'integrità, perché non è più necessario tracciare vincoli di parti per oggetti caricati. È possibile fornire il checksum dell'intero oggetto nella richiesta [CompleteMultipartUpload](#) insieme alla dimensione dell'oggetto.

Quando fornisci un checksum completo dell'oggetto durante un caricamento in più parti, l'AWS SDK passa il checksum ad Amazon S3 e S3 convalida l'integrità dell'oggetto sul server, confrontandolo con il valore ricevuto. Quindi, Amazon S3 memorizza l'oggetto se i valori corrispondono. Se i due valori non coincidono, S3 respinge la richiesta con un errore `BadDigest`. Il checksum dell'oggetto viene memorizzato anche nei metadati dell'oggetto, che verranno utilizzati in seguito per convalidare l'integrità dei dati di un oggetto.

Per i checksum completi degli oggetti, puoi utilizzare gli algoritmi di checksum `()`, `()` o CRC-64/NVME (CRC64NVME) in S3 CRC-32. CRC32 CRC-32C CRC32C I checksum completi degli oggetti nei caricamenti multiparte sono disponibili solo per i checksum perché possono essere linearizzati in un CRC-based checksum completo dell'oggetto. Questa linearizzazione consente ad Amazon S3 di parallelizzare le richieste per migliorare le prestazioni. In particolare, S3 può calcolare il checksum dell'intero oggetto a partire dai checksum a livello di parte. Questo tipo di convalida non è disponibile per altri algoritmi, come SHA e MD5. Poiché S3 dispone di protezioni di integrità predefinite, se gli oggetti vengono caricati senza un checksum, S3 allega automaticamente all'oggetto l'algoritmo di checksum completo `()` consigliato. CRC-64/NVME CRC64NVME

Note

Per avviare il caricamento multiparte, è possibile specificare l'algoritmo di checksum e il tipo di checksum dell'oggetto completo. Dopo aver specificato l'algoritmo di checksum e il tipo di checksum dell'oggetto completo, è possibile fornire il valore di checksum dell'oggetto completo per il caricamento multiparte.

Important

Quando si utilizzano caricamenti in più parti con i nuovi algoritmi di checksum (MD5, xxHash3, xxHash64, xxHash128), è necessario specificare l'algoritmo di checksum nella richiesta utilizzando l'intestazione. SHA-512 `CreateMultipartUpload`

`x-amz-checksum-algorithm` Se fornisci un valore di checksum nella `CompleteMultipartUpload` richiesta (ad esempio `x-amz-checksum-sha512`) senza aver specificato l'algoritmo in, la richiesta avrà esito negativo e verrà generato un errore. `CreateMultipartUpload InvalidRequest`

Note

Per gli algoritmi di checksum esistenti (CRC32, CRC32C,, SHA-256), SHA-1 se l'algoritmo non è specificato in `CreateMultipartUpload`, qualsiasi intestazione di checksum fornita in `CompleteMultipartUpload` è attualmente accettata ma non convalidata o archiviata con l'oggetto. Consigliamo di specificare sempre l'algoritmo per garantire che i checksum siano convalidati e archiviati. `CreateMultipartUpload`

Utilizzo di checksum a livello di parte per il caricamento multiparte

Quando gli oggetti vengono caricati su Amazon S3, possono essere caricati come un singolo oggetto o in parti con il processo di caricamento multiparte. È possibile scegliere un tipo di checksum per il caricamento multiparte. Per i checksum a livello di parte di caricamento multiparte (o checksum compositi), Amazon S3 calcola il checksum per ogni singola parte utilizzando l'algoritmo di checksum specificato. È possibile utilizzare [UploadPart](#) per fornire i valori di checksum per ogni parte. Se l'oggetto che cerchi di caricare nella console Amazon S3 è impostato per utilizzare l'algoritmo di checksum CRC-64/NVME (CRC64NVME) e supera i 16 MB, viene automaticamente designato come checksum completo dell'oggetto.

Amazon S3 utilizza quindi i valori di checksum memorizzati a livello di parte per confermare che ogni parte è stata caricata correttamente. Quando viene fornito il checksum di ogni parte (per l'intero oggetto), S3 utilizza i valori di checksum memorizzati di ogni parte per calcolare internamente il checksum dell'intero oggetto, confrontandolo con il valore di checksum fornito. Questo riduce al minimo i costi di calcolo, poiché S3 può calcolare un checksum dell'intero oggetto utilizzando il checksum delle parti. Per ulteriori informazioni sui caricamenti multiparte, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#) e [Utilizzo di checksum completi degli oggetti per il caricamento multiparte](#).

Quando l'oggetto è stato completamente caricato, è possibile utilizzare il checksum finale calcolato per verificare l'integrità dei dati dell'oggetto.

Quando si carica una parte del caricamento multiparte, tieni presente quanto segue:

- Per recuperare informazioni sull'oggetto, compreso il numero di parti che compongono l'intero oggetto, si può usare l'operazione [GetObjectAttributes](#). Con i checksum aggiuntivi, è possibile recuperare anche le informazioni per ogni singolo componente, che includono il valore del checksum del componente.
- Per i caricamenti completati, è possibile ottenere la somma di controllo di una singola parte utilizzando i tasti [GetObject](#) o [HeadObject](#) e specificando un numero di parte o un intervallo di byte che corrisponde a una singola parte. Se si desidera recuperare i valori di checksum per le singole parti dei caricamenti multiparte che sono ancora in corso, si può usare [ListParts](#).
- A causa del modo in cui Amazon S3 calcola il checksum per gli oggetti in più parti, il valore del checksum dell'oggetto potrebbe cambiare se lo si copia. Se si utilizza un SDK o la REST API e si chiama [CopyObject](#), Amazon S3 copia qualsiasi oggetto fino alle limitazioni di dimensione dell'operazione dell'API CopyObject. Amazon S3 esegue questa copia come un'unica operazione, indipendentemente dal fatto che l'oggetto sia stato caricato in una singola richiesta o come parte di un caricamento in più parti. Con il comando copy, il checksum dell'oggetto è un checksum diretto dell'oggetto completo. Se l'oggetto è stato originariamente caricato con un caricamento multiparte, il valore del checksum cambia anche se i dati non cambiano.
- Gli oggetti di dimensioni superiori alle limitazioni di dimensione dell'operazione API CopyObject devono utilizzare [comandi di copia di caricamento multiparte](#).
- Quando esegui alcune operazioni utilizzando il Console di gestione AWS, Amazon S3 utilizza un caricamento in più parti se l'oggetto ha una dimensione superiore a 16 MB.

Metodi di checksum

Dopo aver caricato gli oggetti, è possibile ottenere il valore di checksum e confrontarlo con un valore di checksum precalcolato o precedentemente archiviato dello stesso tipo di algoritmo di checksum. Gli esempi seguenti mostrano quali metodi di calcolo del checksum si possono utilizzare per verificare l'integrità dei dati.

Utilizzo della console S3

Per ulteriori informazioni sull'utilizzo della console e sulla specifica degli algoritmi di checksum da utilizzare durante il caricamento degli oggetti, consultare [Caricamento degli oggetti](#) e [Tutorial: Verifica dell'integrità dei dati in Amazon S3 con checksum aggiuntivi](#).

Utilizzo di AWS SDK

L'esempio seguente mostra come è possibile utilizzare AWS gli SDK per caricare un file di grandi dimensioni con caricamento in più parti, scaricare un file di grandi dimensioni e convalidare un file caricato in più parti, il tutto utilizzando per la convalida dei file. SHA-256

Java

Example Esempio: caricamento, download e verifica di un file di grandi dimensioni con SHA-256

Per istruzioni su come creare e testare un campione funzionante, consulta [Getting Started](#) nella AWS SDK per Java Developer Guide.

```
import software.amazon.awssdk.auth.credentials.AwsCredentials;
import software.amazon.awssdk.auth.credentials.AwsCredentialsProvider;
import software.amazon.awssdk.core.ResponseInputStream;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.AbortMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.ChecksumMode;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.CompletedMultipartUpload;
import software.amazon.awssdk.services.s3.model.CompletedPart;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesRequest;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesResponse;
import software.amazon.awssdk.services.s3.model.GetObjectRequest;
import software.amazon.awssdk.services.s3.model.GetObjectResponse;
import software.amazon.awssdk.services.s3.model.GetObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.ObjectAttributes;
import software.amazon.awssdk.services.s3.model.PutObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.Tag;
import software.amazon.awssdk.services.s3.model.Tagging;
import software.amazon.awssdk.services.s3.model.UploadPartRequest;
import software.amazon.awssdk.services.s3.model.UploadPartResponse;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
```

```

import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.nio.ByteBuffer;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.Base64;
import java.util.List;

public class LargeObjectValidation {
    private static String FILE_NAME = "sample.file";
    private static String BUCKET = "sample-bucket";
    //Optional, if you want a method of storing the full multipart object
checksum in S3.
    private static String CHECKSUM_TAG_KEYNAME = "fullObjectChecksum";
    //If you have existing full-object checksums that you need to validate
against, you can do the full object validation on a sequential upload.
    private static String SHA256_FILE_BYTES = "htCM5g7ZNdoSw8bN/
mkgiAhXt5MFoVowVg+LE9aIQmI=";
    //Example Chunk Size - this must be greater than or equal to 5MB.
    private static int CHUNK_SIZE = 5 * 1024 * 1024;

    public static void main(String[] args) {
        S3Client s3Client = S3Client.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(new AwsCredentialsProvider() {
                @Override
                public AwsCredentials resolveCredentials() {
                    return new AwsCredentials() {
                        @Override
                        public String accessKeyId() {
                            return Constants.ACCESS_KEY;
                        }

                        @Override
                        public String secretAccessKey() {
                            return Constants.SECRET;
                        }
                    };
                }
            })
            .build();
        uploadLargeFileBracketedByChecksum(s3Client);
    }
}

```

```

        downloadLargeFileBracketedByChecksum(s3Client);
        validateExistingFileAgainstS3Checksum(s3Client);
    }

    public static void uploadLargeFileBracketedByChecksum(S3Client s3Client) {
        System.out.println("Starting uploading file validation");
        File file = new File(FILE_NAME);
        try (InputStream in = new FileInputStream(file)) {
            MessageDigest sha256 = MessageDigest.getInstance("SHA-256");
            CreateMultipartUploadRequest createMultipartUploadRequest =
CreateMultipartUploadRequest.builder()
                .bucket(BUCKET)
                .key(FILE_NAME)
                .checksumAlgorithm(ChecksumAlgorithm.SHA256)
                .build();
            CreateMultipartUploadResponse createdUpload =
s3Client.createMultipartUpload(createMultipartUploadRequest);
            List<CompletedPart> completedParts = new ArrayList<CompletedPart>();
            int partNumber = 1;
            byte[] buffer = new byte[CHUNK_SIZE];
            int read = in.read(buffer);
            while (read != -1) {
                UploadPartRequest uploadPartRequest =
UploadPartRequest.builder()

                .partNumber(partNumber).uploadId(createdUpload.uploadId()).key(FILE_NAME).bucket(BUCKET).ch
                    UploadPartResponse uploadedPart =
s3Client.uploadPart(uploadPartRequest,
RequestBody.fromByteBuffer(ByteBuffer.wrap(buffer, 0, read)));
                CompletedPart part =
CompletedPart.builder().partNumber(partNumber).checksumSHA256(uploadedPart.checksumSHA256())
                    completedParts.add(part);
                sha256.update(buffer, 0, read);
                read = in.read(buffer);
                partNumber++;
            }
            String fullObjectChecksum =
Base64.getEncoder().encodeToString(sha256.digest());
            if (!fullObjectChecksum.equals(SHA256_FILE_BYTES)) {
                //Because the SHA256 is uploaded after the part is uploaded; the
upload is bracketed and the full object can be fully validated.

s3Client.abortMultipartUpload(AbortMultipartUploadRequest.builder().bucket(BUCKET).key(FILE

```

```

        throw new IOException("Byte mismatch between stored checksum and
upload, do not proceed with upload and cleanup");
    }
    CompletedMultipartUpload completedMultipartUpload =
CompletedMultipartUpload.builder().parts(completedParts).build();
    CompleteMultipartUploadResponse completedUploadResponse =
s3Client.completeMultipartUpload(

CompleteMultipartUploadRequest.builder().bucket(BUCKET).key(FILE_NAME).uploadId(createdUploadId)
        .tag checksumTag =
Tag.builder().key(CHECKSUM_TAG_KEYNAME).value(fullObjectChecksum).build();
        //Optionally, if you need the full object checksum stored with the
file; you could add it as a tag after completion.

s3Client.putObjectTagging(PutObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).tags(checksumTag)
    } catch (IOException | NoSuchAlgorithmException e) {
        e.printStackTrace();
    }
    GetObjectAttributesResponse
        objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_NAME)
        .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
    System.out.println(objectAttributes.objectParts().parts());
    System.out.println(objectAttributes.checksum().checksumSHA256());
}

public static void downloadLargeFileBracketedByChecksum(S3Client s3Client) {
    System.out.println("Starting downloading file validation");
    File file = new File("DOWNLOADED_" + FILE_NAME);
    try (OutputStream out = new FileOutputStream(file)) {
        GetObjectAttributesResponse
            objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_NAME)
            .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
        //Optionally if you need the full object checksum, you can grab a
tag you added on the upload
        List<Tag> objectTags =
s3Client.getObjectTagging(GetObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).tags(objectTags)
        String fullObjectChecksum = null;
        for (Tag objectTag : objectTags) {
            if (objectTag.key().equals(CHECKSUM_TAG_KEYNAME)) {
                fullObjectChecksum = objectTag.value();
            }
        }
    }
}

```

```

        break;
    }
}
MessageDigest sha256FullObject =
MessageDigest.getInstance("SHA-256");
MessageDigest sha256ChecksumOfChecksums =
MessageDigest.getInstance("SHA-256");

//If you retrieve the object in parts, and set the ChecksumMode to
enabled, the SDK will automatically validate the part checksum
for (int partNumber = 1; partNumber <=
objectAttributes.objectParts().totalPartsCount(); partNumber++) {
    MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
    ResponseInputStream<GetObjectResponse> response =
s3Client.getObject(GetObjectRequest.builder().bucket(BUCKET).key(FILE_NAME).partNumber(part
GetObjectResponse getObjectResponse = response.response();
    byte[] buffer = new byte[CHUNK_SIZE];
    int read = response.read(buffer);
    while (read != -1) {
        out.write(buffer, 0, read);
        sha256FullObject.update(buffer, 0, read);
        sha256Part.update(buffer, 0, read);
        read = response.read(buffer);
    }
    byte[] sha256PartBytes = sha256Part.digest();
    sha256ChecksumOfChecksums.update(sha256PartBytes);
    //Optionally, you can do an additional manual validation again
the part checksum if needed in addition to the SDK check
    String base64PartChecksum =
Base64.getEncoder().encodeToString(sha256PartBytes);
    String base64PartChecksumFromObjectAttributes =
objectAttributes.objectParts().parts().get(partNumber - 1).checksumSHA256();
    if (!
base64PartChecksum.equals(getObjectResponse.checksumSHA256()) || !
base64PartChecksum.equals(base64PartChecksumFromObjectAttributes)) {
        throw new IOException("Part checksum didn't match for the
part");
    }
    System.out.println(partNumber + " " + base64PartChecksum);
}
//Before finalizing, do the final checksum validation.
String base64FullObject =
Base64.getEncoder().encodeToString(sha256FullObject.digest());

```



```

        String base64ChecksumOfChecksums =
Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
        if (fullObjectChecksum != null && !
fullObjectChecksum.equals(base64FullObject)) {
            throw new IOException("Failed checksum validation for full
object");
        }
        System.out.println(fullObjectChecksum);
        String base64ChecksumOfChecksumFromAttributes =
objectAttributes.checksum().checksumSHA256();
        if (base64ChecksumOfChecksumFromAttributes != null && !
base64ChecksumOfChecksums.equals(base64ChecksumOfChecksumFromAttributes)) {
            throw new IOException("Failed checksum validation for full
object checksum of checksums");
        }
        System.out.println(base64ChecksumOfChecksumFromAttributes);
        out.flush();
    } catch (IOException | NoSuchAlgorithmException e) {
        //Cleanup bad file
        file.delete();
        e.printStackTrace();
    }
}

public static void validateExistingFileAgainstS3Checksum(S3Client s3Client)
{
    System.out.println("Starting existing file validation");
    File file = new File("DOWNLOADED_" + FILE_NAME);
    GetObjectAttributesResponse
        objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
        .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
    try (InputStream in = new FileInputStream(file)) {
        MessageDigest sha256ChecksumOfChecksums =
MessageDigest.getInstance("SHA-256");
        MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
        byte[] buffer = new byte[CHUNK_SIZE];
        int currentPart = 0;
        int partBreak =
objectAttributes.objectParts().parts().get(currentPart).size();
        int totalRead = 0;
        int read = in.read(buffer);
        while (read != -1) {

```

```

        totalRead += read;
        if (totalRead >= partBreak) {
            int difference = totalRead - partBreak;
            byte[] partChecksum;
            if (totalRead != partBreak) {
                sha256Part.update(buffer, 0, read - difference);
                partChecksum = sha256Part.digest();
                sha256ChecksumOfChecksums.update(partChecksum);
                sha256Part.reset();
                sha256Part.update(buffer, read - difference,
difference);
            } else {
                sha256Part.update(buffer, 0, read);
                partChecksum = sha256Part.digest();
                sha256ChecksumOfChecksums.update(partChecksum);
                sha256Part.reset();
            }
            String base64PartChecksum =
Base64.getEncoder().encodeToString(partChecksum);
            if (!
base64PartChecksum.equals(objectAttributes.objectParts().parts().get(currentPart).checksumSH
{
                throw new IOException("Part checksum didn't match S3");
            }
            currentPart++;
            System.out.println(currentPart + " " + base64PartChecksum);
            if (currentPart <
objectAttributes.objectParts().totalPartsCount()) {
                partBreak +=
objectAttributes.objectParts().parts().get(currentPart - 1).size();
            }
        } else {
            sha256Part.update(buffer, 0, read);
        }
        read = in.read(buffer);
    }
    if (currentPart != objectAttributes.objectParts().totalPartsCount())
{
        currentPart++;
        byte[] partChecksum = sha256Part.digest();
        sha256ChecksumOfChecksums.update(partChecksum);
        String base64PartChecksum =
Base64.getEncoder().encodeToString(partChecksum);
        System.out.println(currentPart + " " + base64PartChecksum);
    }
}

```

```

    }

    String base64CalculatedChecksumOfChecksums =
Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
    System.out.println(base64CalculatedChecksumOfChecksums);
    System.out.println(objectAttributes.checksum().checksumSHA256());
    if (!
base64CalculatedChecksumOfChecksums.equals(objectAttributes.checksum().checksumSHA256()))
    {
        throw new IOException("Full object checksum of checksums don't
match S3");
    }

    } catch (IOException | NoSuchAlgorithmException e) {
        e.printStackTrace();
    }
}
}
}

```

Utilizzo della REST API

È possibile inviare richieste REST per caricare un oggetto con un valore di checksum con [PutObject](#) cui verificare l'integrità dei dati. È inoltre possibile recuperare il valore di checksum per gli oggetti utilizzando o. [GetObject](#) [HeadObject](#)

Utilizzo di AWS CLI

È possibile inviare una richiesta PUT per caricare un oggetto di un massimo di 5 GB in una singola operazione. Per ulteriori informazioni, consulta [PutObject](#) nella documentazione di riferimento dei comandi della AWS CLI . Puoi utilizzare anche [get-object](#) e [head-object](#) per recuperare il checksum di un oggetto già caricato per verificare l'integrità dei dati.

Per informazioni, consulta le [Domande frequenti sulla CLI di Amazon S3](#) nella Guida all'utente AWS Command Line Interface .

Utilizzo durante il Content-MD5 caricamento di oggetti

Un altro modo per verificare l'integrità dell'oggetto dopo il caricamento consiste nel fornire un digest MD5 dell'oggetto durante il caricamento. Se calcoli il digest MD5 dell'oggetto, puoi fornire il digest con il comando PUT utilizzando l'intestazione Content-MD5.

Dopo aver caricato l'oggetto, Amazon S3 calcola il digest MD5 dell'oggetto e lo confronta con il valore fornito. La richiesta ha esito positivo solo se i due digest corrispondono.

Non è obbligatorio fornire un digest MD5, ma è possibile utilizzarlo per verificare l'integrità dell'oggetto come parte del processo di caricamento.

Utilizzo Content-MD5 e ETag per verificare gli oggetti caricati

Il tag di entità (ETag) di un oggetto rappresenta una versione specifica di tale oggetto. Tieni presente che l'ETag riflette solo le modifiche al contenuto di un oggetto, non le modifiche ai suoi metadati. Se cambiano solo i metadati di un oggetto, l'ETag rimane invariato.

In base all'oggetto, l'ETag dell'oggetto potrebbe essere un digest MD5 dei dati dell'oggetto:

- Se un oggetto viene creato tramite, o CopyObject tramite PutObject PostObject Console di gestione AWS, e tale oggetto è anche in testo normale o crittografato mediante crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3), quell'oggetto ha un ETag che è un digest MD5 dei suoi dati oggetto.
- Se un oggetto viene creato dall'CopyObjectoperazione PutObjectPostObject, o o tramite il Console di gestione AWS, e tale oggetto è crittografato mediante crittografia lato server con chiavi fornite dal cliente (SSE-C) o crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS), quell'oggetto ha un ETag che non è un digest MD5 dei suoi dati oggetto.
- Se un oggetto viene creato dal processo di caricamento multiparte o dall'operazione UploadPartCopy, l'ETag dell'oggetto non è un digest MD5, indipendentemente dal metodo di crittografia. Se un oggetto è più grande di 16 MB, Console di gestione AWS carica o copia quell'oggetto come caricamento in più parti e quindi l'ETag non è un digest MD5.

Per gli oggetti in cui l'ETag è il digest Content-MD5 dell'oggetto, puoi confrontare il valore ETag dell'oggetto con un digest Content-MD5 calcolato o precedentemente archiviato.

Utilizzo dei checksum finali

Quando carichi oggetti di grandi dimensioni su Amazon S3, puoi fornire un checksum precalcolato per l'oggetto o utilizzare un AWS SDK per creare automaticamente i checksum finali per i caricamenti in blocchi, per tuo conto. Se utilizzi un checksum finale, Amazon S3 genera automaticamente il valore di checksum utilizzando l'algoritmo specificato per convalidare l'integrità dell'oggetto durante il caricamento in blocchi di un oggetto.

Per creare un checksum finale quando usi un SDK, compila il parametro con il tuo algoritmo preferito. AWS ChecksumAlgorithm SDK utilizza l'algoritmo per calcolare il valore di checksum dell'oggetto (o delle parti dell'oggetto) e lo aggiunge automaticamente alla fine della richiesta di caricamento in blocchi. Questo comportamento ti consente di risparmiare tempo perché Amazon S3 esegue sia la verifica che il caricamento dei tuoi dati in un unico passaggio.

 Important

Se utilizzi S3 Object Lambda, tutte le richieste a S3 Object Lambda vengono firmate tramite `s3-object-lambda` anziché `s3`. Questo comportamento influisce sulla firma dei valori di checksum finali. Per ulteriori informazioni su Lambda per oggetti S3, consulta [Trasformazione di oggetti con S3 Object Lambda](#).

Intestazioni di checksum finali

Per effettuare una richiesta di codifica del contenuto in blocchi, Amazon S3 richiede che i server client includano diverse intestazioni per analizzare correttamente la richiesta. I server client devono includere le intestazioni seguenti:

- **x-amz-decoded-content-length**: questa intestazione indica la dimensione in testo normale dei dati effettivi che vengono caricati su Amazon S3 con la richiesta.
- **x-amz-content-sha256**: questa intestazione indica il tipo di caricamento in blocchi incluso nella richiesta. Per i caricamenti in blocchi con checksum finali, il valore dell'intestazione è `STREAMING-UNSIGNED-PAYLOAD-TRAILER` per le richieste che non utilizzano la firma del payload e `STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER` per le richieste che utilizzano la firma del payload SigV4. Per ulteriori informazioni sull'implementazione dei payload firmati, consulta [Calcoli della firma per l'intestazione di autorizzazione: trasferimento di un payload in più blocchi](#).
- **x-amz-trailer**: questa intestazione indica il nome dell'intestazione finale nella richiesta. Se esistono checksum finali (dove gli AWS SDK aggiungono checksum ai corpi delle richieste codificati), il valore dell'intestazione include il prefisso e termina con il nome dell'`x-amz-trailer`algoritmo. `x-amz-checksum-` Attualmente sono supportati i seguenti valori `x-amz-trailer`:
 - `x-amz-checksum-crc32`
 - `x-amz-checksum-crc32c`
 - `x-amz-checksum-crc64nvme`

- `x-amz-checksum-sha1`
- `x-amz-checksum-sha256`

Note

Puoi anche includere nella richiesta l'intestazione `Content-Encoding`, con il valore in blocchi. Sebbene questa intestazione non sia obbligatoria, la sua specifica può ridurre i problemi del proxy HTTP durante la trasmissione di dati codificati. Se nella richiesta è presente un'altra intestazione `Content-Encoding` (come `gzip`), l'intestazione `Content-Encoding` include il valore in blocchi in un elenco di codifiche separate da virgole. Ad esempio, `Content-Encoding: aws-chunked, gzip`.

Parti in blocchi

Quando carichi un oggetto su Amazon S3 utilizzando la codifica in blocchi, la richiesta di caricamento include i seguenti tipi di blocchi (formattati nell'ordine elencato):

- Blocchi del corpo dell'oggetto: a una richiesta di caricamento in blocchi possono essere associati uno, più o zero blocchi del corpo.
- Blocchi di completamento: a una richiesta di caricamento in blocchi possono essere associati uno, più o zero blocchi del corpo.
- Blocchi finali: il checksum finale viene elencato dopo il blocco di completamento. È consentito un solo blocco finale.

Note

Ogni caricamento in blocchi deve terminare con un CRLF finale (ad esempio `\r\n`) per indicare la fine della richiesta.

Per esempi di formattazione in blocchi, consulta [Esempi: caricamenti in blocchi con checksum finali](#).

Blocchi del corpo dell'oggetto

I blocchi del corpo dell'oggetto sono i blocchi che contengono i dati effettivi dell'oggetto che vengono caricati su S3. Questi blocchi hanno vincoli di dimensione e formato coerenti.

Dimensione dei blocchi del corpo dell'oggetto

Questi blocchi devono contenere almeno 8.192 byte (o 8 KiB) di dati dell'oggetto, ad eccezione del blocco del corpo finale, che può essere più piccolo. Non esiste una dimensione massima esplicita dei blocchi, ma è necessario che tutti i blocchi siano inferiori alla dimensione massima di caricamento di 5 GB. Le dimensioni dei blocchi possono variare da un blocco all'altro in base all'implementazione del server client.

Formato dei blocchi del corpo dell'oggetto

I blocchi del corpo dell'oggetto iniziano con la codifica esadecimale del numero di byte nel blocco del corpo dell'oggetto, seguita da un CRLF (Carriage Return Line Feed, ritorno a capo con avanzamento riga), dai byte dell'oggetto per il blocco e da un altro CRLF.

Ad esempio:

```
hex-encoding-of-object-bytes-in-chunk\r\n  
chunk-object-bytes\r\n
```

Tuttavia, quando il blocco è firmato, il blocco del corpo dell'oggetto segue un formato diverso, in cui la firma viene aggiunta alla dimensione del blocco con un punto e virgola come delimitatore. Ad esempio:

```
hex-encoding-of-object-bytes-in-chunk;chunk-signature\r\n  
chunk-object-bytes\r\n
```

Per ulteriori informazioni sulla firma dei blocchi, vedi [Calcoli della firma per](#)

[l'Authorizationintestazione: trasferimento di un payload in più blocchi \(Signature versione 4\).AWS](#) Per ulteriori informazioni sulla formattazione dei blocchi, consulta [Chunked transfer encoding](#) sul sito web RFC Editor.

Blocchi di completamento

I blocchi di completamento devono essere il blocco finale del corpo dell'oggetto di ogni caricamento in blocchi. Il formato di un blocco di completamento è simile a quello del blocco del corpo, ma contiene sempre zero byte di dati dell'oggetto. Gli zero byte dei dati dell'oggetto indicano che tutti i dati sono stati caricati. I caricamenti in blocchi devono includere un blocco di completamento come blocco finale del corpo dell'oggetto, secondo un formato come il seguente:

```
0\r\n
```

Tuttavia, se la richiesta di codifica del contenuto utilizza la firma del payload, il formato è il seguente:

```
0;chunk-signature\r\n
```

Blocchi finali

I blocchi finali contengono il checksum calcolato per tutte le richieste di caricamento S3. I blocchi finali includono due campi: un campo con il nome dell'intestazione e un campo con il valore dell'intestazione. Il campo del nome dell'intestazione per una richiesta di caricamento deve corrispondere al valore passato nell'intestazione della richiesta `x-amz-trailer`. Ad esempio, se una richiesta contiene `x-amz-trailer: x-amz-checksum-crc32` e il blocco finale ha il nome dell'intestazione `x-amz-checksum-sha1`, la richiesta ha esito negativo. Il campo del valore nel blocco finale include una codifica in base64 del valore di checksum big-endian per l'oggetto. L'ordinamento big-endian archivia il byte di dati più significativo nell'indirizzo di memoria più basso e il byte meno significativo nell'indirizzo di memoria più alto. L'algoritmo utilizzato per calcolare questo checksum è lo stesso del suffisso per il nome dell'intestazione (ad esempio, `crc32`).

Formato del blocco finale

I blocchi finali utilizzano il seguente formato per le richieste di payload non firmate:

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\n\r\n\r\n
```

Per le richieste con [payload firmati SigV4](#), il blocco finale include una firma finale dopo il blocco finale.

```
trailer-checksum\n\r\n\r\ntrailer-signature\r\n
```

Puoi anche aggiungere il CRLF direttamente alla fine del valore di checksum in base64. Ad esempio:

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\r\n\r\n
```

Esempi: caricamenti in blocchi con checksum finali

Amazon S3 supporta i caricamenti in blocchi che utilizzano la codifica dei contenuti `aws-chunked` per le richieste `PutObject` e `UploadPart` con checksum finali.

Example 1 — Richiesta in blocchi non firmata con un checksum finale **PutObject** CRC-32

Di seguito è riportato un esempio di richiesta in blocchi con un checksum finale **PutObject**. CRC-32
In questo esempio, il client carica un oggetto da 17 KB in tre blocchi non firmati e aggiunge un blocco di checksum finale utilizzando l'intestazione. CRC-32 `x-amz-checksum-crc32`

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-UNSIGNED-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

2000\r\n                // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000\r\n                // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400\r\n                 // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0\r\n                  // Completion chunk
x-amz-checksum-crc32: YABb/g==\n\r\n\r\n\r\n // Trailer chunk (note optional \n
character)
\r\n                  // CRLF
```

Ecco un esempio di risposta:

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

Note

L'utilizzo dell'avanzamento riga `\n` alla fine del valore di checksum può variare tra i client.

Example 2 — SigV4-signed richiesta suddivisa in blocchi con un checksum finale (CRC32) **PutObject** CRC-32

Di seguito è riportato un esempio di richiesta in blocchi con un **PutObject** checksum finale. CRC-32
Questa richiesta utilizza la firma del payload SigV4. In questo esempio, il client carica un oggetto

da 17 KB in tre blocchi firmati. Oltre ai blocchi `object body`, vengono firmati anche `completion chunk` e `trailer chunk`.

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

authorization-code                                // SigV4 headers authorization

2000;chunk-signature=signature-value...\r\n // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000;chunk-signature\r\n // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400;chunk-signature\r\n // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0;chunk-signature\r\n // Completion chunk
x-amz-checksum-crc32: YABb/g==\n\r\n // Trailer chunk (note optional \n
character)
trailer-signature\r\n
\r\n // CRLF
```

Ecco un esempio di risposta:

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

Verifica dell'integrità degli oggetti per i dati a riposo in Amazon S3

Per verificare il contenuto dei set di dati archiviati in Amazon S3, l'operazione [Calcola il checksum](#) di Operazioni in batch S3 calcola i checksum dell'oggetto completo o composti per gli oggetti a riposo. L'operazione Calcola il checksum utilizza Operazioni in batch per calcolare in modo asincrono i valori di checksum per un gruppo di oggetti e genera automaticamente un report di integrità consolidato, senza creare nuove copie dei dati oppure ripristinare o scaricare dati.

Con l'operazione Calcola il checksum, puoi verificare in modo efficiente miliardi di oggetti con una singola richiesta di processo. Per ogni richiesta di processo Calcola il checksum, S3 calcola i valori di checksum e li include in un report di integrità generato automaticamente (noto anche come report di

completamento). È quindi possibile utilizzare il report di completamento per convalidare l'integrità del set di dati.

L'operazione Calcola il checksum funziona con qualsiasi oggetto archiviato in S3, indipendentemente dalla classe di archiviazione o dalla dimensione dell'oggetto. Che sia necessario verificare gli oggetti come best practice di conservazione dei dati o soddisfare i requisiti di conformità, l'operazione Calcola il checksum riduce i costi, i tempi e le attività necessari per la convalida dei dati eseguendo calcoli di checksum a riposo. Per informazioni sui prezzi di Calcola il checksum, consulta la scheda Gestione e approfondimenti in [Prezzi di Amazon S3](#).

Quindi, puoi utilizzare l'output del report di completamento generato per confrontarlo con i valori di checksum archiviati nei database per verificare che i set di dati rimangano intatti nel tempo. Questo approccio consente di mantenere l'integrità dei dati end-to-end per le esigenze aziendali e di conformità. Ad esempio, puoi utilizzare l'operazione Calcola il checksum per inviare un elenco di oggetti archiviati nelle classi di archiviazione S3 Glacier per i controlli di sicurezza annuali. Inoltre, la gamma di algoritmi di checksum supportati consente di mantenere la continuità con gli algoritmi utilizzati nelle applicazioni.

Utilizzo di algoritmi di checksum supportati

Per i dati a riposo, è possibile calcolare i checksum utilizzando uno qualsiasi degli algoritmi di checksum supportati:

Tutti gli algoritmi di checksum supportati supportano sia il tipo di checksum completo che quello composito, tranne CRC-64/NVME (CRC64NVME), che supporta solo il tipo di checksum a oggetto completo.

- CRC-64/NVME (CRC64NVME)
- CRC-32 (CRC32)
- CRC-32C (CRC32C)
- SHA-1 (SHA1)
- SHA-256 (SHA256)
- MD5MD5 ()
- XXHash 64 () XXHASH64
- Hash XX (3) XXHASH3
- Hash XX (128) XXHASH128
- SHA-512 (SHA512)

Utilizzo Calcola il checksum

Per gli oggetti archiviati in Amazon S3, puoi utilizzare l'operazione Calcola il checksum con Operazioni in batch S3 per controllare il contenuto dei dati a riposo archiviati. Puoi [creare un processo Compute checksum Batch Operations](#) utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST o l'SDK. AWS Al termine del processo Calcola il checksum, si riceve un report di completamento. Per ulteriori informazioni su come utilizzare il report di completamento, consulta [Monitoraggio dei rapporti sullo stato e sul completamento dei processi](#).

Prima di creare il tuo job Compute checksum, devi creare un ruolo S3 Batch Operations AWS Identity and Access Management (IAM) per concedere ad Amazon S3 le autorizzazioni per eseguire azioni per tuo conto. È necessario fornire le autorizzazioni per leggere il file manifesto e scrivere un report di completamento nel bucket S3. Per ulteriori informazioni, consulta [Calcolo dei checksum](#).

Utilizzo della console S3

Per utilizzare nuovamente il plugin Checksum di calcolo operation

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Scegli la Regione in cui creare il processo.

Note

Per le operazioni di copia, è necessario creare il processo nella stessa Regione del bucket di destinazione. Per tutte le altre operazioni, è necessario creare il processo nella stessa Regione degli oggetti del manifesto.

3. Scegli Operazioni in batch nel pannello di navigazione sinistro della console Amazon S3.
4. Scegli Crea processo.
5. Visualizza Regione AWS dove vuoi creare il tuo lavoro.

Note

Per le operazioni di copia, è necessario creare il processo nella stessa Regione del bucket di destinazione. Per tutte le altre operazioni, è necessario creare il processo nella stessa Regione degli oggetti del manifesto.

6. In Formato manifest scegliere il tipo di oggetto manifest da usare.
 - Se scegli Report di inventario S3 (manifest.json), inserisci il percorso dell'oggetto `manifest.json` e (facoltativamente) l'ID versione dell'oggetto manifesto se desideri utilizzare una versione dell'oggetto specifica. In alternativa, puoi scegliere Sfoglia S3 e scegliere il file JSON manifesto, che popola automaticamente tutte le voci del campo dell'oggetto manifesto.
 - Se scegli CSV, scegli il tipo di posizione del manifesto, quindi inserisci il percorso di un oggetto CSV-formatted manifesto o scegli Sfoglia S3 per selezionare un oggetto manifesto. L'oggetto manifest deve avere il formato descritto nella console. Per utilizzare una versione specifica dell'oggetto manifesto, è anche possibile specificare l'ID versione dell'oggetto.
 - Se scegli Crea manifesto utilizzando la configurazione di replica S3, verrà generato un elenco di oggetti utilizzando la configurazione di replica e facoltativamente salvato nella destinazione scelta. Quando si utilizza una configurazione di replica per generare il manifesto, l'unica operazione disponibile è Replica.
7. Scegli Avanti.
8. In Operazione, scegli l'operazione Calcola il checksum per calcolare i checksum su tutti gli oggetti elencati nel manifesto. Scegli il Tipo di checksum e la Funzione di checksum per il processo. Quindi, seleziona Successivo.
9. Inserisci le informazioni per Configura opzioni aggiuntive, quindi scegli Successivo.
10. Nella pagina Configura opzioni aggiuntive, inserisci le informazioni relative al processo Calcola il checksum.

 Note

Nella sezione Report di completamento, assicurati di confermare la dichiarazione di conferma. Questa dichiarazione conferma che hai compreso che il report di completamento contiene valori di checksum, che vengono utilizzati per verificare l'integrità dei dati archiviati in Amazon S3. Pertanto, il report di completamento deve essere condiviso con cautela. Inoltre, tieni presente che se stai creando una richiesta di checksum Compute e specifichi la posizione del bucket del proprietario di un account esterno in cui archiviare il rapporto di completamento, assicurati di specificare l' Account AWS ID del proprietario del bucket esterno.

11. Scegli Avanti.
12. Nella pagina Esamina, verifica e conferma le impostazioni.

13. (Facoltativo) Per apportare modifiche, scegli Precedente per tornare alla pagina precedente o scegli Modifica per aggiornare una fase specifica.
14. Dopo aver confermato le modifiche, scegli Crea processo.

Per elencare e monitorare lo stato di avanzamento di tutti Calcola il checksum richieste

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Operazioni in batch.
3. Nella pagina Operazioni in batch, è possibile esaminare i dettagli del processo come la priorità del processo, la percentuale di completamento del processo e gli oggetti totali.
4. Se desideri gestire o clonare un job Compute checksum specifico, scegli il Job ID per visualizzare ulteriori informazioni sul lavoro.
5. Nella pagina dello specifico processo Calcola il checksum, esamina i dettagli del processo.

Ogni processo di operazione in batch passa attraverso diversi [stati di processo](#). È anche possibile [abilitare gli eventi AWS CloudTrail](#) nella console S3 per ricevere avvisi su qualsiasi modifica dello stato del processo. Per i processi attivi, puoi esaminare il processo in esecuzione e la percentuale di completamento nella pagina dei Dettagli processo.

Utilizzo di AWS SDK

Java

Example Esempio: creazione di un Calcola il checksum job

L'esempio seguente mostra come creare un processo Calcola il checksum (come parte di una richiesta Crea processo) e come specificare un manifesto:

```
// Required parameters
String accountId = "111122223333";
String roleArn = "arn:aws:iam::111122223333:role/BatchOperations";
String manifestArn = "arn:aws:s3:::my_manifests/manifest.csv";
String manifestEtag = "60e460c9d1046e73f7dde5043ac3ae85";
String reportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-bucket";
String reportExpectedBucketOwner = "111122223333";
String reportPrefix = "demo-report";

// Job Operation
```

```
S3ComputeObjectChecksumOperation s3ComputeObjectChecksum =
    S3ComputeObjectChecksumOperation.builder()
        .checksumAlgorithm(ComputeObjectChecksumAlgorithm.CRC64)
        .checksumType(ComputeObjectChecksumType.COMPOSITE)
        .build();

JobOperation operation = JobOperation.builder()
    .s3ComputeObjectChecksum(s3ComputeObjectChecksum)
    .build();

// Job Manifest
JobManifestLocation location = JobManifestLocation.builder()
    .eTag(manifestEtag)
    .objectArn(manifestArn)
    .build();

JobManifestSpec spec = JobManifestSpec.builder()
    .format(JobManifestFormat.S3_BATCH_OPERATIONS_CSV_20180820)
    .fields(Arrays.asList(JobManifestFieldName.BUCKET, JobManifestFieldName.KEY))
    .build();

JobManifest manifest = JobManifest.builder()
    .location(location)
    .spec(spec)
    .build();

// Completion Report
JobReport report = JobReport.builder()
    .bucket(reportBucketArn)
    .enabled(true) // Must be true
    .expectedBucketOwner(reportExpectedBucketOwner)
    .format(JobReportFormat.REPORT_CSV_20180820)
    .prefix(reportPrefix)
    .reportScope(JobReportScope.ALL_TASKS)
    .build();

// Create Job Request
CreateJobRequest request = CreateJobRequest.builder()
    .accountId(accountId)
    .confirmationRequired(false)
    .manifest(manifest)
    .operation(operation)
    .priority(10)
    .report(report)
```

```

        .roleArn(roleArn);

// Create the client
S3ControlClient client = S3ControlClient.builder()
    .credentialsProvider(new ProfileCredentialsProvider())
    .region(Region.US_EAST_1)
    .build();

// Send the request
try {
    CreateJobResponse response = client.createJob(request);
    System.out.println(response);
} catch (AwsServiceException e) {
    System.out.println("AwsServiceException: " + e.getMessage());
    throw new RuntimeException(e);
} catch (SdkClientException e) {
    System.out.println("SdkClientException: " + e.getMessage());
    throw new RuntimeException(e);
}

```

Example Esempio: visualizzazione Calcola il checksum dettagli del processo

L'esempio seguente mostra come specificare un ID di processo per visualizzare i dettagli del processo (come la percentuale di completamento del processo) per una richiesta di processo Calcola il checksum:

```

DescribeJobRequest request = DescribeJobRequest.builder()
    .accountId("1234567890")
    .jobId("a16217a1-e082-48e5-b04f-31fac3a66b13")
    .build();

```

Utilizzo di AWS CLI

È possibile utilizzare il comando [create-job](#) per creare un nuovo processo di operazioni in batch e fornire l'elenco di oggetti. Quindi, specifica l'algoritmo di checksum e il tipo di checksum, nonché il bucket di destinazione in cui desideri salvare il report Calcola il checksum. L'esempio seguente crea un processo di checksum S3 Batch Operations Compute utilizzando un manifest generato da S3 per Account AWS **111122223333**

Per utilizzare questo comando, sostituisci il *user input placeholders* con le tue informazioni:


```
aws s3control create-job \
  --account-id 111122223333 \
  --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3::my-manifest-bucket/
manifest.csv","ETag":"e0e8bfc50e0f0c5d5a1a5f0e0e8bfc50"}}' \
  --manifest-generator '{
    "S3JobManifestGenerator": {
      "ExpectedBucketOwner": "111122223333",
      "SourceBucket": "arn:aws:s3::amzn-s3-demo-source-bucket",
      "EnableManifestOutput": true,
      "ManifestOutputLocation": {
        "ExpectedManifestBucketOwner": "111122223333",
        "Bucket": "arn:aws:s3::amzn-s3-demo-manifest-bucket",
        "ManifestPrefix": "prefix",
        "ManifestFormat": "S3InventoryReport_CSV_20211130"
      },
      "Filter": {
        "CreatedAfter": "2023-09-01",
        "CreatedBefore": "2023-10-01",
        "KeyNameConstraint": {
          "MatchAnyPrefix": [
            "prefix"
          ],
          "MatchAnySuffix": [
            "suffix"
          ]
        },
        "ObjectSizeGreaterThanOrEqualToBytes": 100,
        "ObjectSizeLessThanBytes": 200,
        "MatchAnyStorageClass": [
          "STANDARD",
          "STANDARD_IA"
        ]
      }
    }
  }' \
  --operation '{"S3ComputeObjectChecksum":
{"ChecksumAlgorithm":"CRC64NVME","ChecksumType":"FULL_OBJECT"}}' \
  --report '{"Bucket":"arn:aws:s3::my-report-
bucket","Format":"Report_CSV_20180820","Enabled":true,"Prefix":"batch-op-
reports/","ReportScope":"AllTasks","ExpectedBucketOwner":"111122223333"}' \
  --priority 10 \
  --role-arn arn:aws:iam::123456789012:role/S3BatchJobRole \
```

```
--client-request-token 6e023a7e-4820-4654-8c81-7247361aeb73 \  
--description "Compute object checksums" \  
--region us-west-2
```

Dopo aver inviato il processo Calcola il checksum, ricevi l'ID del processo come risposta e viene visualizzato nella pagina elenco Operazioni in batch S3. Amazon S3 elabora l'elenco di oggetti e calcola i checksum per ogni oggetto. Al termine del processo, S3 fornisce un report Calcola il checksum consolidato nella destinazione specificata.

Per monitorare l'avanzamento del processo Calcola il checksum, utilizza il comando [describe-job](#). Questo comando controlla lo stato del processo di operazioni in batch specificato. Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

Ad esempio:

```
aws s3control describe-job --account-id 111122223333 --job-id 1234567890abcdef0
```

Per [ottenere un elenco](#) di tutti i processi di operazioni in batch attivi e completi, consulta [Elenco di processi](#) o [list-jobs](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile inviare richieste REST per verificare l'integrità degli oggetti con Compute checksum utilizzando. [CreateJob](#) È possibile monitorare l'avanzamento delle richieste di checksum di Compute inviando richieste REST all'operazione API. [DescribeJob](#) Ogni processo di operazioni in batch passa attraverso i seguenti stati:

- NUOVO
- IN PREPARAZIONE
- PRONTO
- ACTIVE
- PAUSA IN CORSO
- IN PAUSA
- COMPLETO
- ANNULLAMENTO
- Non riuscito

La risposta dell'API ti comunica lo stato corrente del processo.

Eliminazione di oggetti Amazon S3

Puoi eliminare uno o più oggetti direttamente da Amazon S3 utilizzando la console Amazon S3, gli AWS SDK, AWS Command Line Interface (AWS CLI) o l'API REST. Se ad esempio stai eseguendo la raccolta di file di log, è una buona idea eliminarli quando non sono più necessari. È possibile [impostare una regola del ciclo di vita S3](#) per eliminare automaticamente oggetti come i file di log.

Per eliminare un oggetto, è possibile utilizzare una delle seguenti operazioni API:

- Elimina un singolo oggetto: Amazon S3 fornisce l'API DELETE (`DeleteObject`) che consente di eliminare un solo oggetto con una singola richiesta HTTP.
- Elimina più oggetti: Amazon S3 fornisce l'operazione API Multi-Object Delete (`DeleteObjects`) che puoi utilizzare per eliminare fino a 1.000 oggetti in una singola richiesta HTTP.

Quando si eliminano oggetti da un bucket per cui non è abilitato il controllo delle versioni, si fornisce solo il nome della chiave dell'oggetto. Tuttavia, quando si eliminano oggetti da un bucket per cui è abilitato il controllo delle versioni, è possibile fornire l'ID della versione dell'oggetto per eliminare una versione specifica dell'oggetto.

Best practice da considerare prima di eliminare un oggetto

Prima di eliminare un oggetto, considera le seguenti best practice:

- Abilita il [controllo delle versioni per il bucket](#). La funzionalità di [controllo delle versioni S3](#) aggiunge una protezione contro le semplici richieste `DeleteObject` per evitare cancellazioni accidentali. Per i bucket con controllo delle versioni, se si elimina la versione corrente di un oggetto o se una richiesta di eliminazione non specifica un ID di versione specifico, Amazon S3 non elimina definitivamente l'oggetto. Al contrario, S3 aggiunge un marcatore di cancellazione, emettendo una cancellazione rapida dell'oggetto. Il marcatore di cancellazione diventa quindi la versione corrente (o più recente) dell'oggetto con un nuovo ID di versione. Per ulteriori informazioni, consulta [Deleting object versions from a versioning-enabled bucket](#).
- Se desideri eliminare un gran numero di oggetti o eliminare programmaticamente gli oggetti in base alla data di creazione dell'oggetto, [imposta una configurazione del ciclo di vita S3 sul bucket](#). Per monitorare queste cancellazioni, si consiglia di [utilizzare una notifica di evento del ciclo di vita S3](#). Quando si configurano le notifiche del ciclo di vita S3, il tipo di evento

`s3:LifecycleExpiration:Delete` notifica l'eliminazione di un oggetto in un bucket. Notifica inoltre quando una versione dell'oggetto viene eliminata definitivamente da una configurazione del ciclo di vita S3. Il tipo di evento `s3:LifecycleExpiration:DeleteMarkerCreated` notifica quando il ciclo di vita S3 crea un marcatore di cancellazione. Un marcatore di cancellazione viene creato quando viene eliminata la versione corrente di un oggetto in un bucket con controllo delle versioni.

- Prima di effettuare qualsiasi aggiornamento alla configurazione del ciclo di vita S3, verifica che il ciclo di vita abbia completato le azioni su tutti gli oggetti previsti. Per ulteriori informazioni, consulta la sezione [Aggiornamento, disattivazione o eliminazione delle regole del ciclo di vita in Impostazione della configurazione del ciclo di vita S3 su un bucket](#).

Note

Le regole del ciclo di vita S3 devono essere applicate al giusto sottoinsieme di oggetti per evitare cancellazioni involontarie. È possibile filtrare gli oggetti in base ai prefissi, ai tag degli oggetti o alle dimensioni degli oggetti quando si creano le regole del ciclo di vita.

- Considera la possibilità di limitare la rimozione o l'eliminazione di oggetti dal bucket da parte degli utenti. Per limitare gli utenti, è necessario negare esplicitamente agli utenti le autorizzazioni per le seguenti azioni nelle [policy del bucket Amazon S3](#):
 - `s3:DeleteObject`, `s3:DeleteObjectVersion` (per controllare chi può cancellare gli oggetti utilizzando le richieste API)
 - `s3:PutLifecycleConfiguration` (per controllare chi può aggiungere regole di scadenza del ciclo di vita S3)
- Considera l'utilizzo di [Replica S3](#) per creare più copie dei dati e replicarli in più posizioni contemporaneamente. È possibile scegliere tutti i bucket di destinazione necessari. Inoltre, se un oggetto viene involontariamente cancellato, si avrà ancora una copia dei dati.
- Evita di inviare gli ID di versione degli oggetti a bucket senza versione. Inoltre, assicurati di impostare correttamente le `s3:DeleteObjectVersion` autorizzazioni `s3:DeleteObject` e su tutti i bucket (inclusi i bucket senza versione).

Eliminazione di oggetti da un bucket con controllo delle versioni abilitato

Se per il bucket è abilitato il controllo delle versioni, nel bucket stesso possono esistere più versioni dello stesso oggetto. Quando si lavora con i bucket per cui è abilitato il controllo delle versioni, le operazioni API `Delete` consentono le seguenti opzioni:

- Specifica una richiesta di eliminazione senza versione: specifichi solo la chiave dell'oggetto senza l'ID versione. In questo caso, Amazon S3 crea un marcatore di cancellazione sulla versione corrente dell'oggetto e restituisce l'ID della versione nella risposta. L'oggetto scompare dal bucket. Per informazioni sulla funzione Controllo delle versioni degli oggetti e sul concetto di contrassegno di eliminazione, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).
- Specifica una richiesta di cancellazione con controllo delle versioni - Specifica sia la chiave che l'ID della versione. In questo caso, sono possibili i seguenti risultati:
 - Se l'ID versione mappa a una versione dell'oggetto specifica, Amazon S3 elimina la versione specifica dell'oggetto.
 - Se l'ID della versione corrisponde al marcatore di cancellazione di un oggetto, Amazon S3 elimina il marcatore di cancellazione. Quando il marcatore di cancellazione viene eliminato, l'oggetto riappare nel bucket.

Eliminazione di oggetti da un bucket con controllo delle versioni sospeso

Se per un bucket è sospeso il controllo delle versioni, le operazioni API Delete si comportano allo stesso modo per i bucket con controllo delle versioni abilitato (tranne quando la versione corrente ha un ID versione null). Per ulteriori informazioni, consulta [Eliminazione di oggetti da bucket con funzione Controllo delle versioni sospesa](#).

Eliminazione di oggetti da un bucket senza controllo delle versioni

Se il bucket è senza controllo delle versioni, è possibile specificare la chiave dell'oggetto nelle operazioni API Delete e Amazon S3 eliminerà definitivamente l'oggetto. Per evitare la cancellazione permanente di un oggetto, [abilita il controllo delle versioni per il bucket](#).

Per i bucket senza versione, se le `s3:DeleteObjectVersion` autorizzazioni `s3:DeleteObject` o sono esplicitamente negate nella tua policy sui bucket, qualsiasi richiesta o genera un errore. `DeleteObject DeleteObjects DeleteObjectVersion 403 Access Denied`

MFA-enabled Eliminazione di oggetti da un bucket

Quando si eliminano oggetti da un bucket abilitato per l'autenticazione a più fattori (multi-factor authentication, MFA), tieni presente quanto segue:

- Se specifichi un token MFA non valido, la richiesta ha sempre esito negativo.

- Se si dispone di un MFA-enabled bucket e si effettua una richiesta di eliminazione con versione (si forniscono una chiave oggetto e un ID di versione), la richiesta non riesce se non si fornisce un token MFA valido. Inoltre, quando si utilizza l'operazione Delete API multioggetto su un MFA-enabled bucket, se una delle eliminazioni è una richiesta di eliminazione con versione (ovvero, si specifica una chiave oggetto e un ID di versione), l'intera richiesta ha esito negativo se non si fornisce un token MFA.

La richiesta ha invece esito positivo nei seguenti casi:

- Se disponi di un MFA-enabled bucket e fai una richiesta di eliminazione senza versione (non stai eliminando un oggetto con versione) e non fornisci un token MFA, l'eliminazione ha esito positivo.
- Se hai una richiesta di Multi-Object eliminazione che specifica solo oggetti senza versione da eliminare da un MFA-enabled bucket e non fornisci un token MFA, le eliminazioni hanno esito positivo.

Per informazioni sull'eliminazione di MFA, consulta [Configurazione dell'eliminazione di MFA](#).

Argomenti

- [Eliminazione di un singolo oggetto](#)
- [Eliminazione di più oggetti](#)

Eliminazione di un singolo oggetto

Puoi utilizzare la console di Amazon S3 o l'API DELETE per eliminare un singolo oggetto esistente da un bucket S3. Per ulteriori informazioni su come eliminare gli oggetti in Amazon S3, consulta [Eliminazione di oggetti Amazon S3](#).

Tutti gli oggetti nel bucket S3 sono soggetti a costi di storage. È pertanto necessario eliminare quelli di cui non si ha più bisogno. Se ad esempio si esegue la raccolta di file di log, è una buona idea eliminarli quando non sono più necessari. È possibile impostare una regola del ciclo di vita per eliminare automaticamente oggetti come i file di log. Per ulteriori informazioni, consulta [the section called “Impostazione della configurazione del ciclo di vita”](#).

Per informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

Utilizzo della console S3

Segui questi passaggi per utilizzare la console di Amazon S3 per eliminare un singolo oggetto da un bucket.

Warning

Quando si elimina definitivamente un oggetto o una versione specifica di un oggetto nella console Amazon S3, l'eliminazione non può essere annullata.

Per eliminare un oggetto con controllo delle versioni abilitato o sospeso

Note

Se l'ID della versione di un oggetto in un bucket con controllo delle versioni sospeso è contrassegnato come NULL, S3 elimina definitivamente l'oggetto poiché non esistono versioni precedenti. Tuttavia, se viene elencato un ID di versione valido per l'oggetto in un bucket con controllo delle versioni sospeso, S3 crea un marcatore di cancellazione per l'oggetto eliminato, mantenendo le versioni precedenti dell'oggetto.

1. Accedi e apri la console Amazon S3 all' Console di gestione AWS indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.
3. Nell'elenco dei bucket scegli il nome del bucket dal quale desideri eliminare un oggetto.
4. Seleziona l'oggetto e scegli Elimina.
5. Per confermare l'eliminazione dell'elenco degli oggetti in Oggetti specificati, nella casella di testo Eliminare gli oggetti? immetti **delete**.

Per eliminare definitivamente una versione specifica dell'oggetto in un bucket con controllo delle versioni abilitato

Warning

Quando si elimina definitivamente una versione specifica di un oggetto in Amazon S3, l'eliminazione non può essere annullata.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket name (Nome bucket) scegliere il nome del bucket dal quale si desidera eliminare un oggetto.
3. Seleziona l'oggetto da eliminare.
4. Scegli il pulsante Mostra versioni.
5. Seleziona la versione dell'oggetto e scegli Elimina.
6. Per confermare l'eliminazione permanente delle versioni specifiche degli oggetti elencati in Oggetti specificati, nella casella di testo Eliminare gli oggetti? immetti Elimina definitivamente. Amazon S3 elimina definitivamente la versione specifica dell'oggetto.

Per eliminare definitivamente un oggetto in un bucket Amazon S3 non ha il controllo delle versioni abilitato

 Warning

Quando si elimina definitivamente un oggetto in Amazon S3, l'eliminazione non può essere annullata. Inoltre, per tutti i bucket che non hanno il controllo delle versioni abilitato, le cancellazioni sono permanenti.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket dal quale desideri eliminare un oggetto.
4. Seleziona l'oggetto e scegli Elimina.
5. Per confermare l'eliminazione definitiva dell'oggetto elencato in Oggetti specificati, nella casella di testo Eliminare gli oggetti? immetti Elimina definitivamente.

 Note

Se si verificano problemi con l'eliminazione dell'oggetto, consulta [Voglio eliminare definitivamente gli oggetti con il controllo delle versioni abilitato](#).

Utilizzo di AWS CLI

Per eliminare un oggetto per richiesta, utilizza l'API DELETE. Per ulteriori informazioni, consulta [DELETE Object](#). Per ulteriori informazioni sull'utilizzo della CLI per eliminare un oggetto, consulta la sezione [delete-object](#).

Utilizzo di REST API

Puoi utilizzare gli AWS SDK per eliminare un oggetto. Tuttavia, se l'applicazione lo richiede, è possibile inviare richieste REST direttamente. Per ulteriori informazioni, consulta [DELETE Object](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di AWS SDK

Gli esempi seguenti mostrano come utilizzare gli AWS SDK per eliminare un oggetto da un bucket. Per ulteriori informazioni, consulta [DELETE Object](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Se hai la funzione Controllo delle versioni S3 abilitata sul bucket, sono disponibili le seguenti opzioni:

- Eliminazione di una versione specifica di un oggetto specificando un ID versione.
- Elimina un oggetto senza specificare l'ID versione, nel cui caso Amazon S3 aggiunge un contrassegno di eliminazione all'oggetto.

Per ulteriori informazioni sulla funzionalità Controllo delle versioni S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Per altri esempi ed esempi in altre lingue, consulta [Use DeleteObject with an AWS SDK o CLI](#) nel riferimento alle API Amazon S3.

Java

Per eliminare oggetti utilizzando l' AWS SDK per Java, puoi eliminare oggetti da bucket con versione e senza versione:

- Non-versioned bucket: nella richiesta di eliminazione, si specifica solo la chiave dell'oggetto e non un ID di versione.
- Bucket con controllo delle versioni: elimina una specifica versione dell'oggetto, indicando il nome della chiave dell'oggetto e l'ID versione. Se non sono disponibili altre versioni dell'oggetto,

Amazon S3 elimina l'oggetto interamente. In caso contrario, Amazon S3 elimina solo la versione specificata.

 Note

È possibile ottenere gli ID versione di un oggetto inviando una richiesta `ListVersions`.

Per esempi di come eliminare un singolo oggetto con l' AWS SDK per Java, consulta [Eliminare un oggetto](#) nell'API Reference di Amazon S3.

.NET

Gli esempi seguenti mostrano come eliminare un oggetto sia da bucket con versione sia da bucket senza versione. Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Example Eliminazione di un oggetto da un bucket senza versione

Nell'esempio di codice C# seguente viene eliminato un oggetto da un bucket senza versione. L'esempio presuppone che gli oggetti non dispongano degli ID versione, perciò non vengono specificati gli ID versione. Specifichi solo la chiave dell'oggetto.

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class DeleteObjectNonVersionedBucketTest
    {
        private const string bucketName = "**** bucket name ****";
        private const string keyName = "**** object key ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
            RegionEndpoint.USWest2;
    }
}
```

```

private static IAmazonS3 client;

public static void Main()
{
    client = new AmazonS3Client(bucketRegion);
    DeleteObjectNonVersionedBucketAsync().Wait();
}
private static async Task DeleteObjectNonVersionedBucketAsync()
{
    try
    {
        var deleteObjectRequest = new DeleteObjectRequest
        {
            BucketName = bucketName,
            Key = keyName
        };

        Console.WriteLine("Deleting an object");
        await client.DeleteObjectAsync(deleteObjectRequest);
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered on server. Message:'{0}' when
deleting an object", e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when
deleting an object", e.Message);
    }
}
}
}

```

Example Eliminazione di un oggetto da un bucket con versione

Nell'esempio C# seguente viene eliminato un oggetto da un bucket con versione. Elimina una specifica versione dell'oggetto, specificando il nome della chiave dell'oggetto e l'ID versione.

Il codice esegue le attività sotto elencate:

1. Abilita la funzione Controllo delle versioni S3 su un bucket specificato (se la funzione Versione multiple di S3 è già abilitata, tale operazione non ha effetti).

2. Aggiunge un oggetto campione al bucket. In risposta a questa attività, Amazon S3 restituisce l'ID versione del nuovo oggetto aggiunto. L'esempio utilizza questo ID versione nella richiesta di eliminazione.
3. Elimina l'oggetto campione, specificando sia il nome della chiave dell'oggetto sia un ID versione.

 Note

È possibile ottenere l'ID versione di un oggetto anche inviando una richiesta `ListVersions`.

```
var listResponse = client.ListVersions(new ListVersionsRequest { BucketName  
    = bucketName, Prefix = keyName });
```

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;  
using Amazon.S3;  
using Amazon.S3.Model;  
using System;  
using System.Threading.Tasks;  
  
namespace Amazon.DocSamples.S3  
{  
    class DeleteObjectVersion  
    {  
        private const string bucketName = "**** versioning-enabled bucket name ****";  
        private const string keyName = "**** Object Key Name ****";  
        // Specify your bucket region (an example region is shown).  
        private static readonly RegionEndpoint bucketRegion =  
RegionEndpoint.USWest2;  
        private static IAmazonS3 client;  
  
        public static void Main()  
        {  
            client = new AmazonS3Client(bucketRegion);  
            CreateAndDeleteObjectVersionAsync().Wait();  
        }  
    }  
}
```

```
private static async Task CreateAndDeleteObjectVersionAsync()
{
    try
    {
        // Add a sample object.
        string versionID = await PutAnObject(keyName);

        // Delete the object by specifying an object key and a version ID.
        DeleteObjectRequest request = new DeleteObjectRequest
        {
            BucketName = bucketName,
            Key = keyName,
            VersionId = versionID
        };
        Console.WriteLine("Deleting an object");
        await client.DeleteObjectAsync(request);
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered on server. Message:'{0}' when deleting an object", e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when deleting an object", e.Message);
    }
}

static async Task<string> PutAnObject(string objectKey)
{
    PutObjectRequest request = new PutObjectRequest
    {
        BucketName = bucketName,
        Key = objectKey,
        ContentBody = "This is the content body!"
    };
    PutObjectResponse response = await client.PutObjectAsync(request);
    return response.VersionId;
}
}
```

PHP

Questo esempio mostra come utilizzare le classi della versione 3 AWS SDK per PHP per eliminare un oggetto da un bucket senza versione. Per informazioni sull'eliminazione di un oggetto da un bucket con versione, consulta [Utilizzo di REST API](#).

Per ulteriori informazioni sull'API AWS SDK for Ruby, vai a SDK for Ruby - [AWS Version 2](#).

Nell'esempio PHP seguente viene eliminato un oggetto da un bucket. Poiché questo esempio mostra come eliminare gli oggetti da bucket senza versione, questo fornisce solo il nome bucket e la chiave dell'oggetto (non un ID versione) nella richiesta di eliminazione.

```
<?php

require 'vendor/autoload.php';

use Aws\S3\S3Client;
use Aws\S3\Exception\S3Exception;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// 1. Delete the object from the bucket.
try
{
    echo 'Attempting to delete ' . $keyname . '...' . PHP_EOL;

    $result = $s3->deleteObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    if ($result['DeleteMarker'])
    {
        echo $keyname . ' was deleted or does not exist.' . PHP_EOL;
    } else {
        exit('Error: ' . $keyname . ' was not deleted.' . PHP_EOL);
    }
}
```

```
}
catch (S3Exception $e) {
    exit('Error: ' . $e->getAwsErrorMessage() . PHP_EOL);
}

// 2. Check to see if the object was deleted.
try
{
    echo 'Checking to see if ' . $keyname . ' still exists...' . PHP_EOL;

    $result = $s3->getObject([
        'Bucket' => $bucket,
        'Key'     => $keyname
    ]);

    echo 'Error: ' . $keyname . ' still exists.';
}
catch (S3Exception $e) {
    exit($e->getAwsErrorMessage());
}
```

Javascript

```
import { DeleteObjectCommand } from "@aws-sdk/client-s3";
import { s3Client } from "../libs/s3Client.js" // Helper function that creates Amazon
S3 service client module.

export const bucketParams = { Bucket: "BUCKET_NAME", Key: "KEY" };

export const run = async () => {
    try {
        const data = await s3Client.send(new DeleteObjectCommand(bucketParams));
        console.log("Success. Object deleted.", data);
        return data; // For unit tests.
    } catch (err) {
        console.log("Error", err);
    }
};
run();
```

Eliminazione di più oggetti

Tutti gli oggetti nel bucket S3 sono soggetti a costi di storage. È pertanto necessario eliminare quelli di cui non si ha più bisogno. Se ad esempio si esegue la raccolta di file di log, è una buona idea eliminarli quando non sono più necessari. È possibile impostare una regola del ciclo di vita per eliminare automaticamente oggetti come i file di log. Per ulteriori informazioni, consulta [the section called "Impostazione della configurazione del ciclo di vita"](#).

Per informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

Puoi utilizzare la console Amazon S3, gli AWS SDK o l'API REST per eliminare più oggetti contemporaneamente da un bucket S3.

Utilizzo della console S3

Segui questi passaggi per utilizzare la console di Amazon S3 per eliminare più oggetti da un bucket.

Warning

- L'eliminazione di un oggetto specificato non può essere annullata.
- Questa azione elimina tutti gli oggetti specificati. Quando si eliminano le cartelle, attendere che l'azione di eliminazione finisca prima di aggiungere nuovi oggetti alla cartella. In caso contrario, potrebbero essere eliminati anche nuovi oggetti.
- Quando si eliminano gli oggetti in un bucket senza il controllo delle versioni abilitato, compresi i bucket di directory, Amazon S3 elimina gli oggetti in modo permanente.
- Quando si eliminano oggetti in un bucket con il controllo delle versioni abilitato o sospeso, Amazon S3 crea dei marcatori di cancellazione. Per ulteriori informazioni, consulta [Utilizzo dei contrassegni di eliminazione](#).

Per eliminare gli oggetti con controllo delle versioni abilitato o sospeso

Note

Se gli ID di versione dell'oggetto in un bucket con controllo delle versioni sospeso sono contrassegnati come NULL, S3 elimina definitivamente gli oggetti poiché non esistono versioni precedenti. Tuttavia, se viene elencato un ID versione valido per gli oggetti in un

bucket con controllo delle versioni sospeso, S3 crea marcatori di cancellazione per gli oggetti eliminati, mantenendo le versioni precedenti degli oggetti.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket da cui eliminare gli oggetti.
4. Seleziona gli oggetti e scegli Elimina.
5. Per confermare l'eliminazione dell'elenco degli oggetti in Oggetti specificati, nella casella di testo Eliminare gli oggetti? immetti **delete**.

Per eliminare definitivamente versioni specifiche di oggetti in un bucket con controllo delle versioni abilitato

 Warning

Quando si eliminano definitivamente versioni specifiche di oggetti in Amazon S3, l'eliminazione non può essere annullata.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket da cui eliminare gli oggetti.
4. Selezionare gli oggetti che si intendono eliminare.
5. Scegli il pulsante Mostra versioni.
6. Seleziona le versioni dell'oggetto e scegli Elimina.
7. Per confermare l'eliminazione permanente delle versioni specifiche degli oggetti elencati in Oggetti specificati, nella casella di testo Eliminare gli oggetti? immetti Elimina definitivamente. Amazon S3 elimina definitivamente le versioni di oggetti specifici.

Per eliminare definitivamente gli oggetti in un bucket Amazon S3 non avere il controllo delle versioni abilitato

 Warning

Quando si elimina definitivamente un oggetto in Amazon S3, l'eliminazione non può essere annullata. Inoltre, per tutti i bucket senza il controllo delle versioni abilitato, compresi i bucket di directory, le eliminazioni sono permanenti.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.
3. Nell'elenco dei bucket scegli il nome del bucket da cui eliminare gli oggetti.
4. Seleziona gli oggetti e scegli Elimina.
5. Per confermare l'eliminazione permanente degli oggetti elencati in Oggetti specificati, nella casella di testo Eliminare gli oggetti? immetti Elimina definitivamente.

 Note

Se si verificano problemi con l'eliminazione degli oggetti, consulta [Voglio eliminare definitivamente gli oggetti con il controllo delle versioni abilitato](#).

Utilizzo di AWS SDK

Per esempi su come eliminare più oggetti con gli AWS SDK, consulta [Eliminare più oggetti](#) negli esempi di codice AWS SDK.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli SDK](#) negli esempi di AWS codice SDK. AWS

Utilizzo della REST API

Puoi utilizzare gli AWS SDK per eliminare più oggetti utilizzando l'API Delete. Multi-Object Tuttavia, se l'applicazione lo richiede, è possibile inviare richieste REST direttamente.

Per ulteriori informazioni, consulta la sezione relativa all'[eliminazione di più oggetti](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Organizzare, elencare e utilizzare gli oggetti

In Amazon S3, puoi utilizzare i prefissi per organizzare lo spazio di storage. Un prefisso è un raggruppamento logico degli oggetti in un bucket. Il valore del prefisso è simile a un nome di directory che consente di archiviare dati simili nella stessa directory in un bucket. Quando si caricano oggetti a livello di programmazione, è possibile utilizzare i prefissi per organizzare i dati.

Nella console di Amazon S3, i prefissi sono chiamati cartelle. È possibile visualizzare tutti gli oggetti e le cartelle nella console S3 passando a un bucket. È inoltre possibile visualizzare informazioni su ciascun oggetto, incluse le proprietà dell'oggetto.

Per ulteriori informazioni sull'elenco e sull'organizzazione dei dati in Amazon S3, consulta i seguenti argomenti.

Argomenti

- [Organizzazione degli oggetti utilizzando i prefissi](#)
- [Elenco delle chiavi oggetto a livello di programmazione](#)
- [Organizzazione degli oggetti nella console di Amazon S3 utilizzando le cartelle](#)
- [Visualizzazione delle proprietà di un oggetto nella console di Amazon S3](#)

Organizzazione degli oggetti utilizzando i prefissi

Puoi utilizzare i prefissi per organizzare i dati archiviati nei bucket Amazon S3. Un prefisso è una stringa di caratteri all'inizio del nome della chiave dell'oggetto. Un prefisso può essere di qualsiasi lunghezza, soggetto alla lunghezza massima del nome della chiave dell'oggetto (1.024 byte). Puoi pensare ai prefissi come un modo per organizzare i dati in modo simile alle directory. Tuttavia, i prefissi non sono directory.

La ricerca per prefisso limita i risultati solo alle chiavi che iniziano con il prefisso specificato. Il delimitatore fa in modo che l'operazione di elenco esegua il rollup di tutte le chiavi che condividono un prefisso comune in un unico risultato di elenco di riepilogo.

Lo scopo dei parametri Prefix e Delimiter è facilitare l'organizzazione e la visualizzazione delle chiavi in ordine gerarchico. A tale scopo, selezionare un delimitatore per il bucket, ad esempio una

barra (/), che non ricorra nei nomi delle chiavi previsti. È possibile utilizzare un altro carattere come delimitatore. Non c'è nulla di unico nel carattere slash (/), ma è un delimitatore di prefisso molto comune. Creare quindi i nomi delle chiavi concatenando tutti i livelli della gerarchia e separando ciascun livello con il delimitatore.

Ad esempio, se si archiviano informazioni sulle città, è possibile organizzarle naturalmente in base al continente, quindi in base al paese, alla provincia o allo stato. Poiché questi nomi in genere non contengono punteggiatura, è possibile selezionare la barra (/) come delimitatore. I seguenti esempi mostrano come utilizzare la barra (/) come delimitatore.

- Europe/France/Nouvelle-Aquitaine/Bordeaux
- Nord America/Canada/Quebec/Montreal
- Nord America/USA/Washington/Bellevue
- Nord America/USA/Washington/Seattle

Se i dati di ogni città del mondo sono stati archiviati in questo modo, sarebbe strano gestire un namespace di chiavi piatto. Utilizzando Prefix e Delimiter nell'operazione di elenco, puoi usare la gerarchia creata per elencare i dati. Ad esempio, per elencare tutti gli stati degli Stati Uniti, imposta Delimiter='/' e Prefix='North America/USA/'. Per elencare tutte le province del Canada per le quali sono disponibili dati, imposta Delimiter='/' e Prefix='North America/Canada/'.

Per ulteriori informazioni su delimitatori, prefissi e cartelle nidificate, consulta [Differenza tra prefissi e cartelle nidificate](#).

Elenco di oggetti utilizzando prefissi e delimitatori

Se richiedi un elenco con un delimitatore, puoi visualizzare la gerarchia a un solo livello, omettendo e riassumendo le chiavi (possibilmente milioni di esse) nidificate ai livelli più profondi. Ad esempio, supponi di avere un bucket (*amzn-s3-demo-bucket*) con le seguenti chiavi:

sample.jpg

photos/2006/January/sample.jpg

photos/2006/February/sample2.jpg

photos/2006/February/sample3.jpg

photos/2006/February/sample4.jpg

Il bucket di esempio contiene solo l'oggetto `sample.jpg` a livello root. Per elencare solo gli oggetti a livello root nel bucket, invii una richiesta GET nel bucket con il carattere delimitatore della barra (/). In risposta, Amazon S3 restituisce la chiave dell'oggetto `sample.jpg` poiché non contiene il carattere delimitatore /. Tutte le altre chiavi contengono questo carattere. Amazon S3 raggruppa queste chiavi e restituisce un singolo elemento `CommonPrefixes` con il valore di prefisso `photos/`, che è una sottostringa dall'inizio di queste chiavi alla prima occorrenza del delimitatore specificato.

Example

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>amzn-s3-demo-bucket</Name>
  <Prefix></Prefix>
  <Marker></Marker>
  <MaxKeys>1000</MaxKeys>
  <Delimiter>/</Delimiter>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>sample.jpg</Key>
    <LastModified>2011-07-24T19:39:30.000Z</LastModified>
    <ETag>"d1a7fb5eab1c16cb4f7cf341cf188c3d"</ETag>
    <Size>6</Size>
    <Owner>
      <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <CommonPrefixes>
    <Prefix>photos/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

Per ulteriori informazioni sull'elenco delle chiavi oggetto a livello di programmazione, consulta la sezione [Elenco delle chiavi oggetto a livello di programmazione](#).

Elenco delle chiavi oggetto a livello di programmazione

In Amazon S3, le chiavi possono essere elencate per prefisso. È possibile scegliere un prefisso comune per i nomi delle chiavi correlate e contrassegnare queste chiavi con un carattere speciale che delimita la gerarchia. È quindi possibile utilizzare l'operazione elenco per selezionare e sfogliare

le chiavi gerarchicamente. Questa operazione è simile all'archiviazione dei file in directory all'interno di un file system.

Amazon S3 visualizza un'operazione di elenco che consente di elencare le chiavi contenute in un bucket. Le chiavi vengono selezionate per l'elenco in base al bucket e al prefisso. Ad esempio, si prenda in considerazione un bucket denominato "dictionary" contenente una chiave per ogni parola inglese. È possibile eseguire una chiamata per elencare tutte le chiavi in tale bucket che iniziano con la lettera "q". I risultati dell'elenco vengono sempre restituiti in ordine UTF-8 binario.

Sia le operazioni di elenco SOAP che quelle REST restituiscono un documento XML contenente i nomi delle chiavi corrispondenti e informazioni sull'oggetto identificato da ciascuna chiave.

Note

Le API SOAP per Amazon S3 non sono disponibili per i nuovi clienti, con la fine del ciclo di vita prevista per il 31 agosto 2025. Ti consigliamo di utilizzare l'API REST o gli AWS SDK.

È possibile raggruppare i gruppi di chiavi che condividono un prefisso che termina con un delimitatore speciale in base al prefisso comune a scopo di elenco. Ciò consente alle applicazioni di organizzare ed esplorare le chiavi in ordine gerarchico, in modo simile all'organizzazione dei file in directory in un file system.

Ad esempio, per estendere il bucket dictionary in modo che contenga altre parole oltre a quelle inglesi, è possibile creare chiavi anteponendo a ciascuna parola un prefisso insieme alla lingua e a un delimitatore, ad esempio "French/logical". È possibile utilizzare questo schema di denominazione e la funzione di elenco gerarchico per recuperare un elenco costituito solo dalle parole francesi. È inoltre possibile sfogliare l'elenco di livello superiore delle lingue disponibili senza dover scorrere tutte le chiavi utilizzate in ordine lessicografico. Per ulteriori informazioni su questo tipo di elenco, consulta [Organizzazione degli oggetti utilizzando i prefissi](#).

REST API

Tuttavia, se l'applicazione lo richiede, è possibile inviare richieste REST direttamente. È possibile inviare una richiesta GET per restituire alcuni o tutti gli oggetti in un bucket oppure è possibile utilizzare le policy di selezione per restituire un sottoinsieme degli oggetti in un bucket. Per ulteriori informazioni, consulta l'argomento relativo all'operazione [GET Bucket \(List Objects\) Version 2](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Efficacia dell'implementazione degli elenchi

Le prestazioni dell'elenco non sono influenzate in modo sostanziale dal numero totale di chiavi nel bucket. Inoltre, non sono influenzate dalla presenza o dall'assenza degli argomenti `delimiter`, `prefix`, `marker` o `maxkeys`.

Scorrimento dei risultati di più pagine

Poiché i bucket possono contenere un numero potenzialmente illimitato di chiavi, una query di elenco può restituire un numero estremamente elevato di risultati. Per gestire set di risultati di grandi dimensioni, l'API di Amazon S3 supporta la paginazione per suddividerli in più risposte. Ciascuna risposta delle chiavi di elenco restituisce una pagina contenente fino a 1000 chiavi con un indicatore che specifica se la risposta è troncata. Invii una serie di richieste di chiavi di elenco finché non hai ricevuto tutte le chiavi. AWS Le librerie wrapper SDK forniscono la stessa impaginazione.

Esempi

Tieni presente che quando elenchi tutti gli oggetti nel bucket, devi disporre dell'autorizzazione `s3:ListBucket`.

CLI

`list-objects`

L'esempio seguente utilizza il comando `list-objects` per visualizzare i nomi di tutti gli oggetti del bucket specificato:

```
aws s3api list-objects --bucket text-content --query 'Contents[].{Key: Key, Size: Size}'
```

L'esempio utilizza l'argomento `--query` per filtrare l'output di `list-objects` fino al valore della chiave e alla dimensione per ogni oggetto

Per ulteriori informazioni sugli oggetti, consulta [Utilizzo degli oggetti in Amazon S3](#).

- Per i dettagli sull'API, vedi [ListObjects](#) in Command Reference. AWS CLI

`ls`

L'esempio seguente elenca tutti gli oggetti e i prefissi di un bucket utilizzando il comando `ls`.

Per utilizzare questo esempio di comando, sostituisci *amzn-s3-demo-bucket* con il nome del bucket.

```
$ aws s3 ls s3://amzn-s3-demo-bucket
```

- Per ulteriori informazioni sul comando di alto livello `ls`, consulta [Elenco di bucket e oggetti](#) nella Guida all'utente AWS Command Line Interface .

PowerShell

Strumenti per PowerShell V4

Esempio 1: questo comando recupera le informazioni su tutti gli elementi presenti nel bucket "test-files".

```
Get-S3Object -BucketName amzn-s3-demo-bucket
```

Esempio 2: questo comando recupera le informazioni sull'elemento "sample.txt" dal bucket "test-files".

```
Get-S3Object -BucketName amzn-s3-demo-bucket -Key sample.txt
```

Esempio 3: questo comando recupera le informazioni su tutti gli elementi con il prefisso "sample" dal bucket "test-files".

```
Get-S3Object -BucketName amzn-s3-demo-bucket -KeyPrefix sample
```

- Per i dettagli sull'API, vedere [ListObjects](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo comando recupera le informazioni su tutti gli elementi presenti nel bucket "test-files".

```
Get-S3Object -BucketName amzn-s3-demo-bucket
```

Esempio 2: questo comando recupera le informazioni sull'elemento "sample.txt" dal bucket "test-files".

```
Get-S3Object -BucketName amzn-s3-demo-bucket -Key sample.txt
```


Esempio 3: questo comando recupera le informazioni su tutti gli elementi con il prefisso "sample" dal bucket "test-files".

```
Get-S3Object -BucketName amzn-s3-demo-bucket -KeyPrefix sample
```

- Per i dettagli sull'API, vedere [ListObjects](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Organizzazione degli oggetti nella console di Amazon S3 utilizzando le cartelle

In Amazon S3 bucket per uso generico e oggetti sono risorse primarie, dove gli oggetti sono archiviati nei bucket. I bucket per uso generico di Amazon S3 hanno una struttura piatta anziché gerarchica come quella che si vedrebbe in un file system. Tuttavia, per semplicità di organizzazione, la console di Amazon S3 supporta il concetto di cartella come metodo di raggruppamento degli oggetti.

La console esegue questa operazione utilizzando un prefisso di nome condiviso per gli oggetti raggruppati. In altre parole, gli oggetti del gruppo hanno nomi che iniziano con una stringa comune. Questa stringa comune, o prefisso condiviso, è il nome della cartella. I nomi degli oggetti sono inoltre noti come nomi chiave.

È possibile, ad esempio, creare una cartella in un bucket per uso generico nella console denominata photos e archiviarvi un oggetto denominato myphoto.jpg. Tale oggetto viene quindi memorizzato con il nome delle chiave photos/myphoto.jpg, di cui photos/ è il prefisso.

Ecco altri due esempi:

- Se il bucket per uso generico contiene tre oggetti, logs/date1.txt, logs/date2.txt e logs/date3.txt, la console mostrerà una cartella denominata logs. Se si apre la cartella nella console, si vedranno tre oggetti: date1.txt, date2.txt e date3.txt.
- Se è presente un oggetto denominato photos/2017/example.jpg, la console mostra una cartella denominata photos contenente la cartella 2017. La cartella 2017 contiene l'oggetto example.jpg.

Si possono avere cartelle nidificate, ma non bucket all'interno di altri bucket. È possibile caricare e copiare gli oggetti direttamente in una cartella. Le cartelle possono essere create, eliminate e rese pubbliche, ma non possono essere rinominate. Gli oggetti possono essere copiati da una cartella all'altra.

Important

Quando nella console Amazon S3 si crea una cartella, S3 crea un oggetto a 0 byte. Questa chiave dell'oggetto è impostata sul nome della cartella che fornito più un carattere barra (/) finale. Ad esempio, se nella console Amazon S3 si crea una cartella denominata photos nel bucket, la console Amazon S3 crea un oggetto a 0 byte con la chiave photos/. La console crea questo oggetto a supporto del concetto di cartella.

Inoltre, qualsiasi oggetto preesistente il cui nome termina con il carattere barra (/) viene visualizzato come cartella nella console Amazon S3. Ad esempio, un oggetto con il nome della chiave examplekeyname/ viene visualizzato come cartella nella console Amazon S3 e non come oggetto. Altrimenti, si comporta come qualsiasi altro oggetto e può essere visualizzato e manipolato tramite AWS Command Line Interface (AWS CLI), AWS SDK o API REST. Inoltre, non è possibile caricare un oggetto con un nome di chiave che termina con il carattere barra (/) mediante la console Amazon S3. Tuttavia, puoi caricare oggetti denominati con una barra (/) finale utilizzando AWS Command Line Interface (AWS CLI), AWS SDK o API REST.

Inoltre, la console Amazon S3 non mostra il contenuto e i metadati per gli oggetti cartella analogamente ad altri oggetti. Quando si utilizza la console per copiare un oggetto il cui nome termina con il carattere barra (/), viene creata una nuova cartella nella posizione di destinazione, ma i dati e i metadati dell'oggetto non vengono copiati. Inoltre, la barra (/) nei nomi di chiave degli oggetti potrebbe richiedere una gestione speciale. Per ulteriori informazioni, consulta [Denominazione di oggetti Amazon S3](#).

Per creare le cartelle nei bucket di directory, carica una cartella. Per ulteriori informazioni, consulta [Caricamento di oggetti in un bucket di directory](#).

Argomenti

- [Creazione di una cartella](#)
- [Creazione di cartelle pubbliche](#)
- [Calcolo delle dimensioni delle cartelle](#)
- [Eliminazione di cartelle](#)

Creazione di una cartella

Questa sezione spiega come utilizzare la console di Amazon S3 per creare una cartella.

Important

Se la policy del bucket impedisce il caricamento di oggetti in questo bucket senza tag, metadati o assegnatari della lista di controllo degli accessi (ACL), non sarai in grado di creare una cartella utilizzando questa configurazione. Si dovrà invece caricare una cartella vuota e specificare queste impostazioni nella configurazione di caricamento.

Come creare una cartella

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket in cui desideri creare una cartella.
4. Nella scheda Oggetti, scegli Crea cartella.
5. Immettere un nome per la cartella (ad esempio, **favorite-pics**).

Note

I nomi delle cartelle sono soggetti a determinate limitazioni e linee guida e sono considerati parte del nome di chiave dell'oggetto, che è limitato a 1.024 byte. Per ulteriori informazioni, consulta [the section called "Denominazione di oggetti"](#).

6. (Facoltativo) Se la tua bucket policy richiede che gli oggetti siano crittografati con una chiave di crittografia specifica, in Server-side Crittografia, devi scegliere Specifica una chiave di crittografia e specificare la stessa chiave di crittografia quando crei una cartella. In caso contrario, la creazione della cartella avrà esito negativo.
7. Scegliere Create folder (Crea cartella).

Creazione di cartelle pubbliche

Consigliamo di bloccare tutto l'accesso pubblico alle cartelle e ai bucket Amazon S3 a meno che non siano necessari una cartella o un bucket pubblici. Quando si rende pubblica una cartella, chiunque su Internet può visualizzare tutti gli oggetti raggruppati nella cartella.

Nella console di Amazon S3 puoi rendere pubblica una cartella. Una cartella può anche essere resa pubblica creando una policy di bucket che ne limita l'accesso ai dati in base al prefisso. Per ulteriori informazioni, consulta [Identity and Access Management per Amazon S3](#).

Warning

Dopo aver reso pubblica una cartella nella console di Amazon S3 non è possibile renderla nuovamente privata. È necessario invece impostare le autorizzazioni per ogni singolo oggetto nella cartella pubblica affinché gli oggetti non abbiano accesso pubblico. Per ulteriori informazioni, consulta [Configurazione delle ACL](#).

Argomenti

- [Calcolo delle dimensioni delle cartelle](#)
- [Eliminazione di cartelle](#)

Calcolo delle dimensioni delle cartelle

Questa sezione spiega come utilizzare la console di Amazon S3 per calcolare le dimensioni di una cartella.

Calcolo delle dimensioni di una cartella

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco Bucket per uso generico, scegli il nome del bucket in cui è archiviata la cartella.
4. Nell'elenco Oggetti, seleziona la casella di controllo accanto al nome della cartella.
5. Scegli Actions (Azioni), quindi scegli Calculate total size (Calcola dimensione totale).

Note

Le informazioni sulla cartella (inclusa la dimensione totale) non sono più disponibili una volta usciti dalla pagina. È necessario calcolare nuovamente la dimensione totale se si desidera vederla di nuovo.

Important

Quando utilizzi l'azione Calculate total size (Calcola dimensione totale) su oggetti o cartelle specificati all'interno del bucket, Amazon S3 calcola il numero totale di oggetti e la dimensione totale dello spazio di archiviazione. Tuttavia, i caricamenti in più parti incompleti o in corso e le versioni precedenti o non correnti non vengono considerati nel calcolo del numero totale di oggetti o della dimensione totale. Questa azione calcola solo il numero totale di oggetti e la dimensione totale per la versione corrente o più recente di ogni oggetto archiviato nel bucket.

Ad esempio, se nel bucket sono presenti due versioni di un oggetto, il calcolatore dello spazio di archiviazione in Amazon S3 le considera un unico oggetto. Di conseguenza, il numero totale di oggetti calcolato nella console Amazon S3 può differire dalla metrica Object Count mostrata in S3 Storage Lens e dal numero riportato dalla metrica Amazon, CloudWatch NumberOfObjects. Allo stesso modo, la dimensione totale dello storage può anche differire dalla metrica Total Storage mostrata in S3 Storage Lens e dalla metrica mostrata in BucketSizeBytes CloudWatch.

Eliminazione di cartelle

Usa la console Amazon S3 per eliminare cartelle da un bucket S3.

Per informazioni sulle funzionalità e sui prezzi di Amazon S3, consulta [Amazon S3](#).

Per eliminare cartelle da un bucket S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco Bucket per uso generico scegli il nome del bucket da cui desideri eliminare cartelle.
4. Nell'elenco Oggetti, seleziona la casella di controllo accanto alle cartelle e agli oggetti che desideri eliminare.
5. Scegliere Elimina.
6. Nella pagina Elimina oggetti, verifica che le cartelle e gli oggetti scelti siano elencati in Oggetti specificati.
7. Nella casella Elimina oggetti, immetti **delete** e scegli Elimina oggetti.

 Warning

Questa azione elimina tutti gli oggetti specificati. Quando elimini le cartelle, attendi che l'eliminazione finisca prima di aggiungere nuovi oggetti alla cartella. In caso contrario, potrebbero essere eliminati anche nuovi oggetti.

Visualizzazione delle proprietà di un oggetto nella console di Amazon S3

Puoi utilizzare la console di Amazon S3 per visualizzare le proprietà di un oggetto, tra cui classe di storage, impostazioni di crittografia, tag e metadati.

Per visualizzare le proprietà di un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.
3. Nell'elenco dei bucket scegli il nome del bucket contenente l'oggetto.
4. Nell'elenco Oggetti, scegli il nome dell'oggetto del quale desideri visualizzare le proprietà.

Viene visualizzata la Panoramica dell'oggetto. È possibile scorrere verso il basso per visualizzare le proprietà dell'oggetto.

5. Nella pagina Panoramica dell'oggetto è possibile visualizzare o configurare le proprietà dell'oggetto indicate di seguito.

 Note

- Se modifichi una delle proprietà Classe di storage, Crittografia o Metadati, viene creato un nuovo oggetto per sostituire quello precedente. Se è abilitata la funzione Controllo delle versioni S3, viene creata una nuova versione dell'oggetto e l'oggetto esistente diventa una versione precedente. Il ruolo che modifica la proprietà diventa anche il proprietario del nuovo oggetto o della versione dell'oggetto.
- Se si modificano le proprietà Classe di archiviazione, Crittografia o Metadati di un oggetto con tag definiti dall'utente, è necessario disporre dell'autorizzazione `s3:GetObjectTagging`. Se si modificano queste proprietà per un oggetto che non ha tag definiti dall'utente ma ha una dimensione superiore a 16 MB, è necessario disporre dell'autorizzazione `s3:GetObjectTagging`.

Se la policy del bucket di destinazione nega l'azione `s3:GetObjectTagging`, le proprietà dell'oggetto verranno aggiornate, ma i tag definiti dall'utente verranno rimossi dall'oggetto e si riceverà un errore.

- a. **Storage class (Classe di storage):** a ogni oggetto in Amazon S3 è associata una classe di storage. La classe di storage che si sceglie di utilizzare dipende dalla frequenza con cui si accede all'oggetto. La classe di archiviazione predefinita per gli oggetti S3 nei bucket per uso generico è STANDARD. La classe di archiviazione predefinita per gli oggetti S3 nei bucket di directory è S3 Express One Zone. È possibile scegliere la classe di storage quando si carica un oggetto. Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

Per cambiare la classe di archiviazione dopo avere caricato un oggetto in un bucket per uso generico, scegli Classe di archiviazione. Scegliere la classe desiderata, quindi selezionare Save (Salva).

 Note

La classe di archiviazione degli oggetti in un bucket di directory non può essere modificata.

- b. **Server-side impostazioni di crittografia:** puoi utilizzare la crittografia lato server per crittografare i tuoi oggetti S3. Per ulteriori informazioni, consulta le sezioni [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#) o [Specificare la crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).
- c. **Metadata (Metadati):** ciascun oggetto in Amazon S3 dispone di un set di coppie nome-valore che ne rappresenta i metadati. Per informazioni sull'aggiunta di metadati a un oggetto di S3, consulta [Modifica dei metadati degli oggetti nella console di Amazon S3](#).
- d. **Tag:** è possibile classificare l'archiviazione aggiungendo tag a un oggetto S3 in un bucket per uso generico. Per ulteriori informazioni, consulta [Etichettare i tuoi oggetti](#).
- e. **Blocco legale e conservazione di Object Lock:** è possibile impedire l'eliminazione di un oggetto in bucket per uso generico. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).

Download e caricamento di oggetti con URL predefiniti

Per concedere un accesso limitato nel tempo agli oggetti in Amazon S3 senza aggiornare la policy del bucket, puoi utilizzare un URL prefirmato. Un URL prefirmato può essere inserito in un browser o utilizzato da un programma per scaricare un oggetto. Le credenziali utilizzate dall'URL prefirmato sono quelle del principale AWS Identity and Access Management (IAM) che ha generato l'URL.

Puoi anche utilizzare gli URL prefirmati per consentire a qualcuno di caricare un oggetto specifico nel tuo bucket Amazon S3. Ciò consente un caricamento senza che un'altra parte disponga di credenziali o AWS autorizzazioni di sicurezza. Se nel bucket esiste già un oggetto con la stessa chiave specificata nell'URL prefirmato, Amazon S3 sostituisce l'oggetto esistente con l'oggetto caricato.

È possibile utilizzare l'URL prefirmato più volte, fino alla data e all'ora di scadenza.

Le operazioni dell'API di annotazione (`PutObjectAnnotation`, `GetObjectAnnotationListObjectAnnotations`, `DeleteObjectAnnotation`) supportano URL prefirmati.

Quando crei un URL prefirmato, devi fornire le credenziali di sicurezza e specificare quanto segue:

- Un bucket Amazon S3
- Una chiave oggetto (se il download di questo oggetto sarà nel tuo bucket Amazon S3, se lo stai caricando questo è il nome del file da caricare)
- Un metodo HTTP (GET per scaricare oggetti, PUT per caricare, HEAD per leggere i metadati degli oggetti e così via)
- Un intervallo di tempo di scadenza

Quando si utilizzano gli URL prefirmati per caricare oggetti, è possibile verificare l'integrità degli oggetti utilizzando i checksum. Mentre gli URL prefirmati creati con AWS Signature versione 2 supportano solo i checksum MD5, gli URL prefirmati creati con AWS Signature versione 4 supportano algoritmi di checksum aggiuntivi tra cui CRC-64/NVME,,,,,,, e. CRC32 CRC32C SHA-1 SHA-256 MD5 XXHash64 XXHash3 XXHash128 SHA-512 Per utilizzare questi algoritmi di checksum aggiuntivi, assicurati di utilizzare la versione 4 di AWS Signature e includi l'intestazione di checksum appropriata nella richiesta di caricamento. Per ulteriori informazioni sull'integrità degli oggetti, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Argomenti

- [Chi può creare un URL prefirmato](#)
- [Tempo di scadenza per gli URL prefirmati](#)
- [Limitazione delle funzionalità degli URL prefirmati](#)
- [Domande frequenti sugli URL prefirmati](#)
- [Condivisione di oggetti mediante URL prefirmati](#)
- [Caricamento di oggetti con URL prefirmati](#)

Chi può creare un URL prefirmato

Qualsiasi utente che disponga di credenziali di sicurezza valide può creare un URL prefirmato. Tuttavia, per accedere a un oggetto, è necessario che l'URL prefirmato sia creato da un utente che dispone dell'autorizzazione a eseguire l'operazione su cui si basa l'URL prefirmato.

Le credenziali che puoi utilizzare per creare un URL prefirmato sono:

- Utente IAM: valido fino a 7 giorni se utilizzi AWS la versione 4 di Signature.

Per creare un URL prefirmato valido fino a 7 giorni, devi prima delegare le credenziali dell'utente IAM (la chiave di accesso e la chiave segreta) al metodo in uso per creare l'URL prefirmato.

- Credenziali di sicurezza temporanee: non possono essere valide più a lungo delle credenziali stesse. Queste credenziali includono:
 - Credenziali del ruolo IAM: l'URL prefirmato scade alla scadenza della sessione del ruolo, anche se è specificato un tempo più lungo.
 - Credenziali del ruolo IAM utilizzate dalle istanze Amazon EC2: valide per la durata delle credenziali del ruolo (in genere 6 ore).
 - Servizio di token di sicurezza AWS credenziali: valide solo per la durata delle credenziali temporanee.

Note

Se hai creato un URL prefirmato utilizzando credenziali temporanee, l'URL scade insieme alle credenziali. In generale, un URL prefirmato scade quando la credenziale utilizzata per crearlo viene revocata, cancellata o disattivata. Ciò avviene anche se l'URL è stato creato con un orario di scadenza successivo. Per la durata delle credenziali di sicurezza temporanee, consulta [Comparing AWS STS API operations](#) nella IAM User Guide.

Tempo di scadenza per gli URL prefirmati

Un URL prefirmato rimane valido per il periodo di tempo specificato al momento della generazione dell'URL. Se crei un URL prefirmato con la console di Amazon S3, il tempo di scadenza può essere impostato tra 1 minuto e 12 ore. Se utilizzi gli AWS CLI o AWS SDK, la data di scadenza può essere impostata fino a 7 giorni.

Se si è creato un URL prefirmato utilizzando un token temporaneo, l'URL scade quando scade il token. In generale, un URL prefirmato scade quando la credenziale utilizzata per crearlo viene revocata, cancellata o disattivata. Ciò avviene anche se l'URL è stato creato con un orario di scadenza successivo. Per ulteriori informazioni su come le credenziali utilizzate influiscono sulla data di scadenza, consulta [Chi può creare un URL prefirmato](#).

Simple Storage Service (Amazon S3) verifica la data e l'ora di scadenza in un URL firmato al momento della richiesta HTTP. Ad esempio, se un client inizia a scaricare un file di grandi dimensioni immediatamente prima dell'ora di scadenza, il download viene completato anche se l'ora di scadenza viene superata. Se la connessione TCP viene interrotta e il client prova a riavviare il download dopo la scadenza, il download non riesce.

Limitazione delle funzionalità degli URL prefirmati

Le funzionalità dell'URL prefirmato sono limitate dalle autorizzazioni dell'utente che lo ha creato. In sostanza, gli URL prefirmati sono token di connessione che consentono l'accesso agli utenti che li possiedono. Pertanto, consigliamo di proteggerli in modo appropriato. Di seguito sono elencati alcuni metodi che puoi usare per limitare l'uso degli URL prefirmati.

AWS Signature versione 4 (SIGv4)

Per applicare un comportamento specifico quando le richieste dell'URL prefirmato vengono autenticate tramite AWS Signature Version 4 (SigV4), puoi utilizzare le chiavi di condizione nelle policy del bucket e nelle policy dei punti di accesso. Ad esempio, la policy di bucket seguente utilizza la condizione `s3:signatureAge` per negare qualsiasi richiesta di URL prefirmato da Amazon S3 sugli oggetti nel bucket *amzn-s3-demo-bucket* se la firma ha più di 10 minuti. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

JSON

```
{  
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Sid": "Deny a presigned URL request if the signature is more than 10
min old",
        "Effect": "Deny",
        "Principal": {
          "AWS": "*"
        },
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
          "NumericGreaterThan": {
            "s3:signatureAge": "600000"
          }
        }
      }
    ]
  }
}

```

Per ulteriori informazioni sulle chiavi di policy relative a AWS Signature Version 4, consulta [AWS Signature Version 4 Authentication](#) nell'Amazon Simple Storage Service API Reference.

Limitazioni per percorso di rete

Se desideri limitare l'uso di URL prefirmati e tutti gli accessi di Amazon S3 a particolari percorsi di rete, puoi scrivere policy AWS Identity and Access Management (IAM). Puoi impostare queste policy sul principale del servizio IAM che effettua la chiamata, sul bucket Amazon S3 o su entrambi.

Una restrizione del percorso di rete sul principale IAM richiede all'utente di tali credenziali di effettuare le richieste dalla rete specificata. Una restrizione sul bucket o sul punto di accesso richiede che tutte le richieste a quella risorsa provengano dalla rete specificata. Queste restrizioni si applicano anche al di fuori dello scenario di URL prefirmato.

La chiave della condizione globale IAM utilizzata dipende dal tipo di endpoint. Se utilizzi l'endpoint pubblico per Amazon S3, utilizza `aws:SourceIp`. Se utilizzi un endpoint di cloud privato virtuale (VPC) per Amazon S3, usa `aws:SourceVpc` o `aws:SourceVpce`.

La seguente dichiarazione sulla politica IAM richiede che il principale acceda AWS solo dall'intervallo di rete specificato. Con questa istruzione della policy, tutti gli accessi devono avere origine da tale intervallo. Ciò include il caso di un utente che utilizza un URL prefirmato per Amazon S3. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
{
  "Sid": "NetworkRestrictionForIAMPrincipal",
  "Effect": "Deny",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "NotIpAddressIfExists": {"aws:SourceIp": "IP-address-range"},
    "BoolIfExists": {"aws:ViaAWSService": "false"}
  }
}
```

Domande frequenti sugli URL prefirmati

D: Perché gli URL prefirmati scadono prima dell'ora di scadenza configurata?

Gli URL prefirmati rimangono validi solo finché le relative credenziali sottostanti sono valide. Un URL prefirmato scade all'ora di scadenza configurata o alla scadenza delle credenziali associate, a seconda di quale evento si verifica per primo. Per le attività o i container di Amazon Elastic Container Service, le credenziali di ruolo ruotano in genere ogni 1-6 ore. Quando si utilizza Servizio di token di sicurezza AWS (AWS STS) AssumeRole, l'URL prefirmato scade al termine della sessione di ruolo, che per impostazione predefinita è di 1 ora. Per i profili di istanza Amazon EC2, le credenziali dei metadati ruotano periodicamente con un periodo di validità massimo di circa 6 ore.

D: Perché ricevo l'errore 403 Forbidden quando accedo a un URL prefirmato?

Prima di generare un URL prefirmato, verifica di disporre delle autorizzazioni corrette. L'utente o il ruolo IAM che genera l'URL deve disporre delle autorizzazioni necessarie, ad esempio `s3:GetObject`, per l'operazione specifica. Inoltre, verifica che la policy di bucket di Amazon S3 non neghi esplicitamente l'accesso all'oggetto.

D: Perché ricevo un **AccessDenied** errore con **HeadersNotSigned: if-range**?

Quando Range è incluso `X-Amz-SignedHeaders`, Amazon S3 richiede che sia firmato `If-Range` anche se presente nella richiesta. Aggiungi `If-Range` a `X-Amz-SignedHeaders` quando generi l'URL prefirmato.

D: Ricevo errori **SignatureDoesNotMatch**. Come è possibile risolvere il problema?

Se riscontri errori `SignatureDoesNotMatch` durante l'utilizzo di URL prefirmati di Amazon S3, le cause comuni possono essere diverse. Innanzitutto, assicurati che l'orologio di sistema sia

sincronizzato con un server Network Time Protocol (NTP), poiché anche piccole variazioni di tempo possono invalidare le firme. Inoltre, tieni presente che alcuni proxy aziendali possono modificare le intestazioni o le stringhe di query, causando potenzialmente mancate corrispondenze tra le firme. Per risolvere i problemi, prova a eseguire un test senza il proxy. Infine, verifica che tutti i parametri della richiesta, inclusi il metodo HTTP, le intestazioni e la stringa di query, corrispondano esattamente tra la generazione e l'utilizzo dell'URL. La risoluzione di questi problemi può spesso risolvere gli errori `SignatureDoesNotMatch`.

D: Ricevo errori **ExpiredToken**. Cosa devo fare?

Quando ricevi `ExpiredToken` errori durante l'utilizzo di URL prefirmiti, indica che le AWS credenziali utilizzate per generare l'URL non sono più valide. Per risolvere questo problema, aggiorna le AWS credenziali prima di generare nuovi URL prefirmiti. Per le applicazioni di lunga durata, è consigliabile implementare la logica di aggiornamento delle credenziali per mantenere l'accesso continuo. Se appropriato, è possibile utilizzare le credenziali di lunga durata o implementare meccanismi di aggiornamento dei token. Se utilizzi Servizio di token di sicurezza AWS (AWS STS) `AssumeRole`, verifica che la durata della sessione configurata soddisfi i requisiti del tuo caso d'uso. Tieni presente che gli URL prefirmiti rimangono validi solo per la durata delle credenziali sottostanti, quindi è essenziale implementare una corretta gestione delle credenziali.

Condivisione di oggetti mediante URL prefirmiti

Per impostazione predefinita, tutti gli oggetti di Amazon S3 sono privati, solo il proprietario dell'oggetto dispone dell'autorizzazione per accedere agli oggetti di Amazon S3. Tuttavia, il proprietario dell'oggetto può condividere oggetti con altri creando un URL prefirmato. Un URL prefirmato utilizza le credenziali di sicurezza per concedere un'autorizzazione limitata nel tempo per scaricare oggetti. L'URL può essere inserito in un browser o utilizzato da un programma per scaricare l'oggetto. Le credenziali utilizzate dall'URL prefirmato sono quelle dell'AWS utente che ha generato l'URL.

Per ulteriori informazioni sugli URL prefirmiti, consulta [Download e caricamento di oggetti con URL predefiniti](#).

Puoi creare un URL prefirmato per condividere un oggetto senza scrivere alcun codice utilizzando la console Amazon S3, AWS Explorer for Visual Studio (Windows) o. AWS Toolkit for Visual Studio Code. Puoi anche generare un URL prefirmato a livello di codice utilizzando AWS Command Line Interface (AWS CLI) o gli SDK AWS.

Utilizzo della console S3

Puoi utilizzare la console Amazon S3 per generare un URL prefirmato per condividere un oggetto fino a 5 TB seguendo questi passaggi. Nella console, il tempo massimo di scadenza per un URL prefirmato è di 12 ore dal momento della creazione.

Generazione di un URL prefirmato utilizzando la console di Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco Bucket per uso generico scegli il nome del bucket per uso generico contenente l'oggetto per cui desideri ottenere un URL prefirmato.
4. Nell'elenco Objects (Oggetti), seleziona l'oggetto per cui desideri creare un URL prefirmato.
5. Nel menu Operazioni oggetti, scegli Crea URL prefirmato.
6. Specifica per quanto tempo desideri che l'URL prefirmato sia valido.
7. Scegli Create presigned URL (Crea URL prefirmato).
8. Quando viene visualizzata la conferma, l'URL viene automaticamente copiato negli appunti. Verrà visualizzato un pulsante per copiare l'URL preimpostato qualora fosse necessario copiarlo di nuovo.

Utilizzo di AWS CLI

Il seguente AWS CLI comando di esempio genera un URL prefirmato per la condivisione di un oggetto da un bucket Amazon S3. Quando si utilizza il AWS CLI, il tempo massimo di scadenza per un URL prefirmato è di 7 giorni dal momento della creazione. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800
```

Il parametro `--expires-in` specifica il tempo di scadenza in secondi.

 Note

Per tutti Regioni AWS quelli lanciati dopo il 20 marzo 2019 è necessario specificare Regione AWS con `endpoint-url` e con la richiesta. Per un elenco degli endpoint e delle Regioni Amazon S3 disponibili, consulta [Regioni ed endpoint](#) in Riferimenti generali AWS .

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

Per ulteriori informazioni, consulta [presign](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo di AWS SDK

È possibile generare un URL prefirato a livello di codice utilizzando gli SDK. AWS

Python

Il seguente script Python genera un URL prefirato GET per la condivisione di un oggetto.

1. Copia il contenuto dello script e salvalo come file «». *get-only-url.py* Per utilizzare gli esempi seguenti, *user input placeholders* sostituiscili con le tue informazioni (come il nome del file).

```
import argparse
import boto3
from botocore.exceptions import ClientError

def generate_presigned_url(s3_client, client_method, method_parameters,
    expires_in):
    """
    Generate a presigned Amazon S3 URL that can be used to perform an action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
```

```

        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
    except ClientError:
        print(f"Couldn't get a presigned URL for client method
'{client_method}'.")
        raise
    return url

def main():
    parser = argparse.ArgumentParser()
    parser.add_argument("bucket", help="The name of the bucket.")
    parser.add_argument(
        "key", help="The key (path and filename) in the S3 bucket.",
    )
    args = parser.parse_args()

    # By default, this will use credentials from ~/.aws/credentials
    s3_client = boto3.client("s3")

    # The presigned URL is specified to expire in 1000 seconds
    url = generate_presigned_url(
        s3_client,
        "get_object",
        {"Bucket": args.bucket, "Key": args.key},
        1000
    )
    print(f"Generated GET presigned URL: {url}")

if __name__ == "__main__":
    main()

```

2. Per generare un URL prefirato GET per la condivisione di un file, esegui lo script seguente con il nome del bucket e il percorso dell'oggetto desiderato.

Il seguente comando utilizza valori di esempio. Sostituisci *user input placeholders* con le informazioni appropriate.

```
python get-only-url.py amzn-s3-demo-bucket <object-path>
```

Lo script produrrà un URL prefirato GET:


```
Generated GET presigned URL: https://amzn-s3-demo-bucket.s3.amazonaws.com/object.txt?AWS  
AccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=vjbyNxybdZaMmLa  
%2ByT372YEAiv4%3D&Expires=1741978496
```

3. È possibile scaricare il file utilizzando l'URL prefirmato generato con curl:

```
curl -X GET "generated-presigned-url" -o "path/to/save/file"
```

Per altri esempi di utilizzo degli AWS SDK per generare un URL prefirmato per la condivisione di un oggetto, consulta [Creare un URL prefirmato per Amazon S3 utilizzando un SDK. AWS](#)

 Note

Per tutti i modelli Regioni AWS lanciati dopo il 20 marzo 2019, è necessario specificare la e con la endpoint-url richiesta. Regione AWS Per un elenco degli endpoint e delle Regioni Amazon S3 disponibili, consulta [Regioni ed endpoint](#) in Riferimenti generali AWS .

 Note

Quando si utilizzano gli AWS SDK, l'attributo Tagging deve essere un'intestazione e non un parametro di query. Tutti gli altri attributi possono essere passati come parametri per l'URL prefirmato.

Utilizzo di AWS Toolkit for Visual Studio (Windows)

 Note

Al momento, non AWS Toolkit for Visual Studio supporta Visual Studio per Mac.

1. Installa AWS Toolkit for Visual Studio utilizzando le seguenti istruzioni, [Installazione e configurazione del Toolkit per Visual Studio](#) nella Guida per l'AWS Toolkit for Visual Studio utente.

2. Connettiti a AWS utilizzando i seguenti passaggi, [Connessione a AWS](#) nella Guida per l'AWS Toolkit for Visual Studio utente.
3. Nel pannello laterale sinistro denominato AWS Explorer, apri il bucket contenente il tuo oggetto.
4. Apri il menu contestuale dell'oggetto per il quale desideri che venga generato un URL prefirato e seleziona Crea URL... Pre-Signed .
5. Nella finestra a comparsa, imposta la data e l'ora di scadenza dell'URL prefirato.
6. La Chiave dell'oggetto dovrebbe essere precompilata in base all'oggetto selezionato.
7. Scegli GET per specificare che questo URL prefirato verrà utilizzato per scaricare un oggetto.
8. Scegli il pulsante Genera.
9. Per copiare l'URL negli appunti, scegliere Copia.
10. Per utilizzare l'URL generato, incolla l'URL in un qualsiasi browser.

Utilizzo AWS Toolkit for Visual Studio Code

Se utilizzi Visual Studio Code, puoi generare un URL prefirato per condividere un oggetto senza scrivere codice tramite AWS Toolkit for Visual Studio Code. Per ulteriori informazioni, consulta [AWS Toolkit for Visual Studio Code](#) nella Guida per l'utente di AWS Toolkit for Visual Studio Code .

Per istruzioni su come installare il AWS Toolkit for Visual Studio Code, vedere [Installazione di AWS Toolkit for Visual Studio Code](#) nella Guida per l'AWS Toolkit for Visual Studio Code utente.

1. Effettuare la connessione a AWS utilizzando la procedura seguente, [Connessione a AWS Toolkit for Visual Studio Code](#) nella Guida per AWS Toolkit for Visual Studio Code l'utente.
2. Seleziona il AWS logo nel pannello di sinistra in Visual Studio Code.
3. In EXPLORER, seleziona S3.
4. Scegli un bucket e un file e apri il menu contestuale (tasto destro del mouse).
5. Scegli Genera URL prefirato, quindi imposta l'ora di scadenza (in minuti).
6. Premi Invio e l'URL prefirato verrà copiato negli appunti.

Caricamento di oggetti con URL prefirati

Puoi utilizzare gli URL prefirati per consentire a qualcuno di caricare un oggetto nel tuo bucket Amazon S3. L'utilizzo di un URL prefirato consentirà il caricamento senza che un'altra parte disponga di credenziali o autorizzazioni AWS di sicurezza. Le funzionalità dell'URL prefirato sono

limitate dalle autorizzazioni dell'utente che lo ha creato. In altre parole, se si riceve un URL prefirato per caricare un oggetto, è possibile caricarlo solo se il creatore dell'URL dispone delle autorizzazioni necessarie per caricare tale oggetto.

Quando carichi un oggetto nel bucket utilizzando l'URL, Amazon S3 crea l'oggetto in un bucket specifico. Se nel bucket esiste già un oggetto con la stessa chiave specificata nell'URL prefirato, Amazon S3 sostituisce l'oggetto esistente con l'oggetto caricato. Dopo il caricamento, il proprietario del bucket sarà il proprietario dell'oggetto.

Per ulteriori informazioni sugli URL prefirati, consulta [Download e caricamento di oggetti con URL prefirati](#).

Genera un URL prefirato per un oggetto senza scrivere alcun codice mediante AWS Explorer per Visual Studio. È possibile generare un URL prefirato in modo programmatico utilizzando AWS SDK.

Note

Al momento, AWS Toolkit for Visual Studio non supporta Visual Studio per Mac.

Utilizzo di AWS Toolkit for Visual Studio (Windows)

1. Installa AWS Toolkit for Visual Studio utilizzando le seguenti istruzioni, [Installazione e configurazione del Toolkit per Visual Studio](#) nella Guida per l'AWS Toolkit for Visual Studio utente.
2. Connettiti a AWS utilizzando i seguenti passaggi, [Connessione a AWS](#) nella Guida per l'AWS Toolkit for Visual Studio utente.
3. Nel pannello laterale sinistro denominato AWS Explorer, apri il menu contestuale del bucket in cui desideri caricare un oggetto.
4. Scegli Crea Pre-Signed URL... .
5. Nella finestra a comparsa, imposta la data e l'ora di scadenza dell'URL prefirato.
6. Per Chiave dell'oggetto, imposta il nome del file da caricare. Il file che si sta caricando deve corrispondere esattamente a questo nome. Se nel bucket esiste già un oggetto con la stessa chiave dell'oggetto, Amazon S3 sostituirà l'oggetto esistente con quello appena caricato.
7. Scegli PUT per specificare che questo URL prefirato verrà utilizzato per caricare un oggetto.
8. Scegli il pulsante Genera.
9. Per copiare l'URL negli appunti, scegliere Copia.

10 Per utilizzare questo URL, puoi inviare una richiesta PUT con il comando `curl`. Includi il percorso completo del file e l'URL prefirmando stesso.

```
curl -X PUT -T "/path/to/file" "presigned URL"
```

Utilizzo di AWS SDK per generare un URL **prefirmato** PUT per caricare un file

È possibile generare un URL prefirmando in grado di eseguire un'azione S3 per un periodo di tempo limitato.

Note

Se utilizzi la AWS CLI o gli AWS SDK, la data di scadenza per gli URL prefirmando può essere impostata fino a 7 giorni. Per ulteriori informazioni, consulta [Scadenza degli URL prefirmando](#).

Python

Il seguente script Python genera un URL prefirmando PUT per caricare un oggetto in un bucket per uso generico S3.

1. Copia il contenuto dello script e salvalo come file «». *put-only-url.py* Per utilizzare gli esempi seguenti, sostituiscili *user input placeholders* con le tue informazioni (ad esempio il nome del file).

```
import argparse
import boto3
from botocore.exceptions import ClientError

def generate_presigned_url(s3_client, client_method, method_parameters,
    expires_in):
    """
    Generate a presigned Amazon S3 URL that can be used to perform an action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds the presigned URL is valid for.
    :return: The presigned URL.
    """
```

```

    try:
        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
    except ClientError:
        print(f"Couldn't get a presigned URL for client method
'{client_method}'.")
        raise
    return url

def main():
    parser = argparse.ArgumentParser()
    parser.add_argument("bucket", help="The name of the bucket.")
    parser.add_argument(
        "key", help="The key (path and filename) in the S3 bucket.",
    )
    parser.add_argument(
        "--region", help="The AWS region where the bucket is located.",
        default="us-east-1"
    )
    parser.add_argument(
        "--content-type", help="The content type of the file to upload.",
        default="application/octet-stream"
    )
    args = parser.parse_args()

    # Create S3 client with explicit region configuration
    s3_client = boto3.client("s3", region_name=args.region)

    # Optionally set signature version if needed for older S3 regions
    # s3_client.meta.config.signature_version = 's3v4'

    # The presigned URL is specified to expire in 1000 seconds
    url = generate_presigned_url(
        s3_client,
        "put_object",
        {
            "Bucket": args.bucket,
            "Key": args.key,
            "ContentType": args.content_type # Specify content type
        },
        1000
    )

```

```
)  
print(f"Generated PUT presigned URL: {url}")  
  
if __name__ == "__main__":  
    main()
```

2. Per generare un URL prefirato PUT per il caricamento di un file, esegui lo script seguente con il nome del bucket e il percorso dell'oggetto desiderato.

Il seguente comando utilizza valori di esempio. Sostituisci *user input placeholders* con le informazioni appropriate.

```
python put-only-url.py amzn-s3-demo-bucket <object-path> --region us-east-1 --  
content-type application/octet-stream
```

Lo script produrrà un URL prefirato PUT:

```
Generated PUT presigned URL: https://amzn-s3-demo-  
bucket.s3.amazonaws.com/object.txt?AWS  
AccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=vjbyNxybdZaMmLa  
%2ByT372YEAiv4%3D&Expires=1741978496
```

3. È ora possibile caricare il file utilizzando l'URL prefirato generato con curl. Assicurati di includere lo stesso tipo di contenuto utilizzato durante la generazione dell'URL:

```
curl -X PUT -T "path/to/your/local/file" -H "Content-Type: application/octet-  
stream" "generated-presigned-url"
```

Se hai specificato un tipo di contenuto diverso durante la generazione dell'URL, assicurati di utilizzare lo stesso tipo di contenuto nel comando curl.

Per altri esempi di utilizzo degli AWS SDK per generare un URL prefirato per caricare un oggetto, consulta [Creare un URL prefirato per Amazon S3 utilizzando un SDK. AWS](#)

Risoluzione degli errori SignatureDoesNotMatch

Se riscontri un errore SignatureDoesNotMatch durante l'utilizzo di URL prefirati, verifica quanto segue:

- Verifica che l'ora di sistema sia sincronizzata con un server di riferimento dell'ora affidabile
- Assicurati di utilizzare l'URL esattamente come generato, senza alcuna modifica
- Controlla se l'URL è scaduto e generane uno nuovo se necessario
- Assicurati che il tipo di contenuto nella richiesta di caricamento corrisponda al tipo di contenuto specificato durante la generazione dell'URL
- Verifica di utilizzare la Regione corretta per il bucket
- Quando utilizzi curl, racchiudi l'URL tra virgolette per gestire correttamente i caratteri speciali

Trasformazione di oggetti con S3 Object Lambda

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner APN (Partner Network). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

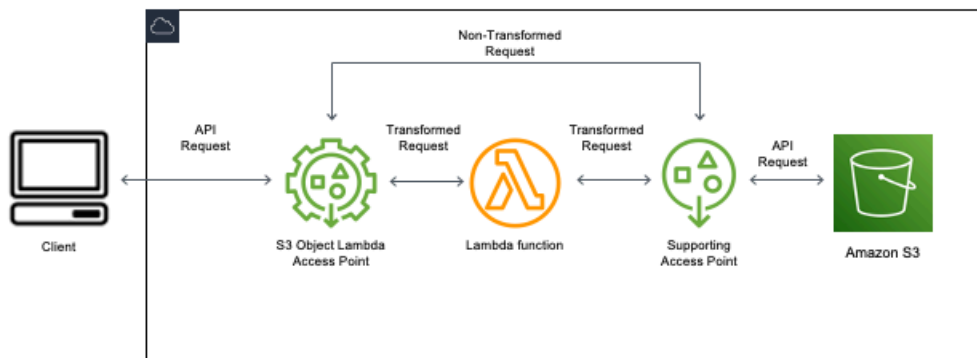
Con Lambda per oggetti Amazon S3, è possibile aggiungere il proprio codice alle richieste di Amazon S3 GET, LIST e HEAD per modificare ed elaborare i dati mentre vengono restituiti a un'applicazione. Puoi utilizzare il codice personalizzato per modificare i dati restituiti dalle richieste GET S3 standard per filtrare le righe, ridimensionare e applicare la filigrana alle immagini in modo dinamico, oscurare i dati riservati e molto altro. Puoi anche utilizzare S3 Object Lambda per modificare l'output delle richieste LIST S3 per creare una vista personalizzata di tutti gli oggetti in un bucket e delle richieste HEAD S3 per modificare i metadati degli oggetti come il nome e la dimensione dell'oggetto. Puoi utilizzare S3 Object Lambda come origine per la tua CloudFront distribuzione Amazon per personalizzare i dati per gli utenti finali, ad esempio il ridimensionamento automatico delle immagini, la transcodifica di formati più vecchi (come da JPEG a WebP) o l'eliminazione dei metadati. Per ulteriori informazioni, consulta il post sul blog [Use Amazon S3 Object Lambda with Amazon CloudFront](#). Basato sulle funzioni AWS Lambda, il codice viene eseguito su un'infrastruttura completamente gestita da AWS. L'utilizzo di S3 Object Lambda riduce la necessità di creare e archiviare copie derivate dei dati o di eseguire proxy senza dover modificare le applicazioni.

Come funziona S3 Object Lambda

S3 Object Lambda utilizza AWS Lambda funzioni per elaborare automaticamente l'output di S3 o richieste GET standard. LIST HEAD AWS Lambda è un servizio di elaborazione serverless che esegue codice definito dal cliente senza richiedere la gestione delle risorse di calcolo sottostanti. Puoi creare ed eseguire le funzioni Lambda personalizzate, adattando la trasformazione dei dati a casi d'uso specifici.

Dopo averla configurata, puoi collegare una funzione Lambda a un endpoint del servizio Lambda per oggetti S3, noto come punto di accesso Lambda per oggetti. Per accedere ai dati, il punto di accesso Lambda per oggetti utilizza un punto di accesso S3 standard, noto come punto di accesso di supporto.

Quando invii una richiesta al punto di accesso Lambda per oggetti, Amazon S3 richiama automaticamente la funzione Lambda. Tutti i dati recuperati utilizzando una richiesta S3 GET, LIST o HEAD tramite il punto di accesso Lambda per oggetti restituirà un risultato trasformato all'applicazione. Tutte le altre richieste vengono elaborate normalmente, come illustrato nel diagramma seguente.



Gli argomenti in questa sezione descrivono come utilizzare S3 Object Lambda.

Argomenti

- [Creazione di punti di accesso Object Lambda](#)

- [Utilizzo dei punti di accesso Amazon S3 Object Lambda](#)
- [Considerazioni sulla sicurezza per i punti di accesso S3 Object Lambda](#)
- [Scrittura di funzioni Lambda per i punti di accesso Lambda per oggetti S3](#)
- [Utilizzo AWS funzioni Lambda integrate](#)
- [Best practice e linee guida per Lambda per oggetti S3](#)
- [Tutorial di Lambda per oggetti S3](#)
- [Debug e risoluzione dei problemi di Lambda per oggetti S3](#)

Creazione di punti di accesso Object Lambda

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner APN (Partner Network). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Un punto di accesso Lambda per oggetti è associato esattamente a un punto di accesso standard, che si specifica durante la creazione. Per creare un punto di accesso Lambda per oggetti, sono necessarie le seguenti risorse:

- Un punto di accesso S3 standard. Quando utilizzi i punti di accesso Lambda per oggetti, il punto di accesso standard è noto come punto di accesso di supporto ed è collegato a un bucket S3 o a un volume Amazon FSx per OpenZFS. Per informazioni sulla creazione di punti di accesso standard, consulta la sezione [the section called “Creazione di un access point”](#).
- Una funzione. AWS Lambda. Puoi creare una funzione Lambda personalizzata oppure utilizzare una funzione predefinita. Per ulteriori informazioni sulla creazione delle funzioni Lambda, consulta [the section called “Scrittura delle funzioni Lambda”](#). Per ulteriori informazioni sulle funzioni incorporate, consulta [Utilizzo AWS funzioni Lambda integrate](#).
- (Facoltativo) Una policy AWS Identity and Access Management (IAM). I punti di accesso Amazon S3 supportano le policy delle risorse IAM che consentono di controllare l'utilizzo del punto di accesso per risorsa, utente o altre condizioni. Per ulteriori informazioni sulla creazione di queste policy, consulta [the section called “Configurazione delle policy IAM”](#).

Nelle sezioni seguenti viene descritto come creare un punto di accesso Lambda per oggetti utilizzando:

- Le Console di gestione AWS
- Il AWS Command Line Interface (AWS CLI)
- Un AWS CloudFormation modello
- Il AWS Cloud Development Kit (AWS CDK)

Per ulteriori informazioni su come creare un punto di accesso Lambda per oggetti tramite REST API, consulta [CreateAccessPointForObjectLambda](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Creazione di un punto di accesso Lambda per oggetti

Utilizza una delle procedure riportate di seguito per creare il punto di accesso Lambda per oggetti.

Utilizzo della console S3

Per creare un punto di accesso Lambda per oggetti utilizzando la console

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione a cui passare.
3. Nel riquadro di navigazione sinistro, scegli Punti di accesso Lambda dell'oggetto.
4. Nella pagina Punti di accesso Lambda dell'oggetto, scegli Crea punto di accesso per le espressioni Lambda dell'oggetto.
5. In Object Lambda Access Point name (Nome punto di accesso Object Lambda), specifica il nome da utilizzare per il punto di accesso.

Come per i punti di accesso standard, esistono regole per la denominazione dei punti di accesso Lambda per oggetti. Per ulteriori informazioni, consulta [Regole di denominazione dei punti di accesso](#).

6. In Supporting Access Point (Punto di accesso di supporto), specifica o seleziona il punto di accesso standard da utilizzare. Il punto di accesso deve trovarsi nello Regione AWS stesso oggetto da trasformare. Per informazioni sulla creazione di punti di accesso standard, consulta la sezione [the section called "Creazione di un access point"](#).

7. In Configurazione della trasformazione puoi aggiungere una funzione che trasforma i dati per il punto di accesso Lambda per oggetti. Esegui una delle seguenti operazioni:
- Se hai già una AWS Lambda funzione nel tuo account, puoi sceglierla in **Invoke Lambda function**. Qui puoi inserire l'Amazon Resource Name (ARN) di una funzione Lambda nella tua Account AWS o scegliere una funzione Lambda dal menu a discesa.
 - Se desideri utilizzare una funzione AWS integrata, scegli il nome della funzione in **Funzione AWS integrata** e seleziona **Crea funzione Lambda**. Verrai indirizzato alla console Lambda dove potrai implementare una funzione integrata nel tuo Account AWS. Per ulteriori informazioni sulle funzioni integrate, consulta [Utilizzo AWS funzioni Lambda integrate](#).

In S3 APIs (API S3), scegli una o più operazioni API da richiamare. Per ogni API selezionata, devi specificare una funzione Lambda da richiamare.

8. (Facoltativo) In **Payload**, aggiungi il testo JSON da fornire come input alla funzione Lambda. Puoi configurare payload con parametri diversi per diversi punti di accesso Lambda per oggetti che invocano la stessa funzione Lambda, estendendo così la flessibilità della funzione stessa.

 Important

Quando utilizzi i punti di accesso Lambda per oggetti, assicurati che il payload non contenga informazioni riservate.

9. (Facoltativo) In **Range and part number** (Intervallo e numero parte), devi abilitare l'opzione se vuoi elaborare le richieste GET e HEAD con intestazioni di intervallo e numero di parte. Selezionando questa opzione confermi che la funzione Lambda è in grado di riconoscere ed elaborare queste richieste. Per ulteriori informazioni sulle intestazioni di intervalli e numeri di parte, consulta [Lavorare con Intervallo and Numero del pezzo headers](#).
10. (Facoltativo) In **Parametri di richiesta** seleziona **Abilita** o **Disabilita** per aggiungere il monitoraggio Amazon S3 al punto di accesso Lambda per oggetti. Le metriche delle richieste vengono fatturate alla tariffa standard di Amazon CloudWatch.
11. (Facoltativo) In **Object Lambda Access Point policy** (Policy punto di accesso Object Lambda), imposta una policy delle risorse. Le policy delle risorse concedono le autorizzazioni per il punto di accesso Lambda per oggetti specificato e possono controllare l'utilizzo del punto di accesso per risorsa, utente o altre condizioni. Per ulteriori informazioni sulle policy delle risorse per i punti di accesso Object Lambda, consulta [Configurazione delle policy IAM per i punti di accesso Lambda per oggetti](#).

12. In Block Public Access settings for this Object Lambda Access Point (Impostazioni blocco accesso pubblico per questo punto di accesso Object Lambda), seleziona le impostazioni di Blocco dell'accesso pubblico Amazon S3 da applicare al punto di accesso. Tutte le impostazioni di blocco dell'accesso pubblico sono abilitate per impostazione predefinita per i nuovi punti di accesso Object Lambda. È consigliabile non modificare questa impostazione predefinita. Amazon S3 attualmente non supporta la modifica delle impostazioni di blocco dell'accesso pubblico dei punti di accesso dopo la creazione del punto di accesso Object Lambda.

Per ulteriori informazioni sull'utilizzo del blocco dell'accesso pubblico in Amazon S3, consulta [Gestione dell'accesso pubblico ai punti di accesso per bucket per uso generico](#).

13. Seleziona Create Object Lambda Access Point (Crea punto di accesso Object Lambda).

Utilizzo di AWS CLI

Per creare un Object Lambda Access Point utilizzando un AWS CloudFormation modello

 Note

Per utilizzare i seguenti comandi, sostituisci *user input placeholders* con le tue specifiche informazioni.

1. Scarica il pacchetto di distribuzione delle AWS Lambda funzioni nella configurazione predefinita di `s3objectlambda_deployment_package.zip` [S3 Object Lambda](#).
2. Esegui il seguente comando `put-object` per caricare il pacchetto in un bucket Amazon S3.

```
aws s3api put-object --bucket Amazon S3 bucket name --key  
s3objectlambda_deployment_package.zip --body release/  
s3objectlambda_deployment_package.zip
```

3. Scarica il AWS CloudFormation modello nella configurazione predefinita di `s3objectlambda_defaultconfig.yaml` [S3 Object Lambda](#).
4. Esegui il seguente comando `deploy` per implementare il modello nell' Account AWS in uso.

```
aws cloudformation deploy --template-file s3objectlambda_defaultconfig.yaml \
  --stack-name CloudFormation stack name \
  --parameter-overrides ObjectLambdaAccessPointName=Object Lambda Access Point name \
```

```
SupportingAccessPointName=Amazon S3 access point S3BucketName=Amazon S3 bucket \  
LambdaFunctionS3BucketName=Amazon S3 bucket containing your Lambda package \  
LambdaFunctionS3Key=Lambda object key LambdaFunctionS3ObjectVersion=Lambda object  
version \  
LambdaFunctionRuntime=Lambda function runtime --capabilities capability_IAM
```

Puoi configurare questo AWS CloudFormation modello per richiamare le operazioni Lambda per GETHEAD, e API. LIST Per ulteriori informazioni sulla modifica della configurazione predefinita del modello, consulta [the section called “Automatizza la configurazione di S3 Object Lambda con AWS CloudFormation”](#).

Per creare un Object Lambda Access Point utilizzando AWS CLI

 Note

Per utilizzare i seguenti comandi, sostituisci *user input placeholders* con le tue specifiche informazioni.

Nell'esempio seguente viene creato un punto di accesso Lambda per oggetti denominato *my-object-lambda-ap* per il bucket *amzn-s3-demo-bucket1* nell'account *111122223333*. L'esempio presuppone che sia già stato creato un punto di accesso standard denominato *example-ap*. Per informazioni sulla creazione di un punto di accesso standard, consulta la sezione [the section called “Creazione di un access point”](#).

Questo esempio utilizza la funzione AWS predefinita. *decompress* Per ulteriori informazioni sulle funzioni incorporate, consulta [the section called “Utilizzo di funzioni AWS integrate”](#).

1. Creare un bucket. In questo esempio verrà utilizzato *amzn-s3-demo-bucket1*. Per ulteriori informazioni sulla creazione dei bucket, consulta la sezione [the section called “Creazione di un bucket per uso generico”](#).
2. Creare un punto di accesso standard e collegarlo al bucket. In questo esempio verrà utilizzato *example-ap*. Per informazioni sulla creazione di punti di accesso standard, consulta la sezione [the section called “Creazione di un access point”](#).
3. Esegui una delle seguenti operazioni:
 - Crea una funzione Lambda nel tuo account da utilizzare per trasformare l'oggetto Amazon S3. Per ulteriori informazioni sulla creazione delle funzioni Lambda, consulta [the section called](#)

[“Scrittura delle funzioni Lambda”](#). Per utilizzare la tua funzione personalizzata con AWS CLI, consulta [Using Lambda with the AWS CLI](#) nella AWS Lambda Developer Guide.

- Usa una funzione AWS Lambda predefinita. Per ulteriori informazioni sulle funzioni incorporate, consulta [Utilizzo AWS funzioni Lambda integrate](#).
4. Crea un file di configurazione JSON denominato `my-olap-configuration.json`. In questa configurazione, fornisci il punto di accesso di supporto e il nome della risorsa Amazon (ARN) per la funzione Lambda creata nei passaggi precedenti o l'ARN per la funzione predefinita che stai utilizzando.

Example

```
{
  "SupportingAccessPoint" : "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
  "TransformationConfigurations": [{
    "Actions" : ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
    "ContentTransformation" : {
      "AwsLambda": {
        "FunctionPayload" : "{\"compressionType\":\"gzip\"}",
        "FunctionArn" : "arn:aws:lambda:us-east-1:111122223333:function/
compress"
      }
    }
  }]
}
```

5. Esegui il comando `create-access-point-for-object-lambda` per creare il punto di accesso Lambda per oggetti.

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-ap --configuration file://my-olap-configuration.json
```

6. (Facoltativo) Crea un file di policy JSON denominato `my-olap-policy.json`.

L'aggiunta di una policy delle risorse per il punto di accesso Object Lambda può controllare l'utilizzo del punto di accesso per risorsa, utente o altre condizioni. Questa policy delle risorse concede l'autorizzazione `GetObject` per l'account `444455556666` al punto di accesso Lambda per oggetti specificato.

Example

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "Grant account 444455556666 GetObject access",
      "Effect": "Allow",
      "Action": "s3-object-lambda:GetObject",
      "Principal": {
        "AWS": "arn:aws:iam::444455556666:root"
      },
      "Resource": "your-object-lambda-access-point-arn"
    }
  ]
}
```

7. (Facoltativo) Esegui il comando `put-access-point-policy-for-object-lambda` per impostare la policy delle risorse.

```
aws s3control put-access-point-policy-for-object-lambda --account-id 111122223333
--name my-object-lambda-ap --policy file://my-olap-policy.json
```

8. (Facoltativo) Specifica un payload.

Un payload è un JSON opzionale che puoi fornire alla tua AWS Lambda funzione come input. Puoi configurare payload con parametri diversi per diversi punti di accesso Lambda per oggetti che invocano la stessa funzione Lambda, estendendo così la flessibilità della funzione stessa.

La seguente configurazione del punto di accesso Lambda per oggetti mostra un payload con due parametri.

```
{
  "SupportingAccessPoint": "AccessPointArn",
  "CloudWatchMetricsEnabled": false,
  "TransformationConfigurations": [{
    "Actions": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
    "ContentTransformation": {
      "AwsLambda": {
        "FunctionArn": "FunctionArn",
        "FunctionPayload": "{\"res-x\": \"100\", \"res-y\": \"100\"}"
      }
    }
  ]
}
```

```

    }
  }
}]
}

```

La seguente configurazione del punto di accesso Lambda per oggetti mostra un payload con un parametro e con `GetObject-Range`, `GetObject-PartNumber`, `HeadObject-Range` e `HeadObject-PartNumber` abilitati.

```

{
  "SupportingAccessPoint": "AccessPointArn",
  "CloudWatchMetricsEnabled": false,
  "AllowedFeatures": ["GetObject-Range", "GetObject-PartNumber", "HeadObject-Range", "HeadObject-PartNumber"],
  "TransformationConfigurations": [{
    "Action": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
    "ContentTransformation": {
      "AwsLambda": {
        "FunctionArn": "FunctionArn",
        "FunctionPayload": "{\"compression-amount\": \"5\"}"
      }
    }
  }]
}

```

Important

Quando utilizzi i punti di accesso Lambda per oggetti, assicurati che il payload non contenga informazioni riservate.

Utilizzo di AWS CloudFormation console e modello

È possibile creare un punto di accesso Lambda per oggetti utilizzando la configurazione predefinita fornita da Amazon S3. È possibile scaricare un AWS CloudFormation modello e il codice sorgente della funzione Lambda dal [GitHub repository](#) e distribuire queste risorse per configurare un Object Lambda Access Point funzionale.

Per informazioni sulla modifica della configurazione predefinita del AWS CloudFormation modello, consulta [the section called “Automatizza la configurazione di S3 Object Lambda con AWS CloudFormation”](#)

Per informazioni sulla configurazione degli access point Object Lambda utilizzando CloudFormation senza il modello, consulta [AWS::S3ObjectLambda::AccessPoint](#) la Guida per l'AWS CloudFormation utente.

Per caricare il pacchetto di implementazione della funzione Lambda

1. Scarica il pacchetto `s3objectlambda_deployment_package.zip` di distribuzione delle AWS Lambda funzioni nella configurazione predefinita di [S3 Object Lambda](#).
2. Carica il pacchetto in un bucket Amazon S3

Per creare un Access Point Object Lambda utilizzando AWS CloudFormation console

1. Scarica il AWS CloudFormation modello nella configurazione `s3objectlambda_defaultconfig.yaml` predefinita di [S3 Object Lambda](#).
2. Accedi alla console di AWS gestione e apri la AWS CloudFormation console all'indirizzo. <https://console.aws.amazon.com/cloudformation>
3. Esegui una delle seguenti operazioni:
 - Se non l'hai mai usato AWS CloudFormation prima, nella AWS CloudFormation home page, scegli Crea stack.
 - Se l'hai già AWS CloudFormation usato, nel riquadro di navigazione a sinistra, scegli Stacks. Scegli Create stack (Crea stack), quindi With new resources (standard) Con nuove risorse (standard).
4. Per Prerequisito - Prepara modello, scegliere Il modello è pronto.
5. In Specify template (Specifica modello), scegli Upload a template file (Carica un file modello), quindi carica `s3objectlambda_defaultconfig.yaml`.
6. Scegli Avanti.
7. Nella pagina Specifica dettagli della pila, immetti un nome per la pila.
8. Nella sezione Parameters (Parametri), specifica i seguenti parametri definiti nel modello dello stack:
 - a. Per `CreateNewSupportingAccessPoint`, esegui una delle seguenti operazioni:

- Se disponi già di un punto di accesso di supporto per il bucket S3 in cui hai caricato il modello, scegli `false`.
 - Se intendi creare un nuovo punto di accesso per questo bucket, scegli `true`.
- b. Per `EnableCloudWatchMonitoring`, scegli `true` o `false`, a seconda che desideri abilitare le metriche e gli allarmi delle CloudWatch richieste di Amazon.
- c. (Facoltativo) Per `LambdaFunctionPayload`, aggiungi il testo JSON che desideri fornire alla tua funzione Lambda come input. Puoi configurare payload con parametri diversi per diversi punti di accesso Lambda per oggetti che invocano la stessa funzione Lambda, estendendo così la flessibilità della funzione stessa.

 Important

Quando utilizzi i punti di accesso Lambda per oggetti, assicurati che il payload non contenga informazioni riservate.

- d. Per `LambdaFunctionRuntime`, inserisci il tuo runtime preferito per la funzione Lambda. Le scelte disponibili sono `nodejs14.x`, `python3.9`, `java11`.
- e. Per `LambdaFunctionS3BucketName`, inserisci il nome del bucket Amazon S3 in cui hai caricato il pacchetto di distribuzione.
- f. Per `LambdaFunctionS3Key`, inserisci la chiave oggetto Amazon S3 su cui hai caricato il pacchetto di distribuzione.
- g. Per `LambdaFunctionS3ObjectVersion`, inserisci la versione dell'oggetto Amazon S3 in cui hai caricato il pacchetto di distribuzione.
- h. Per `ObjectLambdaAccessPointName`, inserisci un nome per il tuo Access Point Object Lambda.
- i. Per `S3BucketName`, inserisci il nome del bucket Amazon S3 che verrà associato al tuo Access Point Object Lambda.
- j. Per `SupportingAccessPointName`, inserisci il nome del punto di accesso di supporto.

 Note

Questo è un punto di accesso associato al bucket Amazon S3 scelto nel passaggio precedente. Se non hai punti di accesso associati al tuo bucket Amazon S3,

puoi configurare il modello in modo da crearne uno per te scegliendo `true` for `CreateNewSupportingAccessPoint`

9. Scegli Avanti.
10. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).

Per ulteriori informazioni sulle impostazioni facoltative in questa pagina, consulta la sezione [Impostazione delle opzioni dello stack AWS CloudFormation](#) nella Guida per l'utente di AWS CloudFormation .

11. Nella pagina Revisione, scegliere Crea pila.

Utilizzo di AWS Cloud Development Kit (AWS CDK)

Per ulteriori informazioni sulla configurazione degli access point Object Lambda utilizzando [AWS::S3ObjectLambda Construct Library](#) nell' AWS CDK API Reference. AWS Cloud Development Kit (AWS CDK)

Automatizza la configurazione di S3 Object Lambda con un modello CloudFormation

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner Partner Network (APN). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Puoi utilizzare un AWS CloudFormation modello per creare rapidamente un Access Point Amazon S3 Object Lambda. Il CloudFormation modello crea automaticamente le risorse pertinenti, configura i ruoli AWS Identity and Access Management (IAM) e imposta una AWS Lambda funzione che gestisce automaticamente le richieste tramite l'Access Point Object Lambda. Con il CloudFormation modello, puoi implementare le migliori pratiche, migliorare il tuo livello di sicurezza e ridurre gli errori causati dai processi manuali.

Questo [GitHub repository](#) contiene il codice sorgente del CloudFormation modello e della funzione Lambda. Per istruzioni su come utilizzare il modello, consulta [the section called “Creazione di punti di accesso Object Lambda”](#).

La funzione Lambda fornita nel modello non esegue alcuna trasformazione. Restituisce invece gli oggetti così come sono dall'origine dati sottostante. È possibile clonare la funzione e aggiungere il proprio codice di trasformazione per modificare ed elaborare i dati man mano che vengono restituiti ad un'applicazione. Per ulteriori informazioni sulla modifica della funzione, consulta [the section called “Modifica della funzione Lambda”](#) e [the section called “Scrittura delle funzioni Lambda”](#).

Modificare il modello

Creazione di un nuovo punto di accesso di supporto

Lambda per oggetti S3 utilizza due punti di accesso, un punto di accesso Lambda per oggetti e un punto di accesso S3 standard, denominato punto di accesso di supporto. Quando effettui una richiesta a un punto di accesso Lambda per oggetti, S3 invoca Lambda per tuo conto o delega la richiesta al punto di accesso di supporto, a seconda della configurazione di Lambda per oggetti S3. È possibile creare un nuovo punto di accesso di supporto passando il seguente parametro come parte del comando `aws cloudformation deploy` durante l'implementazione del modello.

```
CreateNewSupportingAccessPoint=true
```

Configurazione di un payload di funzione

È possibile configurare un payload per fornire dati supplementari alla funzione Lambda passando il seguente parametro come parte del comando `aws cloudformation deploy` al momento dell'implementazione del modello.

```
LambdaFunctionPayload="format=json"
```

Abilitazione del monitoraggio di Amazon CloudWatch

Puoi abilitare il CloudWatch monitoraggio passando il seguente parametro come parte del `aws cloudformation deploy` comando durante la distribuzione del modello.

```
EnableCloudWatchMonitoring=true
```

Questo parametro abilita le metriche di richiesta dell'Object Lambda Access Point per Amazon S3 e crea due CloudWatch allarmi per monitorare gli errori lato client e lato server.

 Note

CloudWatch L'utilizzo di Amazon comporterà costi aggiuntivi. Per ulteriori informazioni sulle metriche delle richieste Amazon S3, consulta la sezione [Monitoraggio e registrazione degli access point](#).

Per i dettagli sui prezzi, vedere [Prezzi di CloudWatch](#).

Configurazione della simultaneità fornita

Per ridurre la latenza, è possibile configurare la simultaneità con provisioning per la funzione Lambda che supporta il punto di accesso Lambda per oggetti modificando il modello per includere le seguenti righe in Resources.

```
LambdaFunctionVersion:
  Type: AWS::Lambda::Version
  Properties:
    FunctionName: !Ref LambdaFunction
    ProvisionedConcurrencyConfig:
      ProvisionedConcurrentExecutions: Integer
```

 Note

Saranno applicati costi aggiuntivi la simultaneità con provisioning. Per ulteriori informazioni sulla simultaneità con provisioning, consulta [Gestione della simultaneità con provisioning di Lambda](#) nella Guida per gli sviluppatori di AWS Lambda.

Per i dettagli sui prezzi, vedere [Prezzi di AWS Lambda](#).

Modifica della funzione Lambda

Modifica dei valori di intestazione per una richiesta **GetObject**

Per impostazione predefinita, la funzione Lambda inoltra tutte le intestazioni, eccetto Content-Length ed ETag, dalla richiesta URL prefirmata al client `GetObject`. In base al codice di trasformazione nella funzione Lambda, puoi scegliere di inviare nuovi valori di intestazione al client `GetObject`.

È possibile aggiornare la funzione Lambda per inviare nuovi valori di intestazione passandoli nell'operazione API `WriteGetObjectResponse`.

Ad esempio, se la funzione Lambda traduce il testo negli oggetti Amazon S3 in una lingua diversa, puoi passare un nuovo valore nell'intestazione Content-Language. Puoi fare ciò modificando la funzione `writeResponse` come descritto di seguito.

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
transformedObject: Buffer,
headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
    },
    ...headers,
    ContentLanguage: 'my-new-language'
  }).promise();
}
```

Per un elenco completo delle intestazioni supportate, consulta [WriteGetObjectResponse](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Restituzione di intestazioni di metadati

È possibile aggiornare la funzione Lambda per inviare nuovi valori di intestazione passandoli nella richiesta dell'operazione API [WriteGetObjectResponse](#).

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
transformedObject: Buffer,
headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest,
```

```
    'my-new-header': 'my-new-value'  
  },  
  ...headers  
}).promise();  
}
```

Restituzione di un nuovo codice di stato

È possibile restituire un codice di stato personalizzato al client `GetObject` passandolo nella richiesta dell'operazione API [WriteGetObjectResponse](#).

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,  
  transformedObject: Buffer,  
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {  
  const { algorithm, digest } = getChecksum(transformedObject);  
  
  return s3Client.writeGetObjectResponse({  
    RequestRoute: requestContext.outputRoute,  
    RequestToken: requestContext.outputToken,  
    Body: transformedObject,  
    Metadata: {  
      'body-checksum-algorithm': algorithm,  
      'body-checksum-digest': digest  
    },  
    ...headers,  
    StatusCode: Integer  
  }).promise();  
}
```

Per un elenco completo degli stati supportati, consulta [WriteGetObjectResponse](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Applicazione dei **parametri Range** e `PartNumber` all'oggetto sorgente

Per impostazione predefinita, l'Object Lambda Access Point creato dal CloudFormation modello è in grado di gestire i parametri `Range` e `partNumber`. La funzione Lambda applica l'intervallo o il numero di parte richiesto all'oggetto trasformato. A tale scopo, è necessario scaricare l'intero oggetto ed eseguire la trasformazione. In alcuni casi, gli intervalli di oggetti trasformati potrebbero essere associati esattamente agli intervalli di oggetti fonte. Ciò significa che la richiesta dell'intervallo di byte A-B sull'oggetto sorgente e l'esecuzione della trasformazione potrebbero produrre lo stesso risultato della richiesta dell'intero oggetto, dell'esecuzione della trasformazione e della restituzione dell'intervallo A-B di byte sull'oggetto trasformato.

In questi casi, è possibile modificare l'implementazione della funzione Lambda per applicare l'intervallo o il numero di parte direttamente all'oggetto fonte. Questo approccio riduce la latenza generale della funzione e la memoria richieste. Per ulteriori informazioni, consulta [the section called “Lavorare con Intervallo and Numero del pezzo headers”](#).

Disattivazione della gestione di **Range** e **PartNumber**

Per impostazione predefinita, l'Object Lambda Access Point creato dal CloudFormation modello è in grado di gestire i Range parametri e. partNumber Se questo comportamento non è necessario, è possibile disabilitarlo rimuovendo le seguenti righe dal modello:

AllowedFeatures:

- GetObject-Range
- GetObject-PartNumber
- HeadObject-Range
- HeadObject-PartNumber

Trasformazione di oggetti di grandi dimensioni

Per impostazione predefinita, la funzione Lambda elabora l'intero oggetto in memoria prima di poter avviare lo streaming della risposta a S3 Object Lambda. È possibile modificare la funzione per effettuare lo streaming della risposta mentre esegue la trasformazione. Ciò aiuta a ridurre la latenza della trasformazione e la dimensione della memoria della funzione Lambda. Per un'implementazione esemplificativa, consulta [Streaming esemplificativo del contenuto compresso](#).

Utilizzo dei punti di accesso Amazon S3 Object Lambda

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner Partner Network (APN). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Le richieste tramite gli punti di accesso Lambda per oggetti Amazon S3 si effettuano esattamente come le richieste tramite altri punti di accesso. Per ulteriori informazioni su come effettuare le richieste tramite un punto di accesso, consulta [Utilizzo dei punti di accesso Amazon S3 per bucket per uso generico](#). Puoi effettuare richieste tramite gli access point Object Lambda utilizzando la

console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Important

Il nome della risorsa Amazon (ARN) del punto di accesso Lambda per oggetti utilizza un nome di servizio di `s3-object-lambda`. Quindi, gli ARN degli punti di accesso Lambda per oggetti iniziano con `arn:aws::s3-object-lambda`, anziché `arn:aws::s3`, che viene utilizzato per altri punti di accesso.

Come trovare l'ARN per un punto di accesso Lambda per oggetti

Per utilizzare un Access Point Object Lambda con i AWS CLI nostri AWS SDK, devi conoscere l'Amazon Resource Name (ARN) dell'Access Point Object Lambda. Gli esempi seguenti mostrano come trovare l'ARN di un punto di accesso Lambda per oggetti utilizzando la console Amazon S3 o la AWS CLI.

Utilizzo della console S3

Per trovare l'ARN per un punto di accesso Lambda per oggetti

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Punti di accesso Lambda dell'oggetto.
3. Seleziona il pulsante di opzione accanto al punto di accesso Lambda per oggetti di cui vuoi copiare l'ARN.
4. Scegli Copy ARN (Copia ARN).

Utilizzo di AWS CLI

Per trovare l'ARN del tuo Access Point Object Lambda utilizzando AWS CLI

1. Per recuperare un elenco degli punti di accesso Lambda per oggetti associati al tuo Account AWS, esegui il comando riportato di seguito. Prima di eseguire il comando, sostituisci l'ID dell'account **111122223333** con il tuo Account AWS ID.

```
aws s3control list-access-points-for-object-lambda --account-id 111122223333
```

2. Esamina l'output del comando per trovare l'ARN del punto di accesso Lambda per oggetti che desideri utilizzare. L'output del comando precedente dovrebbe essere simile all'esempio seguente.

```
{
  "ObjectLambdaAccessPointList": [
    {
      "Name": "my-object-lambda-ap",
      "ObjectLambdaAccessPointArn": "arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-object-lambda-ap"
    },
    ...
  ]
}
```

Come utilizzare un alias in stile bucket per il punto di accesso Lambda per oggetti del bucket S3

Quando crei un punto di accesso Lambda per oggetti, Amazon S3 genera automaticamente un alias univoco per il tuo punto di accesso Lambda per oggetti. Puoi utilizzare questo alias del punto di accesso al posto di un nome del bucket Amazon S3 o del nome della risorsa Amazon (ARN) del punto di accesso Lambda per oggetti in una richiesta per qualsiasi operazione del piano dati del punto di accesso. Per un elenco di queste operazioni, consulta [Compatibilità dei punti di accesso](#).

Un nome alias del punto di accesso Lambda per oggetti viene creato nello stesso spazio dei nomi di un bucket Amazon S3. Questo nome alias viene generato automaticamente e non può essere modificato. Per un punto di accesso Lambda per oggetti esistente, l'alias viene assegnato automaticamente. Un nome alias del punto di accesso Lambda per oggetti soddisfa tutti i requisiti di un nome bucket Amazon S3 valido e comprende le seguenti parti:

Object Lambda Access Point name prefix-metadata--o1-s3

Note

Il suffisso `--o1-s3` è riservato ai nomi alias dei punti di accesso Lambda per oggetti e non può essere utilizzato per i nomi dei bucket o dei punti di accesso Lambda per oggetti. Per ulteriori informazioni sulle regole di denominazione dei bucket Amazon S3, consulta [Regole di denominazione dei bucket per uso generico](#).

Negli esempi seguenti viene illustrato l'ARN e l'alias per un punto di accesso Lambda per oggetti denominato *my-object-lambda-access-point*.

- ARN: `arn:aws:s3-object-lambda:region:account-id:accesspoint/my-object-lambda-access-point`
- Alias del punto di accesso Lambda per oggetti: *my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiuse1a--o1-s3*

Quando si utilizza un punto di accesso Lambda per oggetti, è possibile utilizzare il nome alias del punto di accesso Lambda per oggetti senza la necessità di modifiche estese al codice.

Quando si elimina un punto di accesso Lambda per oggetti, il nome alias del punto di accesso Lambda per oggetti diventa inattivo e non viene allocato.

Come trovare l'alias per il punto di accesso Lambda per oggetti

Utilizzo della console S3

Per trovare l'alias per il tuo punto di accesso Lambda per oggetti utilizzando la console

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, scegli Punti di accesso Lambda dell'oggetto.
3. Per il punto di accesso Lambda per oggetti che desideri utilizzare, copia il valore dell'alias del punto di accesso Lambda per oggetti.

Utilizzo di AWS CLI

Quando crei un punto di accesso Lambda per oggetti, Amazon S3 genera automaticamente un nome alias del punto di accesso Lambda per oggetti, come mostrato nell'esempio seguente. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate. Per informazioni su come creare un Object Lambda Access Point utilizzando il AWS CLI, consulta. [Per creare un Object Lambda Access Point utilizzando AWS CLI](#)

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-access-point --configuration file://my-olap-configuration.json
{
  "ObjectLambdaAccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-
access-point",
```

```
"Alias": {
  "Value": "my-object-lambda-acc-1a4n8yjr3kda96f67zwrwiuse1a--ol-s3",
  "Status": "READY"
}
```

Il nome alias del punto di accesso Lambda per oggetti generato ha due campi:

- Il campo `Value` è il valore dell'alias del punto di accesso Lambda per oggetti.
- Il campo `Status` è lo stato dell'alias del punto di accesso Lambda per oggetti. Se lo stato è `PROVISIONING`, Amazon S3 alloca l'alias del punto di accesso Lambda per oggetti, ma l'alias non è ancora pronto per l'uso. Se lo stato è `READY`, l'alias del punto di accesso Lambda per oggetti è stato allocato correttamente ed è pronto per l'uso.

Per ulteriori informazioni sul tipo di dati `ObjectLambdaAccessPointAlias` nella REST API, consulta [CreateAccessPointForObjectLambda](#) e [ObjectLambdaAccessPointAlias](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Come utilizzare l'alias del punto di accesso Lambda per oggetti

Puoi utilizzare l'alias del punto di accesso Lambda per oggetti al posto di un nome bucket Amazon S3 per le operazioni elencate in [Compatibilità dei punti di accesso](#).

L'AWS CLI esempio seguente del `get-bucket-location` comando utilizza l'alias del punto di accesso del bucket per restituire il valore in Regione AWS cui si trova il bucket. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api get-bucket-location --bucket my-object-lambda-acc-w7i37nq6xuzgax3jw3oqtifiusw2a--ol-s3

{
  "LocationConstraint": "us-west-2"
}
```

Se l'alias del punto di accesso Lambda per oggetti in una richiesta non è valido, viene restituito il codice di errore `InvalidAccessPointAliasError`. Per ulteriori informazioni su `InvalidAccessPointAliasError` consulta [Elenco dei codici di errore](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Le limitazioni di un alias del punto di accesso Lambda per oggetti sono le stesse di un alias del punto di accesso. Per ulteriori informazioni sulle limitazioni di un alias del punto di accesso, consulta [Limitazioni degli alias del punto di accesso](#).

Considerazioni sulla sicurezza per i punti di accesso S3 Object Lambda

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner Partner Network (APN). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Con Amazon S3 Object Lambda, puoi eseguire trasformazioni personalizzate sui dati quando escono da Amazon S3 utilizzando la scalabilità e la flessibilità di una piattaforma di elaborazione. AWS Lambda S3 e Lambda rimangono protetti per impostazione predefinita, ma per conservare questo livello di sicurezza è necessaria un'attenzione speciale da parte dell'autore della funzione Lambda. S3 Object Lambda richiede che tutti gli accessi siano effettuati da entità autenticate (nessun accesso anonimo) e su HTTPS.

Per ridurre i rischi per la sicurezza, è consigliabile:

- Definire l'ambito del ruolo di esecuzione della funzione Lambda in base a un set di autorizzazioni il più limitato possibile.
- Se possibile, assicurati che la funzione Lambda acceda ad Amazon S3 tramite l'URL prefirmato fornito.

Configurazione delle policy IAM

I punti di accesso S3 supportano politiche sulle risorse AWS Identity and Access Management (IAM) che consentono di controllare l'uso del punto di accesso per risorsa, utente o altre condizioni. Per ulteriori informazioni, consulta [Configurazione delle policy IAM per i punti di accesso Lambda per oggetti](#).

Funzionamento della crittografia

Poiché gli Access Point Object Lambda utilizzano sia Amazon S3 che AWS Lambda, esistono differenze nel comportamento di crittografia. Per ulteriori informazioni sul comportamento della

crittografia predefinita di S3, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#).

- Quando si utilizza la crittografia lato server S3 con i punti di accesso Lambda per oggetti, l'oggetto viene decrittato prima di essere inviato a Lambda. Dopo l'invio a Lambda, l'oggetto viene elaborato in modo non crittografato (nel caso di una richiesta GET o HEAD).
- Per impedire la registrazione della chiave di crittografia, S3 rifiuta GET e HEAD richiede gli oggetti crittografati utilizzando la crittografia lato server con chiavi fornite dal cliente (). SSE-C Tuttavia, la funzione Lambda può ancora recuperare questi oggetti a condizione che abbia accesso alla chiave fornita dal client.
- Quando utilizzi la crittografia lato client S3 con i punti di accesso Lambda per oggetti, assicurati che Lambda abbia accesso alla chiave di crittografia affinché possa decrittare ed eseguire nuovamente la crittografia dell'oggetto.

Sicurezza dei punti di accesso

Lambda per oggetti S3 utilizza due punti di accesso, un punto di accesso Lambda per oggetti e un punto di accesso S3 standard, denominato punto di accesso di supporto. Quando effettui una richiesta a un punto di accesso Lambda per oggetti, S3 richiama Lambda per tuo conto o delega la richiesta al punto di accesso di supporto, a seconda della configurazione di Lambda per oggetti S3. Quando Lambda viene richiamato per una richiesta, S3 genera un URL prefirmato per l'oggetto per tuo conto tramite il punto di accesso di supporto. Quando viene richiamata, la funzione Lambda riceverà questo URL come input.

È possibile impostare la funzione Lambda in modo che utilizzi questo URL prefirmato per recuperare l'oggetto originale invece di richiamare direttamente S3. Questo modello consente di applicare limiti di sicurezza migliori agli oggetti. È possibile limitare l'accesso diretto agli oggetti tramite bucket S3 o punti di accesso S3 a un set limitato di ruoli o utenti IAM. Questo approccio protegge anche le funzioni Lambda dall'essere soggette al [problema del "confused deputy"](#), in cui una funzione configurata erroneamente con autorizzazioni diverse rispetto all'invoker potrebbe consentire o negare l'accesso agli oggetti quando non dovrebbe.

Accesso pubblico ai punti di accesso Object Lambda

S3 Object Lambda non consente l'accesso anonimo o pubblico perché Amazon S3 deve autorizzare l'identità per completare qualsiasi richiesta di S3 Object Lambda. Quando si richiamano le richieste tramite un punto di accesso Lambda per oggetti, è necessaria l'autorizzazione `lambda:InvokeFunction` per la funzione Lambda configurata. Allo stesso modo, quando si

richiamano altre operazioni di API tramite un punto di accesso Lambda per oggetti, è necessario disporre delle autorizzazioni s3: *.

Senza queste autorizzazioni, le richieste per richiamare Lambda o delegare a S3 avranno esito negativo e verrà restituito un errore HTTP 403 Accesso negato. Tutti gli accessi devono essere effettuati da principali autenticati. Se hai bisogno di un accesso pubblico, come possibile alternativa può essere utilizzato Lambda@Edge. Per ulteriori informazioni, consulta [Customizing at the edge with Lambda @Edge nella Amazon Developer Guide](#). CloudFront

Indirizzi IP dei punti di accesso Lambda per oggetti

Le sottoreti `describe-managed-prefix-lists` supportano gli endpoint VPC (Virtual Private Cloud) del gateway e sono correlate alla tabella di instradamento degli endpoint VPC. Poiché il punto di accesso per le espressioni Lambda dell'oggetto non supporta il VPC del gateway, i relativi intervalli IP mancano. Gli intervalli mancanti appartengono ad Amazon S3, ma non sono supportati dagli endpoint VPC del gateway. Per ulteriori informazioni su `describe-managed-prefix-lists`, consulta il riferimento per le API di Amazon EC2 e gli intervalli [di indirizzi AWS IP DescribeManagedPrefixLists](#) nel. Riferimenti generali di AWS

Configurazione delle policy IAM per i punti di accesso Lambda per oggetti

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner Partner Network (APN). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

I punti di accesso Amazon S3 supportano le policy relative alle risorse AWS Identity and Access Management (IAM) che puoi utilizzare per controllare l'uso del punto di accesso per risorsa, utente o altre condizioni. È possibile controllare l'accesso tramite una policy di risorse opzionale sul punto di accesso Lambda per oggetti o una policy di risorse sul punto di accesso di supporto. Per esempi dettagliati, consulta le sezioni [Tutorial: trasformazione dei dati per l'applicazione con S3 Object Lambda](#) e [Tutorial: rilevamento e oscuramento dei dati PII con S3 Object Lambda e Amazon Comprehend](#).

Per utilizzare i punti di accesso Lambda per oggetti, le seguenti quattro risorse devono disporre delle seguenti autorizzazioni:

- L'identità IAM, ad esempio un utente o un ruolo. Per ulteriori informazioni sulle identità IAM e sulle best practice, consulta [Identità IAM \(utenti, gruppi di utenti e ruoli\)](#) nella Guida per l'utente di IAM.
- Il punto di accesso standard collegato a un'origine dati sottostante come un bucket S3 o un volume Amazon FSx per OpenZFS. Quando utilizzi i punti di accesso Lambda per oggetti, questo punto di accesso standard è noto come punto di accesso di supporto.
- Il punto di accesso Lambda per oggetti.
- La AWS Lambda funzione.

Important

Prima di salvare la polizza, assicurati di risolvere gli avvisi di sicurezza, gli errori, gli avvisi generali e i suggerimenti di. AWS Identity and Access Management Access Analyzer IAM Access Analyzer esegue controlli sulle policy per convalidare le policy rispetto alla [grammatica delle policy](#) IAM e alle [best practice](#). Questi controlli generano risultati e forniscono raccomandazioni attuabili per aiutarti a creare policy funzionali e conformi alle best practice di sicurezza.

Per ulteriori informazioni sulla convalida delle policy tramite IAM Access Analyzer, consulta [Convalida delle policy di IAM Access Analyzer](#) nella Guida per l'utente di IAM. Per visualizzare un elenco delle avvertenze, degli errori e dei suggerimenti restituiti da IAM Access Analyzer, consulta il [Riferimento al controllo delle policy di IAM Access Analyzer](#).

In questi esempi di policy si presuppone di disporre delle seguenti risorse:

- Un bucket Amazon S3 con il seguente nome della risorsa Amazon (ARN):

```
arn:aws:s3:::amzn-s3-demo-bucket1
```

- Un punto di accesso standard Amazon S3 su questo bucket con il seguente ARN:

```
arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point
```

- Un punto di accesso Lambda per oggetti con il seguente ARN:

```
arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-object-lambda-ap
```

- Una AWS Lambda funzione con il seguente ARN:

```
arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction
```


Note

Se si utilizza una funzione Lambda del proprio account, è necessario includere la versione specifica della funzione nell'istruzione della policy. Nel seguente ARN di esempio, la versione è indicata da **1**:

```
arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction:1
```

Lambda non supporta l'aggiunta di policy IAM alla versione \$LATEST. Per ulteriori informazioni sulle versioni delle funzioni Lambda, consulta [Versioni delle funzioni Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

Example: policy di bucket che delega il controllo degli accessi ai punti di accesso standard

Il seguente esempio di policy di bucket S3 delega il controllo degli accessi di un bucket ai relativi punti di accesso standard. Questa policy consente l'accesso completo a tutti i punti di accesso di proprietà dell'account del proprietario del bucket. Pertanto, tutto l'accesso a questo bucket è controllato dalle policy associate ai punti di accesso. Gli utenti possono eseguire la lettura dal bucket solo mediante un punto di accesso; ciò significa che le operazioni possono essere richiamate solo tramite i punti di accesso. Per ulteriori informazioni, consulta [Delegazione del controllo di accesso agli access point](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect": "Allow",
      "Principal" : { "AWS": "account-ARN" },
      "Action" : "*",
      "Resource" : [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringEquals" : { "s3:DataAccessPointAccount" : "Bucket owner's account ID" }
      }
    }
  ]
}
```

```
}
```

Example- Policy IAM che concede a un utente le autorizzazioni necessarie per utilizzare un punto di accesso Lambda per oggetti

La seguente policy IAM concede a un utente le autorizzazioni per la funzione Lambda, il punto di accesso standard e il punto di accesso Lambda per oggetti.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLambdaInvocation",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction:1",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowStandardAccessPointAccess",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
```

```
        "s3-object-lambda.amazonaws.com"
    ]
  }
},
{
  "Sid": "AllowObjectLambdaAccess",
  "Action": [
    "s3-object-lambda:Get*",
    "s3-object-lambda:List*"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:s3-object-lambda:us-  
east-1:111122223333:accesspoint/my-object-lambda-ap"
}
]
```

Abilitazione delle autorizzazioni per i ruoli di esecuzione Lambda

Quando vengono effettuate richieste GET a un punto di accesso Lambda per oggetti, la funzione Lambda deve essere autorizzata a inviare dati al punto di accesso Lambda per oggetti S3. Per fornire questa autorizzazione, abilita l'autorizzazione `s3-object-lambda:WriteGetObjectResponse` sul ruolo di esecuzione della funzione Lambda. Puoi creare un nuovo ruolo di esecuzione o aggiornare un ruolo esistente.

Note

La funzione richiede l'autorizzazione `s3-object-lambda:WriteGetObjectResponse` solo se stai effettuando una richiesta GET.

Per creare un ruolo di esecuzione nella console IAM

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione a sinistra seleziona Ruoli.
3. Scegliere Crea ruolo.
4. In Common use cases (Casi di utilizzo comuni), scegliere Lambda.
5. Scegli Avanti.

6. Nella pagina **Aggiungi autorizzazioni**, cerca la policy AWS gestita [AmazonS3ObjectLambdaExecutionRolePolicy](#), quindi seleziona la casella di controllo accanto al nome della policy.

Questa politica dovrebbe contenere l'operazione `s3-object-lambda:WriteGetObjectResponse`.
7. Scegli **Avanti**.
8. Nella pagina **Name, review, and create** (Denomina, rivedi e crea), in **Role name** (Nome ruolo) immetti **s3-object-lambda-role**.
9. (Facoltativo) Aggiungi una descrizione e i tag per questo ruolo.
10. Scegliere **Crea ruolo**.
11. Applica il nuovo **s3-object-lambda-role** quale ruolo di esecuzione della funzione Lambda. Questa operazione può essere eseguita durante o dopo la creazione della funzione Lambda nella console Lambda.

Per ulteriori informazioni sui ruoli di esecuzione, consulta la sezione [Ruolo di esecuzione Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

Utilizzo delle chiavi di contesto con i punti di accesso Lambda per oggetti

S3 Object Lambda valuterà le chiavi di contesto come `s3-object-lambda:TlsVersion` o `s3-object-lambda:AuthType` in base alla connessione o alla firma della richiesta. Tutte le altre chiavi di contesto, ad esempio `s3:prefix`, vengono valutate da Amazon S3.

Supporto CORS per Punto di accesso per le espressioni Lambda dell'oggetto

Quando Lambda per oggetti Amazon S3 riceve una richiesta da un browser o la richiesta include un'intestazione `Origin`, Lambda per oggetti Amazon S3 aggiunge sempre un campo di intestazione `"AllowedOrigins": ""`.

Per ulteriori informazioni, consulta [Utilizzo della funzionalità Cross-Origin Resource Sharing \(CORS\)](#).

Scrittura di funzioni Lambda per i punti di accesso Lambda per oggetti S3

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni partner Partner Network (APN). AWS Per

funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Questa sezione descrive come scrivere AWS Lambda funzioni da utilizzare con gli access point Amazon S3 Object Lambda.

Per informazioni sulle procedure complete end-to-end per alcune attività di S3 Object Lambda, consulta quanto segue:

- [Tutorial: trasformazione dei dati per l'applicazione con S3 Object Lambda](#)
- [Tutorial: rilevamento e oscuramento dei dati PII con S3 Object Lambda e Amazon Comprehend](#)
- [Tutorial: utilizzo di Lambda per oggetti S3 per aggiungere filigrane alle immagini in modo dinamico man mano che vengono recuperate](#)

Argomenti

- [Utilizzo di richieste GetObject in Lambda](#)
- [Utilizzo di richieste HeadObject in Lambda](#)
- [Utilizzo di richieste ListObjects in Lambda](#)
- [Utilizzo delle richieste ListObjects V2 in Lambda](#)
- [Formato e utilizzo del contesto degli eventi](#)
- [Lavorare con Intervallo and Numero del pezzo headers](#)

Utilizzo di richieste **GetObject** in Lambda

Questa sezione presuppone che il punto di accesso Lambda per oggetti sia configurato per richiamare la funzione Lambda per GetObject. S3 Object Lambda include l'operazione API Amazon S3 WriteGetObjectResponse, che consente alla funzione Lambda di fornire dati personalizzati e intestazioni di risposta al chiamante GetObject.

WriteGetObjectResponse offre un ampio controllo su codice di stato, intestazioni di risposta e corpo della risposta, in base ai requisiti di elaborazione. È possibile utilizzare WriteGetObjectResponse per rispondere con l'intero oggetto trasformato, con parti dell'oggetto trasformato o con altre risposte in base al contesto dell'applicazione. Nella sezione seguente sono illustrati esempi univoci di utilizzo dell'operazione API WriteGetObjectResponse.

- Esempio 1: risposta con un codice di stato HTTP 403 (Forbidden) (Accesso negato)
- Esempio 2: Rispondere con un'immagine trasformata
- Esempio 3: Streaming di contenuto compresso

Esempio 1: risposta con un codice di stato HTTP 403 (Forbidden) (Accesso negato)

È possibile utilizzare `WriteGetObjectResponse` per rispondere con il codice di stato HTTP 403 (Non consentito) in base al contenuto dell'oggetto.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.WriteGetObjectResponseRequest;

import java.io.ByteArrayInputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example1 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
    Exception {
        S3Client s3Client = S3Client.builder().build();

        // Check to see if the request contains all of the necessary information.
        // If it does not, send a 4XX response and a custom error code and message.
        // Otherwise, retrieve the object from S3 and stream it
        // to the client unchanged.
        var tokenIsNotPresent = !
event.getUserRequest().getHeaders().containsKey("requiredToken");
        if (tokenIsNotPresent) {
            s3Client.writeGetObjectResponse(WriteGetObjectResponseRequest.builder()
                .requestRoute(event.outputRoute())
                .requestToken(event.outputToken())
```

```

        .statusCode(403)
        .contentType(0L)
        .errorCode("MissingRequiredToken")
        .errorMessage("The required token was not present in the
request.")

        .build(),
        RequestBody.fromInputStream(new ByteArrayInputStream(new
byte[0]), 0L));
    return;
}

// Prepare the presigned URL for use and make the request to S3.
HttpClient httpClient = HttpClient.newBuilder().build();
var presignedResponse = httpClient.send(
    HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
    HttpResponse.BodyHandlers.ofInputStream());

// Stream the original bytes back to the caller.
s3Client.writeGetObjectResponse(WriteGetObjectResponseRequest.builder()
    .requestRoute(event.outputRoute())
    .requestToken(event.outputToken())
    .build(),
    RequestBody.fromInputStream(presignedResponse.body(),
        presignedResponse.headers().firstValueAsLong("content-
length").orElse(-1L)));
}
}

```

Python

```

import boto3
import requests

def handler(event, context):
    s3 = boto3.client('s3')

    """
    Retrieve the operation context object from the event. This object indicates
    where the WriteGetObjectResponse request
    should be delivered and contains a presigned URL in 'inputS3Url' where we can
    download the requested object from.
    The 'userRequest' object has information related to the user who made this
    'GetObject' request to
    """

```

```

S3 Object Lambda.
"""
get_context = event["getObjectContext"]
user_request_headers = event["userRequest"]["headers"]

route = get_context["outputRoute"]
token = get_context["outputToken"]
s3_url = get_context["inputS3Url"]

# Check for the presence of a 'CustomHeader' header and deny or allow based on
that header.
is_token_present = "SuperSecretToken" in user_request_headers

if is_token_present:
    # If the user presented our custom 'SuperSecretToken' header, we send the
    requested object back to the user.
    response = requests.get(s3_url)
    s3.write_get_object_response(RequestRoute=route, RequestToken=token,
    Body=response.content)
else:
    # If the token is not present, we send an error back to the user.
    s3.write_get_object_response(RequestRoute=route, RequestToken=token,
    StatusCode=403,
    ErrorCode="NoSuperSecretTokenFound", ErrorMessage="The request was not
    secret enough.")

# Gracefully exit the Lambda function.
return { 'status_code': 200 }

```

Node.js

```

const { S3 } = require('aws-sdk');
const axios = require('axios').default;

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
    where the WriteGetObjectResponse request
    // should be delivered and contains a presigned URL in 'inputS3Url' where we can
    download the requested object from.
    // The 'userRequest' object has information related to the user who made this
    'GetObject' request to S3 Object Lambda.

```



```
const { userRequest, getObjectContext } = event;
const { outputRoute, outputToken, inputS3Url } = getObjectContext;

// Check for the presence of a 'CustomHeader' header and deny or allow based on
that header.
const isTokenPresent = Object
  .keys(userRequest.headers)
  .includes("SuperSecretToken");

if (!isTokenPresent) {
  // If the token is not present, we send an error back to the user. The
  'await' in front of the request
  // indicates that we want to wait for this request to finish sending before
  moving on.
  await s3.writeGetObjectResponse({
    RequestRoute: outputRoute,
    RequestToken: outputToken,
    StatusCode: 403,
    ErrorCode: "NoSuperSecretTokenFound",
    ErrorMessage: "The request was not secret enough.",
  }).promise();
} else {
  // If the user presented our custom 'SuperSecretToken' header, we send the
  requested object back to the user.
  // Again, note the presence of 'await'.
  const presignedResponse = await axios.get(inputS3Url);
  await s3.writeGetObjectResponse({
    RequestRoute: outputRoute,
    RequestToken: outputToken,
    Body: presignedResponse.data,
  }).promise();
}

// Gracefully exit the Lambda function.
return { statusCode: 200 };
}
```

Esempio 2: Rispondere con un'immagine trasformata

Durante la trasformazione dell'immagine, è possibile che siano necessari tutti i byte dell'oggetto di fonte prima di poter iniziare a elaborarli. In questo caso, la tua richiesta `WriteGetObjectResponse` restituisce l'intero oggetto all'applicazione richiedente in una sola chiamata.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.WriteGetObjectResponseRequest;

import javax.imageio.ImageIO;
import java.awt.image.BufferedImage;
import java.awt.Image;
import java.io.ByteArrayOutputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example2V2 {

    private static final int HEIGHT = 250;
    private static final int WIDTH = 250;

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
    Exception {
        S3Client s3Client = S3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Prepare the presigned URL for use and make the request to S3.
        var presignedResponse = httpClient.send(
            HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
            HttpResponse.BodyHandlers.ofInputStream());

        // The entire image is loaded into memory here so that we can resize it.
        // Once the resizing is completed, we write the bytes into the body
        // of the WriteGetObjectResponse request.
        var originalImage = ImageIO.read(presignedResponse.body());
        var resizingImage = originalImage.getScaledInstance(WIDTH, HEIGHT,
        Image.SCALE_DEFAULT);
        var resizedImage = new BufferedImage(WIDTH, HEIGHT,
        BufferedImage.TYPE_INT_RGB);
```

```

        resizedImage.createGraphics().drawImage(resizingImage, 0, 0, WIDTH, HEIGHT,
        null);

        var baos = new ByteArrayOutputStream();
        ImageIO.write(resizedImage, "png", baos);

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(WriteGetObjectResponseRequest.builder()
            .requestRoute(event.outputRoute())
            .requestToken(event.outputToken())
            .build(), RequestBody.fromBytes(baos.toByteArray()));
    }
}

```

Python

```

import boto3
import requests
import io
from PIL import Image

def handler(event, context):
    """
    Retrieve the operation context object from the event. This object indicates
    where the WriteGetObjectResponse request
    should be delivered and has a presigned URL in 'inputS3Url' where we can
    download the requested object from.
    The 'userRequest' object has information related to the user who made this
    'GetObject' request to
    S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    """
    In this case, we're resizing .png images that are stored in S3 and are
    accessible through the presigned URL
    'inputS3Url'.
    """
    image_request = requests.get(s3_url)
    image = Image.open(io.BytesIO(image_request.content))

```

```
image.thumbnail((256,256), Image.ANTIALIAS)

transformed = io.BytesIO()
image.save(transformed, "png")

# Send the resized image back to the client.
s3 = boto3.client('s3')
s3.write_get_object_response(Body=transformed.getvalue(), RequestRoute=route,
RequestToken=token)

# Gracefully exit the Lambda function.
return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const sharp = require('sharp');

exports.handler = async (event) => {
  const s3 = new S3();

  // Retrieve the operation context object from the event. This object indicates
  // where the WriteGetObjectResponse request
  // should be delivered and has a presigned URL in 'inputS3Url' where we can
  // download the requested object from.
  const { getObjectContext } = event;
  const { outputRoute, outputToken, inputS3Url } = getObjectContext;

  // In this case, we're resizing .png images that are stored in S3 and are
  // accessible through the presigned URL
  // 'inputS3Url'.
  const { data } = await axios.get(inputS3Url, { responseType: 'arraybuffer' });

  // Resize the image.
  const resized = await sharp(data)
    .resize({ width: 256, height: 256 })
    .toBuffer();

  // Send the resized image back to the client.
  await s3.writeGetObjectResponse({
    RequestRoute: outputRoute,
    RequestToken: outputToken,
```

```
        Body: resized,
    }).promise();

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

Esempio 3: Streaming di contenuto compresso

Durante la compressione degli oggetti, i dati compressi vengono prodotti in modo incrementale. Di conseguenza, puoi utilizzare la richiesta `WriteGetObjectResponse` per restituire i dati compressi non appena sono pronti. Come mostrato in questo esempio, non è necessario conoscere la lunghezza della trasformazione completata.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.lambda.runtime.Context;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.WriteGetObjectResponseRequest;

import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example3 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
    Exception {
        S3Client s3Client = S3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Request the original object from S3.
        var presignedResponse = httpClient.send(
            HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
            HttpResponse.BodyHandlers.ofInputStream());
    }
}
```

```

        // Consume the incoming response body from the presigned request,
        // apply our transformation on that data, and emit the transformed bytes
        // into the body of the WriteGetObjectResponse request as soon as they're
ready.
        // This example compresses the data from S3, but any processing pertinent
        // to your application can be performed here.
        var bodyStream = new GZIPCompressingInputStream(presignedResponse.body());

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(WriteGetObjectResponseRequest.builder()
            .requestRoute(event.outputRoute())
            .requestToken(event.outputToken())
            .build(),
            RequestBody.fromInputStream(bodyStream,
                presignedResponse.headers().firstValueAsLong("content-
length").orElse(-1L)));
    }
}

```

Python

```

import boto3
import requests
import zlib
from botocore.config import Config

"""
A helper class to work with content iterators. Takes an iterator and compresses the
bytes that come from it. It
implements 'read' and '__iter__' so that the SDK can stream the response.
"""
class Compress:
    def __init__(self, content_iter):
        self.content = content_iter
        self.compressed_obj = zlib.compressobj()

    def read(self, _size):
        for data in self.__iter__():
            return data

    def __iter__(self):
        while True:

```

```
        data = next(self.content)
        chunk = self.compressed_obj.compress(data)
        if not chunk:
            break

        yield chunk

    yield self.compressed_obj.flush()

def handler(event, context):
    """
    Setting the 'payload_signing_enabled' property to False allows us to send a
    streamed response back to the client.
    In this scenario, a streamed response means that the bytes are not buffered into
    memory as we're compressing them,
    but instead are sent straight to the user.
    """
    my_config = Config(
        region_name='eu-west-1',
        signature_version='s3v4',
        s3={
            "payload_signing_enabled": False
        }
    )
    s3 = boto3.client('s3', config=my_config)

    """
    Retrieve the operation context object from the event. This object indicates
    where the WriteGetObjectResponse request
    should be delivered and has a presigned URL in 'inputS3Url' where we can
    download the requested object from.
    The 'userRequest' object has information related to the user who made this
    'GetObject' request to S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    # Compress the 'get' request stream.
    with requests.get(s3_url, stream=True) as r:
        compressed = Compress(r.iter_content())
```

```
# Send the stream back to the client.
s3.write_get_object_response(Body=compressed, RequestRoute=route,
RequestToken=token, ContentType="text/plain",
                           ContentEncoding="gzip")

# Gracefully exit the Lambda function.
return {'status_code': 200}
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const zlib = require('zlib');

exports.handler = async (event) => {
  const s3 = new S3();

  // Retrieve the operation context object from the event. This object indicates
  // where the WriteGetObjectResponse request
  // should be delivered and has a presigned URL in 'inputS3Url' where we can
  // download the requested object from.
  const { getObjectContext } = event;
  const { outputRoute, outputToken, inputS3Url } = getObjectContext;

  // Download the object from S3 and process it as a stream, because it might be a
  // huge object and we don't want to
  // buffer it in memory. Note the use of 'await' because we want to wait for
  // 'writeGetObjectResponse' to finish
  // before we can exit the Lambda function.
  await axios({
    method: 'GET',
    url: inputS3Url,
    responseType: 'stream',
  }).then(
    // Gzip the stream.
    response => response.data.pipe(zlib.createGzip())
  ).then(
    // Finally send the gzip-ed stream back to the client.
    stream => s3.writeGetObjectResponse({
      RequestRoute: outputRoute,
      RequestToken: outputToken,
      Body: stream,
      ContentType: "text/plain",
```



```
        ContentEncoding: "gzip",
    }).promise()
);

// Gracefully exit the Lambda function.
return { statusCode: 200 };
}
```

Note

Sebbene S3 Object Lambda consente fino a 60 secondi per inviare una risposta completa al chiamante tramite la richiesta `WriteGetObjectResponse`, la quantità effettiva di tempo disponibile potrebbe essere inferiore. Ad esempio, il timeout della funzione Lambda potrebbe essere inferiore a 60 secondi. In altri casi, il chiamante potrebbe avere timeout più rigorosi.

Affinché il chiamante originale riceva una risposta diversa dal codice di stato HTTP 500 (Internal Server Error) (Errore interno del server), la chiamata `WriteGetObjectResponse` deve essere completata. Se la funzione Lambda restituisce un risultato, eccezionalmente o in altro modo, prima che l'operazione API `WriteGetObjectResponse` venga richiamata, il chiamante originale riceverà una risposta 500 (Internal Server Error) (Errore interno del server). Le eccezioni generate durante il tempo necessario per completare la risposta comportano risposte troncate al chiamante. Se la funzione Lambda riceve una risposta con codice di stato HTTP 200 (OK) dalla chiamata API `WriteGetObjectResponse`, il chiamante originale ha inviato la richiesta completa. La risposta della funzione Lambda, indipendentemente dal fatto che un'eccezione sia generata o meno, viene ignorata da S3 Object Lambda.

Quando viene richiamata l'operazione API `WriteGetObjectResponse`, Amazon S3 richiede il token dell'instradamento e della richiesta dal contesto dell'evento. Per ulteriori informazioni, consulta [Formato e utilizzo del contesto degli eventi](#).

I parametri relativi ai token dell'instradamento e della richiesta sono necessari per collegare la risposta `WriteGetObjectResult` al chiamante originale. Sebbene sia sempre opportuno riprovare le risposte 500 (Internal Server Error) (Errore interno del server), è necessario considerare che il token della richiesta è un token monouso e i successivi tentativi di utilizzo possono comportare risposte con codice di stato 400 (Bad Request) (Richiesta non valida). Anche se la chiamata a `WriteGetObjectResponse` con i token dell'instradamento e della richiesta non ha bisogno di essere effettuata dalla funzione Lambda richiamata, deve essere effettuata da un'identità nello

stesso account. La chiamata deve anche essere completata prima che la funzione Lambda finisca l'esecuzione.

Utilizzo di richieste **HeadObject** in Lambda

Questa sezione presuppone che il punto di accesso Lambda per oggetti sia configurato per richiamare la funzione Lambda per `HeadObject`. Lambda riceverà un payload JSON contenente una chiave chiamata `headObjectContext`. All'interno del contesto, esiste un'unica proprietà chiamata `inputS3Url`, che è un URL prefirmato per il punto di accesso di supporto per `HeadObject`.

L'URL prefirmato includerà le seguenti proprietà, se specificate:

- `versionId` (nei parametri della query)
- `requestPayer` (nell'intestazione `x-amz-request-payer`)
- `expectedBucketOwner` (nell'intestazione `x-amz-expected-bucket-owner`)

Le altre proprietà non saranno preassegnate e quindi non saranno incluse. Non-signed le opzioni inviate come intestazioni possono essere aggiunte manualmente alla richiesta quando si chiama l'URL prefirmato che si trova nelle intestazioni. `userRequest` Server-side le opzioni di crittografia non sono supportate per `HeadObject`.

Per i parametri URI della sintassi della richiesta, consulta [HeadObject](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Il seguente esempio mostra un payload di input Lambda JSON per `HeadObject`.

```
{
  "xAmzRequestId": "requestId",
  "***headObjectContext***": {
    "***inputS3Url***": "https://my-s3-ap-111122223333.s3-accesspoint.us-east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>"
  },
  "configuration": {
    "accessPointArn": "arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/example-object-lambda-ap",
    "supportingAccessPointArn": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-ap",
    "payload": "{}"
  },
  "userRequest": {
```

```

    "url": "https://object-lambda-111122223333.s3-object-lambda.us-east-1.amazonaws.com/example",
    "headers": {
      "Host": "object-lambda-111122223333.s3-object-lambda.us-east-1.amazonaws.com",
      "Accept-Encoding": "identity",
      "X-Amz-Content-SHA256": "e3b0c44298fc1example"
    }
  },
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
    "accountId": "111122223333",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
      }
    },
    "sessionIssuer": {
      "type": "Role",
      "principalId": "principalId",
      "arn": "arn:aws:iam::111122223333:role/Admin",
      "accountId": "111122223333",
      "userName": "Admin"
    }
  }
},
"protocolVersion": "1.00"
}

```

La funzione Lambda dovrebbe restituire un oggetto JSON contenente le intestazioni e i valori che verranno restituiti per la chiamata `HeadObject`.

Il seguente esempio illustra la struttura dell'oggetto JSON della risposta Lambda per `HeadObject`.

```

{
  "statusCode": <number>; // Required
  "errorCode": <string>;
  "errorMessage": <string>;
  "headers": {
    "Accept-Ranges": <string>,

```

```

    "x-amz-archive-status": <string>,
    "x-amz-server-side-encryption-bucket-key-enabled": <boolean>,
    "Cache-Control": <string>,
    "Content-Disposition": <string>,
    "Content-Encoding": <string>,
    "Content-Language": <string>,
    "Content-Length": <number>, // Required
    "Content-Type": <string>,
    "x-amz-delete-marker": <boolean>,
    "ETag": <string>,
    "Expires": <string>,
    "x-amz-expiration": <string>,
    "Last-Modified": <string>,
    "x-amz-missing-meta": <number>,
    "x-amz-object-lock-mode": <string>,
    "x-amz-object-lock-legal-hold": <string>,
    "x-amz-object-lock-retain-until-date": <string>,
    "x-amz-mp-parts-count": <number>,
    "x-amz-replication-status": <string>,
    "x-amz-request-charged": <string>,
    "x-amz-restore": <string>,
    "x-amz-server-side-encryption": <string>,
    "x-amz-server-side-encryption-customer-algorithm": <string>,
    "x-amz-server-side-encryption-aws-kms-key-id": <string>,
    "x-amz-server-side-encryption-customer-key-MD5": <string>,
    "x-amz-storage-class": <string>,
    "x-amz-tagging-count": <number>,
    "x-amz-version-id": <string>,
    <x-amz-meta-headers>: <string>, // user-defined metadata
    "x-amz-meta-meta1": <string>, // example of the user-defined metadata header,
    it will need the x-amz-meta prefix
    "x-amz-meta-meta2": <string>
    ...
};
}

```

L'esempio seguente mostra come utilizzare l'URL prefirmato per compilare la risposta modificando i valori dell'intestazione secondo necessità prima di restituire l'oggetto JSON.

Python

```
import requests
```

```
def lambda_handler(event, context):
    print(event)

    # Extract the presigned URL from the input.
    s3_url = event["headObjectContext"]["inputS3Url"]

    # Get the head of the object from S3.
    response = requests.head(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        return {
            "statusCode": response.status_code,
            "errorCode": "RequestFailure",
            "errorMessage": "Request to S3 failed"
        }

    # Store the headers in a dictionary.
    response_headers = dict(response.headers)

    # This obscures Content-Type in a transformation, it is optional to add
    response_headers["Content-Type"] = ""

    # Return the headers to S3 Object Lambda.
    return {
        "statusCode": response.status_code,
        "headers": response_headers
    }
```

Utilizzo di richieste **ListObjects** in Lambda

Questa sezione presuppone che il punto di accesso Lambda per oggetti sia configurato per richiamare la funzione Lambda per `ListObjects`. Lambda riceverà il payload JSON con un nuovo oggetto denominato `listObjectContext`. `listObjectContext` contiene un'unica proprietà `inputS3Url`, che è un URL prefirmato per il punto di accesso di supporto per `ListObjects`.

A differenza di `GetObject` e `HeadObject`, l'URL prefirmato includerà le seguenti proprietà, se specificate:

- Tutti i parametri della query
- `requestPayer` (nell'intestazione `x-amz-request-payer`)

- `expectedBucketOwner` (nell'intestazione `x-amz-expected-bucket-owner`)

Per i parametri URI della sintassi della richiesta, consulta [ListObjects](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Important

Si consiglia di utilizzare la versione più recente, la [ListObjects V2](#), per lo sviluppo delle applicazioni. Per la compatibilità con le versioni precedenti, Amazon S3 continua a supportare `ListObjects`.

Il seguente esempio illustra il payload di input Lambda JSON per `ListObjects`.

```
{
  "xAmzRequestId": "requestId",
  "***listObjectsContext***": {
    "***inputS3Url***": "https://my-s3-ap-111122223333.s3-accesspoint.us-east-1.amazonaws.com/?X-Amz-Security-Token=<snip>",
  },
  "configuration": {
    "accessPointArn": "arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/example-object-lambda-ap",
    "supportingAccessPointArn": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-ap",
    "payload": "{}"
  },
  "userRequest": {
    "url": "https://object-lambda-111122223333.s3-object-lambda.us-east-1.amazonaws.com/example",
    "headers": {
      "Host": "object-lambda-111122223333.s3-object-lambda.us-east-1.amazonaws.com",
      "Accept-Encoding": "identity",
      "X-Amz-Content-SHA256": "e3b0c44298fc1example"
    }
  },
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
  }
}
```

```

    "accountId": "111122223333",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
        },
        "sessionIssuer": {
            "type": "Role",
            "principalId": "principalId",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "userName": "Admin"
        }
    },
    "protocolVersion": "1.00"
}

```

La funzione Lambda deve restituire un oggetto JSON che contenga il codice di stato, l'elenco dei risultati XML o le informazioni di errore che verranno restituite da Lambda per oggetti S3.

Lambda per oggetti S3 non elabora né convalida `listResultXml`, ma lo inoltra al chiamante `ListObjects`. Per `listBucketResult`, Lambda per oggetti S3 si aspetta che determinate proprietà siano di un tipo specifico e genererà eccezioni se non è in grado di analizzarle. `listResultXml` e `listBucketResult` non possono essere specificati contemporaneamente.

L'esempio seguente illustra come utilizzare l'URL prefirmato per richiamare Amazon S3 e utilizzare il risultato per compilare una risposta, incluso il controllo degli errori.

Python

```

import requests
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsContext"]["inputS3Url"]

    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)

```

```

# Return the error to S3 Object Lambda (if applicable).
if (response.status_code >= 400):
    error = xmltodict.parse(response.content)
    return {
        "statusCode": response.status_code,
        "errorCode": error["Error"]["Code"],
        "errorMessage": error["Error"]["Message"]
    }

# Store the XML result in a dict.
response_dict = xmltodict.parse(response.content)

# This obscures StorageClass in a transformation, it is optional to add
for item in response_dict['ListBucketResult']['Contents']:
    item['StorageClass'] = ""

# Convert back to XML.
listResultXml = xmltodict.unparse(response_dict)

# Create response with listResultXml.
response_with_list_result_xml = {
    'statusCode': 200,
    'listResultXml': listResultXml
}

# Create response with listBucketResult.
response_dict['ListBucketResult'] =
sanitize_response_dict(response_dict['ListBucketResult'])
response_with_list_bucket_result = {
    'statusCode': 200,
    'listBucketResult': response_dict['ListBucketResult']
}

# Return the list to S3 Object Lambda.
# Can return response_with_list_result_xml or response_with_list_bucket_result
return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
            newlist = []

```



```

        for element in value:
            if type(element) == type(dict()):
                element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict

```

Il seguente esempio illustra la struttura dell'oggetto JSON della risposta Lambda per `ListObjects`.

```

{
  "statusCode": <number>; // Required
  "errorCode": <string>;
  "errorMessage": <string>;
  "listResultXml": <string>; // This can also be Error XML string in case S3 returned
  error response when calling the pre-signed URL

  "listBucketResult": { // listBucketResult can be provided instead of listResultXml,
  however they can not both be provided in the JSON response
    "name": <string>, // Required for 'listBucketResult'
    "prefix": <string>,
    "marker": <string>,
    "nextMarker": <string>,
    "maxKeys": <int>, // Required for 'listBucketResult'
    "delimiter": <string>,
    "encodingType": <string>
    "isTruncated": <boolean>, // Required for 'listBucketResult'
    "contents": [ {
      "key": <string>, // Required for 'content'
      "lastModified": <string>,
      "eTag": <string>,
      "checksumAlgorithm": <string>, // CRC32, CRC32C, SHA1, SHA256
      "size": <int>, // Required for 'content'
      "owner": {
        "displayName": <string>, // Required for 'owner'
        "id": <string>, // Required for 'owner'
      },
      "storageClass": <string>
    },
    ...
  ]
}

```

```

    ],
    "commonPrefixes": [ {
        "prefix": <string>    // Required for 'commonPrefix'
    },
    ...
    ],
}
}

```

Utilizzo delle richieste **ListObjects V2** in Lambda

Questa sezione presuppone che il punto di accesso Lambda per oggetti sia configurato per richiamare la funzione Lambda per ListObjectsV2. Lambda riceverà il payload JSON con un nuovo oggetto denominato listObjectsV2Context. listObjectsV2Context contiene un'unica proprietà inputS3Url, che è un URL prefirmato per il punto di accesso di supporto per ListObjectsV2.

A differenza di GetObject e HeadObject, l'URL prefirmato includerà le seguenti proprietà, se specificate:

- Tutti i parametri della query
- requestPayer (nell'intestazione x-amz-request-payer)
- expectedBucketOwner (nell'intestazione x-amz-expected-bucket-owner)

Per i parametri URI della sintassi della richiesta, consulta [ListObjectsV2](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Il seguente esempio illustra il payload di input Lambda JSON per ListObjectsV2.

```

{
  "xAmzRequestId": "requestId",
  "**listObjectsV2Context**": {
    "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-east-1.amazonaws.com/?list-type=2&X-Amz-Security-Token=<snip>",
  },
  "configuration": {
    "accessPointArn": "arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/example-object-lambda-ap",
    "supportingAccessPointArn": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-ap",
  }
}

```

```

    "payload": "{}"
  },
  "userRequest": {
    "url": "https://object-lambda-111122223333.s3-object-lambda.us-east-1.amazonaws.com/example",
    "headers": {
      "Host": "object-lambda-111122223333.s3-object-lambda.us-east-1.amazonaws.com",
      "Accept-Encoding": "identity",
      "X-Amz-Content-SHA256": "e3b0c44298fc1example"
    }
  },
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
    "accountId": "111122223333",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
      }
    }
  },
  "protocolVersion": "1.00"
}

```

La funzione Lambda deve restituire un oggetto JSON che contenga il codice di stato, l'elenco dei risultati XML o le informazioni di errore che verranno restituite da Lambda per oggetti S3.

Lambda per oggetti S3 non elabora né convalida `listResultXml`, ma lo inoltra al chiamante `ListObjectsV2`. Per `listBucketResult`, Lambda per oggetti S3 si aspetta che determinate proprietà siano di un tipo specifico e genererà eccezioni se non è in grado di analizzarle. `listResultXml` e `listBucketResult` non possono essere specificati contemporaneamente.

L'esempio seguente illustra come utilizzare l'URL prefirmato per richiamare Amazon S3 e utilizzare il risultato per compilare una risposta, incluso il controllo degli errori.

Python

```
import requests
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsV2Context"]["inputS3Url"]

    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)

    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
```

```

    response_dict['ListBucketResult'] =
    sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict

```

Il seguente esempio illustra la struttura dell'oggetto JSON della risposta Lambda per ListObjectsV2.

```

{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
    "listResultXml": <string>; // This can also be Error XML string in case S3 returned
    error response when calling the pre-signed URL

    "listBucketResult": { // listBucketResult can be provided instead of
    listResultXml, however they can not both be provided in the JSON response
        "name": <string>, // Required for 'listBucketResult'
        "prefix": <string>,

```

```

    "startAfter": <string>,
    "continuationToken": <string>,
    "nextContinuationToken": <string>,
    "keyCount": <int>, // Required for 'listBucketResult'
    "maxKeys": <int>, // Required for 'listBucketResult'
    "delimiter": <string>,
    "encodingType": <string>
    "isTruncated": <boolean>, // Required for 'listBucketResult'
    "contents": [ {
        "key": <string>, // Required for 'content'
        "lastModified": <string>,
        "eTag": <string>,
        "checksumAlgorithm": <string>, // CRC32, CRC32C, SHA1, SHA256
        "size": <int>, // Required for 'content'
        "owner": {
            "displayName": <string>, // Required for 'owner'
            "id": <string>, // Required for 'owner'
        },
        "storageClass": <string>
    },
    ...
],
    "commonPrefixes": [ {
        "prefix": <string> // Required for 'commonPrefix'
    },
    ...
],
}
}

```

Formato e utilizzo del contesto degli eventi

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner APN (Partner Network). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Amazon S3 Object Lambda fornisce un contesto sulla richiesta che viene effettuata nel caso in cui venga passata alla tua funzione. AWS Lambda Il risultato è illustrato nello screenshot seguente. Le descrizioni dei campi sono riportate dopo l'esempio.

```
{
  "xAmzRequestId": "requestId",
  "getObjectContext": {
    "inputS3Url": "https://my-s3-ap-111122223333.s3-accesspoint.us-east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>",
    "outputRoute": "io-use1-001",
    "outputToken": "OutputToken"
  },
  "configuration": {
    "accessPointArn": "arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/example-object-lambda-ap",
    "supportingAccessPointArn": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-ap",
    "payload": "{}"
  },
  "userRequest": {
    "url": "https://object-lambda-111122223333.s3-object-lambda.us-east-1.amazonaws.com/example",
    "headers": {
      "Host": "object-lambda-111122223333.s3-object-lambda.us-east-1.amazonaws.com",
      "Accept-Encoding": "identity",
      "X-Amz-Content-SHA256": "e3b0c44298fc1example"
    }
  },
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
    "accountId": "111122223333",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
```

```
        "arn": "arn:aws:iam::111122223333:role/Admin",
        "accountId": "111122223333",
        "userName": "Admin"
    }
},
"protocolVersion": "1.00"
}
```

I seguenti campi sono inclusi nella richiesta:

- **xAmzRequestId**: l'ID della richiesta di Amazon S3 per questa richiesta. Si consiglia di registrare questo valore per facilitare il debug.
- **getObjectContext**: i dettagli di input e output per le connessioni ad Amazon S3 e S3 Object Lambda.
 - **inputS3Url**: un URL prefirmato che può essere utilizzato per recuperare l'oggetto originale da Amazon S3. L'URL viene firmato utilizzando l'identità del chiamante originale e quando viene utilizzato l'URL vengono applicate le autorizzazioni dell'utente associato. Se nell'URL sono presenti intestazioni firmate, la funzione Lambda deve includerle nella chiamata ad Amazon S3, ad eccezione dell'intestazione Host.
 - **outputRoute** - Un token di routing che viene aggiunto all'URL di S3 Object Lambda quando la funzione Lambda richiama `WriteGetObjectResponse`.
 - **outputToken**: un token opaco utilizzato da S3 Object Lambda per abbinare la chiamata `WriteGetObjectResponse` al chiamante originale.
- **configuration**: informazioni di configurazione sul punto di accesso Lambda per oggetti.
 - **accessPointArn**: il nome della risorsa Amazon (ARN) del punto di accesso Lambda per oggetti che ha ricevuto questa richiesta.
 - **supportingAccessPointArn**: l'ARN del punto di accesso di supporto specificato nella configurazione del punto di accesso Lambda per oggetti.
 - **payload**: dati personalizzati applicati alla configurazione del punto di accesso Lambda per oggetti. S3 Object Lambda tratta questi dati come una stringa opaca, quindi potrebbe essere necessario decodificarli prima dell'utilizzo.
- **userRequest**: informazioni sulla chiamata originale a S3 Object Lambda.
 - **url**: l'URL decodificato della richiesta come ricevuto da S3 Object Lambda, esclusi eventuali parametri di query relativi all'autorizzazione.

- **headers**: una mappa di stringa alle stringhe contenenti le intestazioni HTTP e i relativi valori dalla chiamata originale, escluse eventuali intestazioni relative all'autorizzazione. Se la stessa intestazione viene visualizzata più volte, i valori di ogni istanza della stessa intestazione vengono combinati in un elenco delimitato da virgole. Il formato maiuscolo/minuscolo delle intestazioni originali viene mantenuto in questa mappa.
- **userIdentity**: dettagli sull'identità che ha effettuato la chiamata a S3 Object Lambda. Per ulteriori informazioni, consulta [Registrazione di eventi di dati per i percorsi](#) nella Guida per l'utente di AWS CloudTrail .
 - **type**: il tipo di identità.
 - **accountId**— Il nome Account AWS a cui appartiene l'identità.
 - **userName**: il nome descrittivo dell'identità che ha effettuato la chiamata.
 - **principalId**: l'identificatore univoco per l'identità che ha effettuato la chiamata.
 - **arn**: l'ARN del principale che ha effettuato la chiamata. L'ultima sezione dell'ARN contiene l'utente o il ruolo che ha effettuato la chiamata.
 - **sessionContext**: se la richiesta è stata effettuata con le credenziali di sicurezza temporanee, questo elemento fornisce informazioni sulla sessione creata per tali credenziali.
 - **invokedBy**— Il nome di chi Servizio AWS ha effettuato la richiesta, ad esempio Amazon EC2 Auto Scaling o. AWS Elastic Beanstalk
 - **sessionIssuer**: se la richiesta è stata effettuata con le credenziali di sicurezza temporanee, questo elemento fornisce informazioni su come sono state ottenute tali credenziali.
- **protocolVersion**: l'ID versione del contesto fornito. Il formato di questo campo è {Major Version}.{Minor Version}. I numeri di versione secondari sono sempre numeri a due cifre. Qualsiasi rimozione o modifica alla semantica di un campo necessita un aumento della versione principale e richiede l'opt-in attivo. Amazon S3 può aggiungere nuovi campi in qualsiasi momento e in quel punto si potrebbe riscontrare un bump di versione minore. A causa della natura delle implementazioni software, più versioni secondarie potrebbero essere visualizzati in uso contemporaneamente.

Lavorare con Intervallo and Numero del pezzo headers

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner APN (Partner Network). Per

funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Quando vengono utilizzati oggetti di grandi dimensioni in Amazon S3 Object Lambda, è possibile utilizzare l'intestazione HTTP Range per scaricare un intervallo di byte specificato da un oggetto. Puoi utilizzare connessioni simultanee ad Amazon S3 per recuperare diversi intervalli di byte all'interno dello stesso oggetto. Puoi inoltre specificare il parametro `partNumber` (un numero intero compreso tra 1 e 10.000) che esegue una richiesta basata su intervallo per la parte specificata dell'oggetto.

Perché ci sono diversi modi in cui potresti voler gestire una richiesta che include i parametri Range o `partNumber`, S3 Object Lambda non applica questi parametri all'oggetto trasformato. Invece, la tua AWS Lambda funzione deve implementare questa funzionalità in base alle necessità della tua applicazione.

Per utilizzare i parametri Range e `partNumber` con S3 Object Lambda, procedi come segue:

- Abilita questi parametri nella configurazione del punto di accesso Lambda per oggetti.
- Scrivi una funzione Lambda in grado di gestire le richieste contenente questi parametri.

Di seguito viene descritto come realizzarlo.

Fase 1: configura il punto di accesso Lambda per oggetti

Per impostazione predefinita, gli punti di accesso Lambda per oggetti rispondono con un errore con codice di stato HTTP 501 (Not Implemented) a qualsiasi richiesta `GetObject` o `HeadObject` contenente un parametro Range o `partNumber` nelle intestazioni o nei parametri di query.

Per abilitare un punto di accesso Lambda per oggetti ad accettare tali richieste, devi includere `GetObject-Range`, `GetObject-PartNumber`, `HeadObject-Range` o `HeadObject-PartNumber` nella sezione `AllowedFeatures` della configurazione del punto di accesso Lambda per oggetti. Per ulteriori informazioni sull'aggiornamento della configurazione del punto di accesso Lambda per oggetti, consulta [Creazione di punti di accesso Object Lambda](#).

Fase 2: Implementa la **gestione di Range o PartNumber** nella tua funzione Lambda

Quando il punto di accesso Lambda per oggetti richiama la funzione Lambda con una richiesta `GetObject` o `HeadObject` basata su intervallo, il parametro Range o `partNumber` è incluso nel

contesto dell'evento. La posizione del parametro nel contesto dell'evento dipende dal parametro utilizzato e dal modo in cui è stato incluso nella richiesta originale al punto di accesso Lambda per oggetti, come illustrato nella tabella seguente.

Parametro	Posizione del contesto dell'evento
Range (intestazione)	<code>userRequest.headers.Range</code>
Range (parametro di query)	<code>userRequest.url</code> (Range del parametro di query)
<code>partNumber</code>	<code>userRequest.url</code> (<code>partNumber</code> del parametro di query)

 Important

L'URL prefirmato fornito per il punto di accesso Lambda per oggetti non contiene il parametro `Range` o `partNumber` della richiesta originale. Vedi le seguenti opzioni su come gestire questi parametri nella tua AWS Lambda funzione.

Dopo aver estratto il valore `Range` o `partNumber`, è possibile adottare uno dei seguenti approcci in base alle esigenze dell'applicazione:

A. Mappare il valore **Range** o **partNumber** richiesto all'oggetto trasformato (consigliato).

Per gestire le richieste `Range` o `partNumber` nel modo più affidabile, procedi come segue:

- Recupera l'oggetto completo da Amazon S3.
- Trasforma l'oggetto.
- Applica i parametri `Range` o `partNumber` obbligatori all'oggetto trasformato.

Per fare ciò, utilizza l'URL prefirmato fornito per recuperare l'intero oggetto da Amazon S3 e quindi elaborare l'oggetto secondo necessità. Per un esempio di funzione Lambda che elabora un `Range` parametro in questo modo, consultate [questo esempio](#) nel GitHub repository AWS Samples.

B. Mappatura del **Range** richiesto all'URL prefirmato URL.

In alcuni casi, la funzione Lambda può mappare il valore o il Range richiesto direttamente all'URL prefissato per recuperare solo parte dell'oggetto da Amazon S3. Questo approccio è appropriato solo se la trasformazione soddisfa entrambi i seguenti criteri:

1. La funzione di trasformazione può essere applicata a intervalli di oggetti parziali.
2. Applicando il parametro Range prima o dopo la funzione di trasformazione produce lo stesso oggetto trasformato.

Ad esempio, una funzione di trasformazione che converte tutti i caratteri di un ASCII-encoded oggetto in lettere maiuscole soddisfa entrambi i criteri precedenti. La trasformazione può essere applicata a una parte di un oggetto e applicando il parametro Range prima della trasformazione si ottiene lo stesso risultato dell'applicazione del parametro dopo la trasformazione.

Al contrario, una funzione che inverte i caratteri di un ASCII-encoded oggetto non soddisfa questi criteri. Tale funzione soddisfa il criterio 1, poiché può essere applicata a intervalli di oggetti parziali. Tuttavia, non soddisfa il criterio 2, perché l'applicazione del parametro Range prima che la trasformazione raggiunga risultati diversi rispetto all'applicazione del parametro dopo la trasformazione.

Considera una richiesta di applicare la funzione ai primi tre caratteri di un oggetto con il contenuto abcdefg. L'applicazione del parametro Range prima della trasformazione recupera solo abc e poi inverte i dati, restituendo cba. Ma se il parametro viene applicato dopo la trasformazione, la funzione recupera l'intero oggetto, lo inverte e quindi applica il parametro Range, restituendo gfe. Poiché questi risultati sono diversi, questa funzione non dovrebbe applicare il parametro Range durante il recupero dell'oggetto da Amazon S3. Invece, dovrebbe recuperare l'intero oggetto, eseguire la trasformazione e solo successivamente applicare il parametro Range.

Warning

In molti casi, l'applicazione del parametro Range o dell'URL prefissato risulterà in un comportamento imprevisto da parte della funzione Lambda o del client richiedente. A meno che non sia sicuro che la tua applicazione funzioni correttamente quando recuperi solo un oggetto parziale da Amazon S3, ti consigliamo di recuperare e trasformare oggetti completi come descritto in precedenza nell'approccio A.

Se l'applicazione soddisfa i criteri descritti in precedenza nell'approccio B, è possibile semplificare la AWS Lambda funzione recuperando solo l'intervallo di oggetti richiesto e quindi eseguendo la trasformazione su tale intervallo.

Il seguente esempio di codice Java illustra come eseguire le seguenti operazioni:

- Recuperare l'intestazione Range dalla richiesta `GetObject`.
- Aggiungere l'intestazione Range all'URL prefirmato che Lambda può utilizzare per recuperare l'intervallo richiesto da Amazon S3.

```
private HttpRequest.Builder applyRangeHeader(ObjectLambdaEvent event,
HttpRequest.Builder presignedRequest) {
    var header = event.getUserRequest().getHeaders().entrySet().stream()
        .filter(e -> e.getKey().toLowerCase(Locale.ROOT).equals("range"))
        .findFirst();

    // Add check in the query string itself.
    header.ifPresent(entry -> presignedRequest.header(entry.getKey(),
entry.getValue()));
    return presignedRequest;
}
```

Utilizzo AWS funzioni Lambda integrate

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner Partner Network (APN). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

AWS fornisce alcune AWS Lambda funzioni predefinite che puoi utilizzare con Amazon S3 Object Lambda per rilevare e oscurare le informazioni di identificazione personale (PII) e decomprimere gli oggetti S3. Queste funzioni Lambda sono disponibili nel AWS Serverless Application Repository. È possibile selezionare queste funzioni mediante la Console di gestione AWS quando si crea il punto di accesso Lambda per oggetti.

Per ulteriori informazioni su come distribuire applicazioni serverless da, consulta [Deploying Applications nella Developer Guide. AWS Serverless Application Repository](https://docs.aws.amazon.com/serverlessrepo/latest/devguide/serverlessrepo-consuming-applications.html)<https://docs.aws.amazon.com/serverlessrepo/latest/devguide/serverlessrepo-consuming-applications.html>
AWS Serverless Application Repository

 Note

I seguenti esempi possono essere utilizzati solo con richieste `GetObject`.

Esempio 1: Controllo degli accessi alle informazioni personali di identificazione (PII)

Questa funzione Lambda utilizza Amazon Comprehend, un servizio di elaborazione del linguaggio naturale (NLP) basato sul machine learning per trovare informazioni e relazioni in un testo. Questa funzionalità rileva automaticamente le informazioni personali di identificazione (PII) come nomi, indirizzi, date, numeri di carta di credito e numeri di previdenza sociale nei documenti presenti in un bucket Amazon S3. Se nel bucket sono presenti documenti che includono questo tipo di informazioni, è possibile configurare la funzione di controllo degli accessi alle queste informazioni di S3 Object Lambda per rilevare questi tipi di entità PII e bloccare l'accesso agli utenti non autorizzati.

Per iniziare, è sufficiente implementare la seguente funzione Lambda nell'account in uso e aggiungere il nome della risorsa Amazon (ARN) della funzione nella configurazione del punto di accesso Lambda per oggetti.

Di seguito è riportato un esempio di ARN per questa funzione:

```
arn:aws:serverlessrepo:us-east-1:111122223333:applications/  
ComprehendPiiAccessControlS3ObjectLambda
```

È possibile aggiungere o visualizzare questa funzione su Console di gestione AWS utilizzando il seguente AWS Serverless Application Repository link:

[ComprehendPiiAccessControlS3ObjectLambda](#)

Per visualizzare questa funzione su GitHub, consulta [Amazon Comprehend S3 Object Lambda](#).

Esempio 2: oscuramento di PII

Questa funzione Lambda utilizza Amazon Comprehend, un servizio di elaborazione del linguaggio naturale (NLP) basato sul machine learning per trovare informazioni e relazioni in un testo. Questa

funzione oscura automaticamente le informazioni personali di identificazione (PII) come nomi, indirizzi, date, numeri di carta di credito e numeri di previdenza sociale provenienti da documenti contenuti in un bucket Amazon S3.

Se nel bucket sono presenti documenti che includono informazioni quali numeri di carta di credito o informazioni sul conto corrente, è possibile configurare la funzione Oscuramento di PII di S3 Object Lambda per rilevare le informazioni personali e quindi restituire una copia di questi documenti in cui i tipi di entità PII sono redatti.

Per iniziare, è sufficiente implementare la seguente funzione Lambda nell'account in uso e aggiungere l'ARN della funzione nella configurazione del punto di accesso Lambda per oggetti.

Di seguito è riportato un esempio di ARN per questa funzione:

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/  
ComprehendPiiRedactionS3ObjectLambda
```

Puoi aggiungere o visualizzare questa funzione su Console di gestione AWS utilizzando il seguente AWS Serverless Application Repository link: [ComprehendPiiRedactionS3ObjectLambda](#)

Per visualizzare questa funzione su GitHub, consulta [Amazon Comprehend S3 Object Lambda](#).

Per informazioni sulle procedure complete end-to-end per alcune attività di S3 Object Lambda nella redazione delle informazioni di identificazione personali, consulta [Tutorial: rilevamento e oscuramento dei dati PII con S3 Object Lambda e Amazon Comprehend](#).

Esempio 3: Decompressione

La funzione Lambda S3ObjectLambdaDecompression può decomprimere gli oggetti archiviati in Amazon S3 in uno dei sei formati di file compressi: bzip2, gzip, snappy, zlib, zstandard e ZIP.

Per iniziare, è sufficiente implementare la seguente funzione Lambda nell'account in uso e aggiungere l'ARN della funzione nella configurazione del punto di accesso Lambda per oggetti.

Di seguito è riportato un esempio di ARN per questa funzione:

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/S3ObjectLambdaDecompression
```

Puoi aggiungere o visualizzare questa funzione su Console di gestione AWS utilizzando il seguente AWS Serverless Application Repository link: [S3ObjectLambdaDecompression](#)

Per visualizzare questa funzione su GitHub, vedere [S3 Object Lambda Decompression](#).

Best practice e linee guida per Lambda per oggetti S3

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner Partner Network (APN). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Quando utilizzi Lambda per oggetti S3, segui le seguenti best practice e linee guida per ottimizzare le operazioni e le prestazioni.

Argomenti

- [Utilizzo di S3 Object Lambda](#)
- [Servizi AWS utilizzato in connessione con S3 Object Lambda](#)
- [Intestazioni Range e PartNumber](#)
- [Trasformazione della data di scadenza](#)
- [Lavorare con il AWS CLI and AWS SDK](#)

Utilizzo di S3 Object Lambda

S3 Object Lambda supporta solo l'elaborazione delle richieste GET, LIST e HEAD. Qualsiasi altra richiesta non richiama AWS Lambda e restituisce invece risposte API standard non trasformate. È possibile creare un massimo di 1.000 Object Lambda Access Point per regione. Account AWS La AWS Lambda funzione utilizzata deve trovarsi nella stessa Account AWS regione dell'Access Point Object Lambda.

S3 Object Lambda richiede fino a 60 secondi per trasmettere una risposta completa al suo chiamante. La tua funzione è inoltre soggetta a quote AWS Lambda predefinite. Per ulteriori informazioni, consulta la sezione [Quote Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

Quando S3 Object Lambda richiama la funzione Lambda specificata, è responsabilità dell'utente garantire che tutti i dati sovrascritti o eliminati in Amazon S3 dalla funzione Lambda o dall'applicazione specificata siano quelli desiderati e corretti.

S3 Object Lambda può essere utilizzato solo per eseguire operazioni sugli oggetti. Non è possibile utilizzarlo per eseguire altre operazioni Amazon S3, ad esempio la modifica o l'eliminazione dei bucket. Per un elenco completo delle operazioni S3 che supportano i punti di accesso, consulta [Compatibilità dei punti di accesso con le operazioni S3](#).

Oltre a questo elenco, i punti di accesso Lambda per oggetti non supportano le operazioni [POST Object](#), [CopyObject](#) (come origine) e le operazioni API [SelectObjectContent](#).

Servizi AWS utilizzato in connessione con S3 Object Lambda

S3 Object Lambda connette Amazon S3 e AWS Lambda, facoltativamente, altri Servizi AWS a tua scelta per fornire oggetti pertinenti alle applicazioni richiedenti. Tutti quelli Servizi AWS utilizzati con S3 Object Lambda sono regolati dai rispettivi Service Level Agreement (SLA). Ad esempio, se uno di essi Servizio AWS non rispetta l'impegno di assistenza, hai diritto a ricevere un credito di servizio, come documentato nello SLA del servizio.

Intestazioni Range e PartNumber

In caso di utilizzo di oggetti di grandi dimensioni, è possibile usare l'intestazione HTTP Range per scaricare un intervallo di byte specificato da un oggetto. Quando si utilizza l'intestazione Range, la richiesta recupera solo la parte specificata dell'oggetto. È anche possibile utilizzare l'intestazione partNumber per eseguire una richiesta basata su intervallo per la parte specificata dall'oggetto.

Per ulteriori informazioni, consulta [Lavorare con Intervallo and Numero del pezzo headers](#).

Trasformazione della data di scadenza

Puoi aprire o scaricare oggetti trasformati dal tuo Object Lambda Access Point su. Console di gestione AWS Questi oggetti non devono essere scaduti. Se la funzione Lambda trasforma expiry-date degli oggetti, potrebbero venire visualizzati oggetti scaduti che non possono essere aperti o scaricati. Questo comportamento si applica solo agli oggetti ripristinati in S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

Lavorare con il AWS CLI and AWS SDK

AWS Command Line Interface (AWS CLI) I sottocomandi S3 (cpmv, esync) e l'uso della AWS SDK per Java `TransferManager` classe non sono supportati per l'uso con S3 Object Lambda.

Tutorial di Lambda per oggetti S3

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni partner Partner Network (APN). AWS Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

I seguenti tutorial illustrano le procedure complete end-to-end per le attività comuni di S3 Object Lambda.

Con S3 Object Lambda puoi aggiungere il tuo codice per elaborare i dati recuperati da S3 prima di restituirli a un'applicazione. Ciascuna delle seguenti esercitazioni modifica i dati man mano che vengono recuperati da Amazon S3, senza modificare l'oggetto esistente o mantenere più copie dei dati. Il primo tutorial spiegherà come aggiungere una AWS Lambda funzione a una richiesta S3 GET per modificare un oggetto recuperato da S3. La seconda esercitazione mostra come utilizzare una funzione Lambda precostituita alimentata da Amazon Comprehend per proteggere le informazioni di identificazione personale (PII) recuperate da S3 prima di restituirle a un'applicazione. La terza esercitazione utilizza Lambda per oggetti S3 per aggiungere una filigrana a un'immagine mentre viene recuperata da Amazon S3.

- [Tutorial: trasformazione dei dati per l'applicazione con S3 Object Lambda](#)
- [Tutorial: rilevamento e oscuramento dei dati PII con S3 Object Lambda e Amazon Comprehend](#)
- [Tutorial: utilizzo di Lambda per oggetti S3 per aggiungere filigrane alle immagini in modo dinamico man mano che vengono recuperate](#)

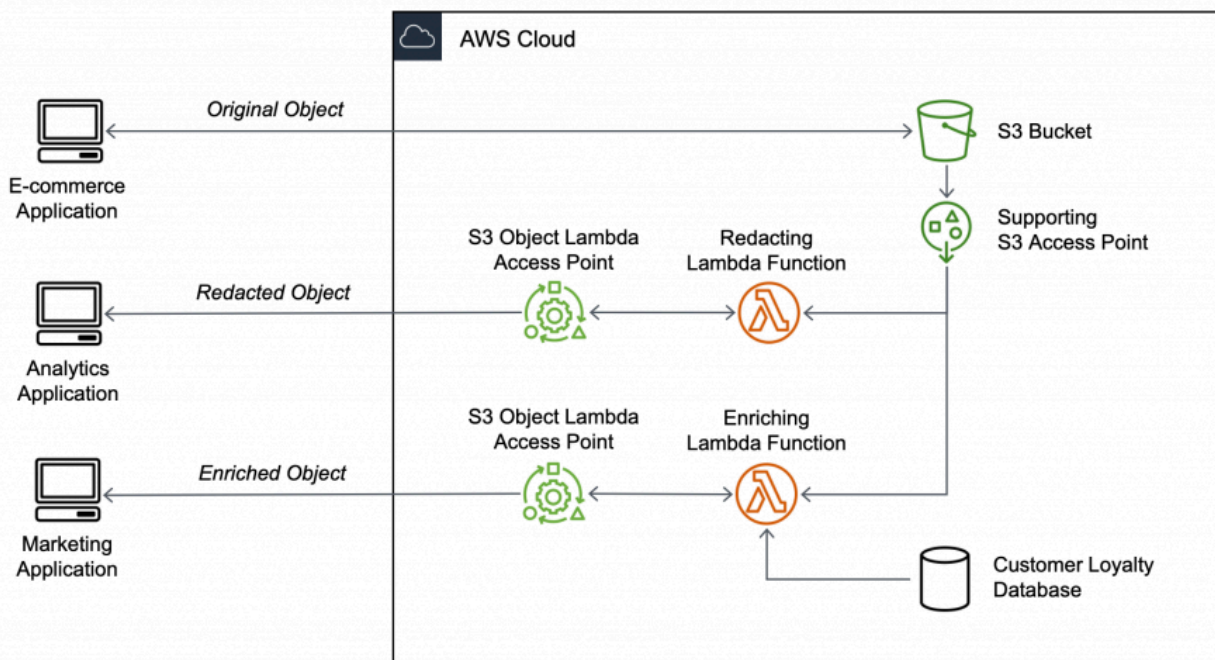
Tutorial: trasformazione dei dati per l'applicazione con S3 Object Lambda

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni AWS partner Partner Network (APN). Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Quando archivi dati in Amazon S3, puoi condividerli facilmente per utilizzarli da più applicazioni. Tuttavia, ogni applicazione potrebbe avere requisiti univoci in merito al formato dei dati e richiedere la modifica o l'elaborazione dei dati per un caso d'uso specifico. Ad esempio, un set di dati creato da un'applicazione e-commerce potrebbe includere informazioni personali di identificazione (PII). Quando gli stessi dati vengono elaborati per l'analisi, queste PII non sono necessarie e devono essere oscurate. Tuttavia, se lo stesso set di dati viene utilizzato per una campagna di marketing, potresti dover arricchire i dati con ulteriori dettagli, come informazioni dal database che raccoglie i dati sulla fidelizzazione dei clienti.

Con [S3 Object Lambda](#) puoi aggiungere il tuo codice per elaborare i dati recuperati da S3 prima di restituirli a un'applicazione. In particolare, puoi configurare una AWS Lambda funzione e collegarla a un Access Point S3 Object Lambda. Quando un'applicazione invia [richieste GET S3 standard](#) tramite il punto di accesso Lambda per oggetti S3, la funzione Lambda specificata viene invocata per elaborare i dati recuperati dall'origine dati sottostante attraverso il punto di accesso S3 di supporto, quindi il punto di accesso Lambda per oggetti S3 restituisce il risultato trasformato all'applicazione. Puoi creare ed eseguire funzioni Lambda personalizzate, adattando la trasformazione dei dati S3 Object Lambda al tuo specifico caso d'uso, il tutto senza che siano necessarie modifiche alla tua applicazione.



Obiettivo

In questo tutorial imparerai come aggiungere codice personalizzato alle richieste GET S3 standard per modificare l'oggetto richiesto recuperato da S3 in modo che questo soddisfi le esigenze del client o dell'applicazione richiedente. In particolare, apprendi come trasformare in maiuscolo tutto il testo dell'oggetto originale archiviato in un bucket S3 tramite Lambda per oggetti S3.

Note

Questo tutorial utilizza il codice Python per trasformare i dati, ad esempio utilizzando altri AWS SDK, consulta [Trasformare i dati per la tua applicazione con S3 Object Lambda](#) nella SDK Code Examples Library. AWS

Argomenti

- [Prerequisiti](#)
- [Fase 1: Creazione di un bucket S3](#)
- [Fase 2: Caricamento di un file nel bucket S3](#)
- [Fase 3: Creazione di un punto di accesso S3](#)
- [Fase 4: Creazione di una funzione Lambda](#)
- [Fase 5: Configurazione di una policy IAM per il ruolo di esecuzione della funzione Lambda](#)
- [Fase 6: Creazione di un punto di accesso Lambda per oggetti S3](#)
- [Fase 7: Visualizzazione dei dati trasformati](#)
- [Fase 8: Pulizia](#)
- [Fasi successive](#)

Prerequisiti

Prima di iniziare questo tutorial, devi disporre di un account a Account AWS cui puoi accedere come utente AWS Identity and Access Management (IAM) con le autorizzazioni corrette. Devi inoltre installare la versione 3.8 o successiva di Python.

Fasi secondarie

- [Crea un utente IAM con autorizzazioni nel tuo Account AWS \(console\)](#)
- [Installazione di Python 3.8 o versioni successive sul computer locale](#)

Crea un utente IAM con autorizzazioni nel tuo Account AWS (console)

Puoi creare un utente IAM per il tutorial. Per completare questo tutorial, l'utente IAM deve allegare le seguenti politiche IAM per accedere alle AWS risorse pertinenti ed eseguire azioni specifiche. Per ulteriori informazioni su come creare un utente IAM, consulta [Creazione di utenti IAM \(console\)](#) nella Guida per l'utente di IAM.

L'utente IAM richiede le seguenti policy:

- [AmazonS3FullAccess](#)— Concede le autorizzazioni per tutte le azioni di Amazon S3, incluse le autorizzazioni per creare e utilizzare un Access Point Object Lambda.
- [AWS Lambda_FullAccess](#): concede le autorizzazioni per tutte le azioni Lambda.
- [IAMFullAccess](#)— Concede le autorizzazioni per tutte le azioni IAM.
- [IAMAccessAnalyzerReadOnlyAccess](#)— Concede le autorizzazioni per leggere tutte le informazioni di accesso fornite da IAM Access Analyzer.
- [CloudWatchLogsFullAccess](#)— Concede l'accesso completo ai log. CloudWatch

Note

Per semplicità, questo tutorial crea e utilizza un utente IAM. Dopo aver completato il tutorial, ricordati di [Eliminazione dell'utente IAM](#). Per l'uso in produzione, consigliamo di seguire le [best practice di sicurezza in IAM](#) disponibili nella Guida per l'utente di IAM. Come best practice, richiedi agli utenti di utilizzare la federazione con un gestore dell'identità digitale per accedere a AWS utilizzando credenziali temporanee. Un'ulteriore suggerimento derivante dalle best practice è richiedere ai carichi di lavoro di utilizzare credenziali temporanee con ruoli IAM per l'accesso ad AWS. Per informazioni su come Centro identità AWS IAM creare utenti con credenziali temporanee, consulta la [Guida introduttiva](#) nella Guida per l'Centro identità AWS IAM utente.

Per semplicità, questo tutorial utilizza policy gestite AWS di accesso completo. Per l'utilizzo in produzione, è consigliabile invece concedere solo le autorizzazioni minime necessarie per il caso d'uso, in conformità con le [best practice in fatto di sicurezza](#).

Installazione di Python 3.8 o versioni successive sul computer locale

Utilizza la procedura seguente per installare Python 3.8 o una versione successiva sul computer locale. Per maggiori istruzioni sull'installazione, consulta la pagina [Download di Python](#) nella Guida per principianti di Python.

1. Apri il terminale o la shell locale ed esegui il seguente comando per determinare se Python è già installato e, in caso affermativo, la versione installata.

```
python --version
```

2. Se non disponi di Python 3.8 o versioni successive, scarica il [programma di installazione ufficiale](#) di Python 3.8 o versioni successive adatto al computer locale.
3. Esegui il programma di installazione facendo doppio clic sul file scaricato e segui i passaggi per completare l'installazione.

Per utenti Windows: scegli Add Python 3.X to PATH (Aggiungi Python 3.X a [percorso]) nella procedura guidata di installazione prima di scegliere Install Now (Installa adesso).

4. Chiudi e riapri il terminale per riavviarlo.
5. Per verificare che Python 3.8 o versioni successive sia installato correttamente, esegui il comando seguente.

Se sei un utente macOS, esegui questo comando:

```
python3 --version
```

Per utenti Windows: esegui questo comando:

```
python --version
```

6. Esegui il seguente comando per verificare che il gestore di pacchetti pip3 sia installato. Se vedi un numero di versione di pip e Python 3.8 o versione successiva nella risposta al comando, significa che il gestore di pacchetti pip3 è installato correttamente.

```
pip --version
```

Fase 1: Creazione di un bucket S3

Crea un bucket per archiviare i dati originali che intendi trasformare.

Note

I punti di accesso possono essere collegati a un'altra origine dati, come un volume Amazon FSx per OpenZFS, tuttavia questo tutorial utilizza un punto di accesso di supporto collegato a un bucket S3.

Per creare un bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Scegliere Create bucket (Crea bucket).

Viene visualizzata la pagina Create bucket (Crea bucket).

4. In Bucket name (Nome bucket), inserisci un nome per il bucket (ad esempio **tutorial-bucket**).

Per ulteriori informazioni sulle regole di denominazione del bucket in Amazon S3, consulta [Regole di denominazione dei bucket per uso generico](#).

5. Per la regione, scegli Regione AWS dove vuoi che risieda il bucket.

Per ulteriori informazioni sulla Regione del bucket, consulta [Panoramica dei bucket per uso generico](#).

6. In Block Public Access settings for this bucket (Blocca le impostazioni di accesso pubblico per questo bucket), mantieni le impostazioni predefinite (è abilitato Block all public access (Blocca tutto l'accesso pubblico)).

È consigliabile di lasciare abilitate tutte le impostazioni di blocco dell'accesso pubblico, a meno che non abbia bisogno di disattivarne una o più per il caso d'uso. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

7. Mantieni le impostazioni rimanenti impostate sui valori di default.

(Facoltativo) Se desideri configurare ulteriori impostazioni del bucket per il tuo caso d'uso specifico, consulta [Creazione di un bucket per uso generico](#).

8. Seleziona Crea bucket.

Fase 2: Caricamento di un file nel bucket S3

Carica il file di testo nel bucket S3. Questo file di testo contiene i dati originali che trasformerai in maiuscolo più avanti in questo tutorial.

Ad esempio, puoi caricare un file `tutorial.txt` che contiene il testo seguente:

```
Amazon S3 Object Lambda Tutorial:  
You can add your own code to process data retrieved from S3 before  
returning it to an application.
```

Per caricare un file in un bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) scegli il nome del bucket creato nella [Fase 1](#) (ad esempio, **tutorial-bucket**) in cui caricare il file.
4. Nella scheda Oggetti del bucket seleziona Carica.
5. Nella pagina Upload (Caricamento), sotto Files and Folders (File e cartelle) scegli Add Files (Aggiungi file).
6. Seleziona un file da caricare, quindi scegli Apri. Ad esempio, puoi caricare il file di esempio `tutorial.txt` menzionato in precedenza.
7. Scegli Carica.

Fase 3: Creazione di un punto di accesso S3

Per utilizzare un punto di accesso Lambda per oggetti S3 per accedere e trasformare i dati originali, devi creare un punto di accesso S3 e associarlo al bucket S3 creato nella [Fase 1](#). Il punto di accesso deve trovarsi nello Regione AWS stesso oggetto da trasformare.

Più avanti in questo tutorial, utilizzerai questo punto di accesso come punto di accesso di supporto per il tuo punto di accesso Lambda per oggetti.

Per creare un punto di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Access Points (Punti di accesso).
3. Nella pagina Punto di accesso, scegli Crea punto di accesso.
4. Nel campo Nome del punto di accesso, inserisci il nome (ad esempio, **tutorial-access-point**) del punto di accesso.

Per ulteriori informazioni sulla denominazione dei punti di accesso, consulta [Regole di denominazione dei punti di accesso](#).

5. Nel campo Origine dati inserisci il nome del bucket creato nella [Fase 1](#) (ad esempio, **tutorial-bucket**). S3 allega quindi il punto di accesso a questo bucket.

(Facoltativo) Puoi scegliere Browse S3 (Sfoglia S3) per sfogliare e cercare i bucket nell'account. Se scegli Browse S3 (Sfoglia S3), scegli il bucket desiderato e scegli Choose path (Scegli percorso) per popolare il campo Bucket name (Nome bucket) con il nome del bucket.

6. In Network origin (Origine rete), scegli Internet.

Per ulteriori informazioni sulle origini della rete per i punti di accesso, consulta [Creazione di access point limitati a un cloud privato virtuale](#).

7. Tutte le impostazioni di blocco dell'accesso pubblico sono abilitate per impostazione predefinita per il punto di accesso. È consigliabile lasciare abilitato Block all public access (Blocca tutto l'accesso pubblico).

Per ulteriori informazioni, consulta [Gestione dell'accesso pubblico ai punti di accesso per bucket per uso generico](#).

8. Per tutte le altre impostazioni del punto di accesso, mantieni i valori di default.

(Facoltativo) Puoi modificare le impostazioni del punto di accesso per supportare il caso d'uso. Per questo tutorial, ti consigliamo di mantenere le impostazioni di default.

(Facoltativo) Se è necessario gestire l'accesso al punto di accesso, puoi specificare una policy per il punto di accesso. Per ulteriori informazioni, consulta [Esempi di policy per i punti di accesso](#).

9. Scegli Crea punto di accesso.

Fase 4: Creazione di una funzione Lambda

Per trasformare i dati originali, crea una funzione Lambda utilizzabile con il punto di accesso Lambda per oggetti S3.

Fasi secondarie

- [Scrittura del codice della funzione Lambda e creazione di un pacchetto di implementazione in un ambiente virtuale](#)
- [Creare una funzione Lambda con un ruolo di esecuzione \(console\)](#)
- [Implementa il codice della tua funzione Lambda con gli archivi in file .zip e configura la funzione Lambda \(console\)](#)

Scrittura del codice della funzione Lambda e creazione di un pacchetto di implementazione in un ambiente virtuale

1. Sul computer locale, crea una cartella denominata `object-lambda` per l'ambiente virtuale da utilizzare più avanti in questo tutorial.
2. Nella cartella `object-lambda`, crea un file con una funzione Lambda che modifica tutto il testo dell'oggetto originale in maiuscolo. Ad esempio, puoi utilizzare la seguente funzione scritta in Python. Salva questa funzione in un file denominato `transform.py`.

```
import boto3
import requests
from botocore.config import Config

# This function capitalizes all text in the original object
def lambda_handler(event, context):
    object_context = event["getObjectContext"]
    # Get the presigned URL to fetch the requested original object
    # from S3
    s3_url = object_context["inputS3Url"]
    # Extract the route and request token from the input context
    request_route = object_context["outputRoute"]
    request_token = object_context["outputToken"]

    # Get the original S3 object using the presigned URL
    response = requests.get(s3_url)
    original_object = response.content.decode("utf-8")

    # Transform all text in the original object to uppercase
```

```
# You can replace it with your custom code based on your use case
transformed_object = original_object.upper()

# Write object back to S3 Object Lambda
s3 = boto3.client('s3', config=Config(signature_version='s3v4'))
# The WriteGetObjectResponse API sends the transformed data
# back to S3 Object Lambda and then to the user
s3.write_get_object_response(
    Body=transformed_object,
    RequestRoute=request_route,
    RequestToken=request_token)

# Exit the Lambda function: return the status code
return {'status_code': 200}
```

Note

La precedente funzione Lambda di esempio carica l'intero oggetto richiesto in memoria prima di trasformarlo e restituirlo al client. In alternativa, puoi trasmettere l'oggetto da S3 per evitare di caricare l'intero oggetto in memoria. Questo approccio può essere utile quando lavori con oggetti di grandi dimensioni. Per ulteriori informazioni sullo streaming delle risposte con i punti di accesso Lambda per oggetti, consulta gli esempi di streaming in [Utilizzo di richieste GetObject in Lambda](#).

Quando scrivi una funzione Lambda utilizzabile con un punto di accesso Lambda per oggetti S3, la funzione si basa sul contesto dell'evento di input che Lambda per oggetti S3 fornisce alla funzione stessa. Il contesto dell'evento fornisce informazioni relative alla richiesta eseguita nell'evento inviato da Lambda per oggetti S3 a Lambda, e che contiene i parametri utilizzati per crearla.

I campi utilizzati per creare la funzione Lambda precedente sono i seguenti:

Il campo `getObjectContext` si riferisce ai dettagli di ingresso e uscita per le connessioni ad Amazon S3 e S3 Object Lambda. Ha i seguenti campi:

- `inputS3Url`: un URL prefirmato che la funzione Lambda può utilizzare per scaricare l'oggetto originale dal punto di accesso di supporto. Utilizzando un URL prefirmato, la funzione Lambda non ha bisogno di avere le autorizzazioni di lettura di Amazon S3 per recuperare l'oggetto originale e può accedere solo all'oggetto elaborato da ogni chiamata.

- `outputRoute`: un token di routing che viene aggiunto all'URL di S3 Object Lambda quando la funzione Lambda richiama `WriteGetObjectResponse` per reinviare l'oggetto trasformato.
- `outputToken`: un token utilizzato da S3 Object Lambda per associare la chiamata `WriteGetObjectResponse` al chiamante originale quando reinvia l'oggetto trasformato.

Per ulteriori informazioni su tutti i campi del contesto dell'evento, consulta [Formato e utilizzo del contesto degli eventi](#) e [Scrittura di funzioni Lambda per i punti di accesso Lambda per oggetti S3](#).

3. Nel terminale locale, inserisci il seguente comando per installare il pacchetto `virtualenv`:

```
python -m pip install virtualenv
```

4. Nel terminale locale, apri la cartella `object-lambda` creata in precedenza e inserisci il seguente comando per creare e inizializzare un nuovo ambiente virtuale denominato `venv`.

```
python -m virtualenv venv
```

5. Per attivare l'ambiente virtuale, inserire il seguente comando per eseguire il file `activate` dalla cartella dell'ambiente:

Se sei un utente macOS, esegui questo comando:

```
source venv/bin/activate
```

Per utenti Windows: esegui questo comando:

```
.\venv\Scripts\activate
```

Il prompt dei comandi si modifica per mostrare `(venv)`, indicando che l'ambiente virtuale è attivo.

6. Per installare le librerie richieste, esegui i seguenti comandi riga per riga nell'ambiente virtuale `venv`.

Questi comandi installano versioni aggiornate delle dipendenze della funzione Lambda `lambda_handler`. Queste dipendenze sono gli SDK per Python (Boto3) AWS e il modulo delle richieste.

```
pip3 install boto3
```

```
pip3 install requests
```

7. Per disattivare l'ambiente virtuale, esegui il comando seguente:

```
deactivate
```

8. Per creare un pacchetto di implementazione con le librerie installate come file `.zip` denominato `lambda.zip` alla root della directory `object-lambda`, eseguire i seguenti comandi riga per riga nel terminale locale.

 Tip

È possibile che i seguenti comandi debbano essere regolati per funzionare in un ambiente specifico. Ad esempio, una libreria potrebbe essere visualizzata in `site-packages` o `dist-packages` e la prima cartella potrebbe essere `lib` o `lib64`. Inoltre, la cartella `python` potrebbe essere denominata con una versione di Python diversa. Per localizzare un pacchetto specifico, utilizza il comando `pip show`.

Se sei un utente macOS, esegui questi comandi:

```
cd venv/lib/python3.8/site-packages
```

```
zip -r ../../../../lambda.zip .
```

Se sei un utente Windows, esegui questi comandi:

```
cd .\venv\Lib\site-packages\
```

```
powershell Compress-Archive * ../../../../lambda.zip
```

L'ultimo comando salva il pacchetto di implementazione nella directory principale della directory `object-lambda`.

9. Aggiungere il file del codice della funzione `transform.py` alla root del pacchetto di implementazione.

Se sei un utente macOS, esegui questi comandi:

```
cd ../../../../
```

```
zip -g lambda.zip transform.py
```

Se sei un utente Windows, esegui questi comandi:

```
cd ../../..\
```

```
powershell Compress-Archive -update transform.py lambda.zip
```

Dopo aver completato questa fase, si dovrà avere la seguente struttura della directory:

```
lambda.zip$  
# transform.py  
# __pycache__  
| boto3/  
# certifi/  
# pip/  
# requests/  
...
```

Creare una funzione Lambda con un ruolo di esecuzione (console)

1. Accedi Console di gestione AWS e apri la AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>.
2. Nel pannello di navigazione a sinistra, scegli Functions (Funzioni).
3. Selezionare Create function (Crea funzione).
4. Scegli Author from scratch (Crea da zero).
5. In Basic information (Informazioni di base) eseguire queste operazioni:
 - a. Nel campo Function name (Nome funzione), immettere **tutorial-object-lambda-function**.
 - b. In Runtime (Runtime), scegli Python 3.8 o una versione successiva.

6. Espandi la sezione Change default execution role (Cambia ruolo di esecuzione predefinito). In Execution role (Ruolo di esecuzione), scegli Create a new role with basic Lambda permissions (Crea un nuovo ruolo con le autorizzazioni Lambda di base).

Nel [passaggio 5](#) più avanti in questo tutorial, si collega il ruolo AmazonS3ObjectLambdaExecutionRolePolicy di esecuzione di questa funzione Lambda.

7. Mantieni le impostazioni rimanenti impostate sui valori predefiniti.
8. Scegli Crea funzione.

Implementa il codice della tua funzione Lambda con gli archivi in file .zip e configura la funzione Lambda (console)

1. Nella AWS Lambda console di <https://console.aws.amazon.com/lambda/>, scegli Funzioni nel riquadro di navigazione a sinistra.
2. Scegli la funzione Lambda creata in precedenza (ad esempio, **tutorial-object-lambda-function**).
3. Nella pagina dei dettagli della funzione Lambda, scegli la scheda Code (Codice). Nella sezione Code source (Origine codice), scegli Upload from (Carica da) e quindi .zip file (file .zip).
4. Scegli Upload (Carica) per selezionare il file .zip locale.
5. Scegli il file `lambda.zip` creato in precedenza, quindi scegli Open (Apri).
6. Selezionare Salva.
7. Nel pannello Runtime settings (Impostazioni runtime), scegli Edit (Modifica).
8. Nella pagina Edit runtime settings (Modifica impostazioni runtime), verifica che Runtime (Runtime) sia impostato su Python 3.8 o una versione successiva.
9. Per indicare al runtime Lambda quale metodo gestore richiamare nel codice della funzione Lambda, inserisci **transform.lambda_handler** in Handler (Gestore).

Quando si configura una funzione in Python, il valore dell'impostazione del gestore è costituito dal nome del file e dal nome del modulo del gestore esportato, separati da un punto. Ad esempio, `transform.lambda_handler` richiama il metodo `lambda_handler` definito nel file `transform.py`.

10. Selezionare Salva.
11. (Facoltativo) Nella pagina dei dettagli della funzione Lambda, scegli la scheda Configuration (Configurazione). Nel pannello di navigazione a sinistra, scegli General configuration

(Configurazione generale), quindi scegli Edit (Modifica). Nel campo Timeout inserisci **1 min 0** sec. Mantieni le impostazioni rimanenti sui valori predefiniti e scegli Save (Salva).

Il Timeout è la quantità di tempo consentita da Lambda per l'esecuzione di una funzione per una chiamata prima di arrestarla. Il valore predefinito è 3 secondi. La durata massima per una funzione Lambda utilizzata da S3 Object Lambda è di 60 secondi. I prezzi si basano sulla quantità di memoria configurata e sulla quantità di tempo di esecuzione del codice.

Fase 5: Configurazione di una policy IAM per il ruolo di esecuzione della funzione Lambda

Per abilitare la funzione Lambda a fornire dati personalizzati e intestazioni di risposta al chiamante GetObject, il ruolo di esecuzione della funzione Lambda deve disporre delle autorizzazioni IAM per chiamare l'API WriteGetObjectResponse.

Allegare una policy IAM al ruolo della funzione Lambda

1. Nella AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>, scegli Funzioni nel riquadro di navigazione a sinistra.
2. Scegli la funzione creata nella [Fase 4](#) (ad esempio, **tutorial-object-lambda-function**).
3. Nella pagina dei dettagli della funzione Lambda, scegli la scheda Configuration (Configurazione), quindi scegli Permissions (Autorizzazioni) nel pannello di navigazione a sinistra.
4. In Execution role (Ruolo di esecuzione) scegli il collegamento Role Name (Nome ruolo). Si apre la console IAM.
5. Nella pagina Summary (Riepilogo) della console IAM del ruolo di esecuzione della funzione Lambda, seleziona la scheda Permissions (Autorizzazioni). Quindi, nel menu Add Permissions (Aggiungi autorizzazioni), scegli Attach policies (Collega policy).
6. Nella pagina Attach permissions (Allega autorizzazioni) inserisci **AmazonS3ObjectLambdaExecutionRolePolicy** nella casella di ricerca per filtrare l'elenco di policy. Seleziona la casella di controllo accanto al nome della AmazonS3ObjectLambdaExecutionRolePolicy policy.
7. Scegli Collega policy.

Fase 6: Creazione di un punto di accesso Lambda per oggetti S3

Un punto di accesso Lambda per oggetti S3 offre la flessibilità di richiamare una funzione Lambda direttamente da una richiesta GET S3 in modo che la funzione possa elaborare i dati recuperati da

un punto di accesso S3. Quando crei e configuri un punto di accesso Lambda per oggetti S3, devi specificare la funzione Lambda da richiamare e fornire il contesto dell'evento in formato JSON come parametri personalizzati utilizzabili da Lambda.

Per creare un punto di accesso Lambda per oggetti S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, scegli Punti di accesso Lambda dell'oggetto.
3. Nella pagina Object Lambda Access Points (Punti di accesso Object Lambda), scegli Create Object Lambda Access Point (Crea punto di accesso Object Lambda).
4. In Nome del punto di accesso per le espressioni Lambda dell'oggetto immetti il nome che desideri utilizzare per il punto di accesso Lambda per oggetti (per esempio, **tutorial-object-lambda-accesspoint**).
5. Per Punto di accesso di supporto, immetti o cerca il punto di accesso standard creato al [punto 3](#) (ad esempio, **tutorial-access-point**), quindi seleziona Scegli punto di accesso di supporto.
6. Per le API S3, per recuperare oggetti dal bucket S3 per l'elaborazione della funzione Lambda, seleziona. GetObject
7. In Invoke Lambda function (Chiama una funzione Lambda) per questo tutorial puoi scegliere una delle due opzioni seguenti.
 - Seleziona Scegli tra le funzioni nel tuo account, dopodiché scegli la funzione Lambda creata nella [Fase 4](#) (ad esempio, **tutorial-object-lambda-function**) dall'elenco a discesa Funzione Lambda.
 - Scegli Inserisci ARN, quindi inserisci il nome della risorsa Amazon (ARN) della funzione Lambda creata nella [Fase 4](#).
8. In Lambda function version (Versione delle funzioni Lambda), scegli \$LATEST (l'ultima versione della funzione Lambda creata nella [Fase 4](#)).
9. (Facoltativo) Se hai bisogno che la tua funzione Lambda riconosca ed elabori le richieste GET con intestazioni con intervalli e numeri di parte, seleziona Lambda function supports requests using range (La funzione Lambda supporta le richieste che utilizzano l'intervallo) e Lambda function supports requests using part numbers (La funzione Lambda supporta le richieste che utilizzano numeri di parte). Altrimenti, deseleziona queste due caselle di controllo.

Per ulteriori informazioni sull'utilizzo di intervalli o numeri di parte con Lambda per oggetti S3, consulta [Lavorare con Intervallo and Numero del pezzo headers](#).

10. (Facoltativo) In Payload - optional (Payload - facoltativo), aggiungi il testo JSON per fornire alla tua funzione Lambda ulteriori informazioni.

Un payload è un testo JSON opzionale che puoi fornire alla tua funzione Lambda come input per tutte le chiamate provenienti da uno specifico punto di accesso Lambda per oggetti S3. Per personalizzare il comportamento di più punti di accesso Lambda per oggetti che invocano la stessa funzione Lambda, puoi configurare i payload con parametri diversi, estendendo così la flessibilità della funzione stessa.

Per ulteriori informazioni sul payload, consulta [Formato e utilizzo del contesto degli eventi](#).

11. (Facoltativo) In Parametri di richiesta - facoltativo, scegli Disabilita o Abilita per aggiungere il monitoraggio Amazon S3 al punto di accesso Lambda per oggetti. Le metriche delle richieste vengono fatturate alla tariffa standard di Amazon. CloudWatch Per ulteriori informazioni, consulta [Prezzi di CloudWatch](#).
12. In Policy del punto di accesso per le espressioni Lambda dell'oggetto - opzionale mantieni l'impostazione predefinita.

(Facoltativo) Puoi impostare una policy delle risorse. Questa policy delle risorse fornisce all'API `GetObject` l'autorizzazione per utilizzare il punto di accesso Lambda per oggetti specificato.
13. Mantieni le impostazioni rimanenti sui valori predefiniti, quindi scegli Crea punto di accesso per le espressioni Lambda dell'oggetto.

Fase 7: Visualizzazione dei dati trasformati

S3 Object Lambda è ora pronto a trasformare i tuoi dati per il tuo caso d'uso. In questo tutorial, S3 Object Lambda trasforma tutto il testo dell'oggetto in maiuscolo.

Fasi secondarie

- [Visualizzazione dei dati trasformati nel punto di accesso Lambda per oggetti S3](#)
- [Esegui uno script Python per stampare i dati originali e trasformati](#)

Visualizzazione dei dati trasformati nel punto di accesso Lambda per oggetti S3

Quando si richiede di recuperare un file attraverso il proprio punto di accesso Lambda per oggetti S3, si effettua una chiamata API `GetObject` a Lambda per oggetti S3. S3 Object Lambda richiama la funzione Lambda per trasformare i dati, dopodiché restituisce i dati trasformati come risposta alla chiamata API `GetObject` S3 standard.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Object Lambda Access Points (Punti di accesso Object Lambda).
3. Nella pagina Punti di accesso Lambda dell'oggetto scegli il punto di accesso Lambda per oggetti S3 creato nella [Fase 6](#) (ad esempio, **tutorial-object-lambda-accesspoint**).
4. Nella scheda Oggetti del punto di accesso Lambda per oggetti S3, seleziona il file con lo stesso nome (ad esempio, `tutorial.txt`) di quello che hai caricato nel bucket S3 nella [Fase 2](#).

Questo file deve contenere tutti i dati trasformati.

5. Per visualizzare i dati trasformati, scegli Open (Apri) o Download (Scarica).

Esegui uno script Python per stampare i dati originali e trasformati

Puoi utilizzare S3 Object Lambda con le tue applicazioni esistenti. A tale scopo, aggiorna la configurazione dell'applicazione in modo da utilizzare l'ARN del nuovo punto di accesso Lambda per oggetti S3 creato nella [Fase 6](#) per recuperare i dati da S3.

Il seguente script Python di esempio stampa sia i dati originali dal bucket S3 sia i dati trasformati dal punto di accesso Lambda per oggetti S3.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Object Lambda Access Points (Punti di accesso Object Lambda).
3. Nella pagina Punti di accesso Lambda dell'oggetto scegli il pulsante di opzione a sinistra del punto di accesso Lambda per oggetti S3 creato nella [Fase 6](#) (ad esempio, **tutorial-object-lambda-accesspoint**).
4. Scegli Copy ARN (Copia ARN).
5. Salva l'ARN per utilizzarlo in un secondo momento.
6. Scrivi uno script Python sul tuo computer locale per stampare sia i dati originali (ad esempio, `tutorial.txt`) dal tuo bucket S3 sia i dati trasformati (ad esempio, `tutorial.txt`) dal punto di accesso Lambda per oggetti S3. Puoi utilizzare il seguente script di esempio.

```
import boto3
from botocore.config import Config
```

```
s3 = boto3.client('s3', config=Config(signature_version='s3v4'))

def getObject(bucket, key):
    objectBody = s3.get_object(Bucket = bucket, Key = key)
    print(objectBody["Body"].read().decode("utf-8"))
    print("\n")

print('Original object from the S3 bucket:')
# Replace the two input parameters of getObject() below with
# the S3 bucket name that you created in Step 1 and
# the name of the file that you uploaded to the S3 bucket in Step 2
getObject("tutorial-bucket",
         "tutorial.txt")

print('Object transformed by S3 Object Lambda:')
# Replace the two input parameters of getObject() below with
# the ARN of your S3 Object Lambda Access Point that you saved earlier and
# the name of the file with the transformed data (which in this case is
# the same as the name of the file that you uploaded to the S3 bucket
# in Step 2)
getObject("arn:aws:s3-object-lambda:us-west-2:111122223333:accesspoint/tutorial-
object-lambda-accesspoint",
         "tutorial.txt")
```

7. Salva il tuo script Python con un nome personalizzato (ad esempio, `tutorial_print.py`) nella cartella (ad esempio, `object-lambda`) che hai creato nella [Fase 4](#) sul computer locale.
8. Nel terminale locale, esegui il seguente comando dalla root della directory (ad esempio, `object-lambda`) che hai creato nella [Fase 4](#).

```
python3 tutorial_print.py
```

Dovresti vedere sia i dati originali sia i dati trasformati (tutto il testo in maiuscolo) attraverso il terminale. Per esempio l'output visualizzato sarà simile al testo seguente.

```
Original object from the S3 bucket:
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.

Object transformed by S3 Object Lambda:
AMAZON S3 OBJECT LAMBDA TUTORIAL:
```

YOU CAN ADD YOUR OWN CODE TO PROCESS DATA RETRIEVED FROM S3 BEFORE RETURNING IT TO AN APPLICATION.

Fase 8: Pulizia

Se hai trasformato i dati attraverso S3 Object Lambda solo come esercizio di apprendimento, elimina le risorse AWS che hai allocato per non accumulare più addebiti.

Fasi secondarie

- [Eliminazione del punto di accesso Lambda per oggetti](#)
- [Eliminazione del punto di accesso S3](#)
- [Eliminazione del ruolo di esecuzione per la funzione Lambda](#)
- [Eliminazione della funzione Lambda](#)
- [Elimina il gruppo di CloudWatch log](#)
- [Eliminazione del file originale nel bucket S3 di origine](#)
- [Eliminazione del bucket S3 di origine](#)
- [Eliminazione dell'utente IAM](#)

Eliminazione del punto di accesso Lambda per oggetti

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Object Lambda Access Points (Punti di accesso Object Lambda).
3. Nella pagina Punti di accesso Lambda dell'oggetto scegli il pulsante di opzione a sinistra del punto di accesso Lambda per oggetti S3 creato nella [Fase 6](#) (ad esempio, **tutorial-object-lambda-accesspoint**).
4. Scegliere Elimina.
5. Conferma di voler eliminare il punto di accesso Lambda per oggetti inserendone il nome nel campo di testo che viene visualizzato, quindi scegli Elimina.

Eliminazione del punto di accesso S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Points (Punti di accesso).
3. Passa al punto di accesso creato nella [Fase 3](#) (ad esempio, **tutorial-access-point**), quindi scegli il pulsante di opzione accanto al nome del punto di accesso.
4. Scegliere Elimina.
5. Conferma di voler eliminare il punto di accesso inserendone il nome nel campo di testo che viene visualizzato, quindi scegli Delete (Elimina).

Eliminazione del ruolo di esecuzione per la funzione Lambda

1. Accedi Console di gestione AWS e apri la AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>.
2. Nel pannello di navigazione a sinistra, scegli Functions (Funzioni).
3. Scegli la funzione creata nella [Fase 4](#) (ad esempio, **tutorial-object-lambda-function**).
4. Nella pagina dei dettagli della funzione Lambda, scegli la scheda Configuration (Configurazione), quindi scegli Permissions (Autorizzazioni) nel pannello di navigazione a sinistra.
5. In Execution role (Ruolo di esecuzione) scegli il collegamento Role Name (Nome ruolo). Si apre la console IAM.
6. Nella pagina Summary (Riepilogo) della console IAM del ruolo di esecuzione della funzione Lambda, scegli Delete role (Elimina ruolo).
7. Nella finestra di dialogo Delete role (Elimina ruolo), scegli Yes, Delete (Sì, elimina).

Eliminazione della funzione Lambda

1. Nella AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>, scegli Funzioni nel riquadro di navigazione a sinistra.
2. Seleziona la casella di controllo a sinistra del nome della funzione creata nella [Fase 4](#) (ad esempio, **tutorial-object-lambda-function**).
3. Scegli Azioni, quindi Elimina.
4. Nella finestra di dialogo Delete function (Elimina funzione), scegli Delete (Elimina).

Elimina il gruppo di CloudWatch log

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel pannello di navigazione a sinistra, scegli Log groups (Gruppi di log).
3. Individua il gruppo di log il cui nome termina con la funzione Lambda creata nella [Fase 4](#) (ad esempio, **tutorial-object-lambda-function**).
4. Seleziona la casella di controllo a sinistra del nome del gruppo di registri.
5. Scegli Actions (Operazioni), quindi scegli Delete log group(s) (Elimina gruppi di log).
6. Nella finestra di dialogo Delete log group(s) (Elimina gruppo/i di log) scegli Delete (Elimina).

Eliminazione del file originale nel bucket S3 di origine

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket name (Nome bucket) scegli il nome del bucket su cui hai caricato il file originale nella [Fase 2](#) (ad esempio, **tutorial-bucket**).
4. Seleziona la casella di controllo a sinistra del nome dell'oggetto da eliminare (ad esempio, **tutorial.txt**).
5. Scegliere Elimina.
6. Nella pagina Delete objects (Elimina oggetti), nella sezione Permanently delete objects? (Eliminare definitivamente gli oggetti?) conferma che desideri eliminare questo oggetto inserendo **permanently delete** nella casella di testo.
7. Scegliere Delete objects (Elimina oggetti).

Eliminazione del bucket S3 di origine

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) seleziona il pulsante di opzione accanto al nome del bucket creato nella [Fase 1](#) (ad esempio, **tutorial-bucket**).
4. Scegliere Elimina.

5. Nella pagina Delete bucket (Elimina bucket) conferma che desideri eliminare il bucket inserendone il nome nel campo di testo e quindi scegli Delete bucket (Elimina bucket).

Eliminazione dell'utente IAM

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione a sinistra, scegli Users (Utenti), quindi seleziona la casella di controllo accanto al nome utente che desideri eliminare.
3. Scegliere Elimina.
4. Nella sezione Elimina **user name**? nella finestra di dialogo, inserisci il nome utente nel campo di immissione del testo per confermare l'eliminazione dell'utente. Scegliere Elimina.

Fasi successive

Dopo aver completato questo tutorial, puoi personalizzare la funzione Lambda per il tuo caso d'uso in modo da modificare i dati restituiti dalle richieste GET S3 standard.

Di seguito è riportato un elenco di casi d'uso comuni per S3 Object Lambda:

- Mascheramento dei dati sensibili per la sicurezza e la conformità.

Per ulteriori informazioni, consulta [Tutorial: rilevamento e oscuramento dei dati PII con S3 Object Lambda e Amazon Comprehend](#).

- Filtraggio di determinate righe di dati per fornire informazioni specifiche.
- Arricchimento dei dati con informazioni provenienti da altri servizi o database.
- Conversione tra formati di dati, come la conversione di XML in JSON per la compatibilità delle applicazioni.
- Compressione o decompressione dei file durante il download.
- Ridimensionamento delle immagini e creazione della filigrana.

Per ulteriori informazioni, consulta [Tutorial: utilizzo di S3 Object Lambda per aggiungere filigrane alle immagini in modo dinamico man mano che vengono recuperate](#).

- Implementazione di regole di autorizzazione personalizzate per accedere ai dati.

Per ulteriori informazioni su S3 Object Lambda, consulta [Trasformazione di oggetti con S3 Object Lambda](#).

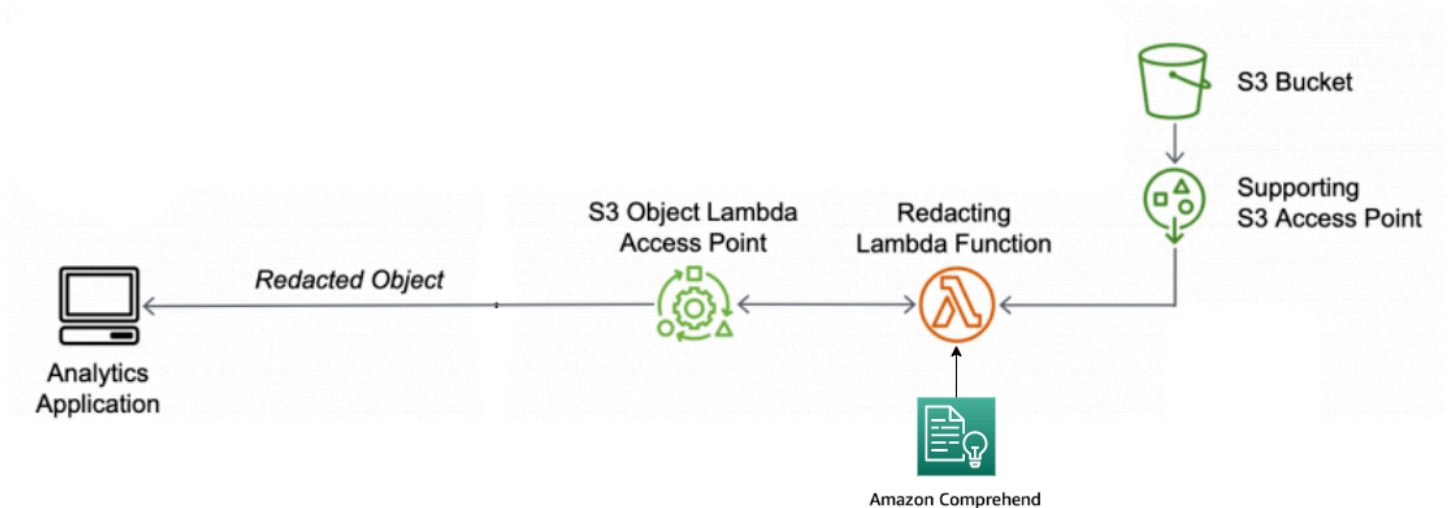
Tutorial: rilevamento e oscuramento dei dati PII con S3 Object Lambda e Amazon Comprehend

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni partner Partner Network (APN). AWS Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Quando utilizzi Amazon S3 per set di dati condivisi per l'accesso di più applicazioni e utenti, è importante limitare le informazioni privilegiate, ad esempio le informazioni personali di identificazione (PII), solo alle entità autorizzate. Ad esempio, quando un'applicazione di marketing utilizza alcuni dati contenenti PII, in primo luogo potrebbe essere necessario mascherare i dati PII per soddisfare i requisiti di privacy dei dati. Inoltre, quando un'applicazione di analisi dei dati utilizza un set di dati di inventario con ordine di produzione, in primo luogo potrebbe essere necessario oscurare le informazioni della carta di credito del cliente per evitare perdite di dati non intenzionali.

Con [S3 Object Lambda](#) e una funzione AWS Lambda precostituita basata su Amazon Comprehend, puoi proteggere i dati PII recuperati da S3 prima di restituirli a un'applicazione. Nello specifico, puoi utilizzare la [funzione Lambda](#) precostituita come funzione di oscuramento e allegarla a un punto di accesso Lambda per oggetti S3. Quando un'applicazione (ad esempio un'applicazione di analisi) invia [richieste GET S3 standard](#), queste richieste effettuate tramite il punto di accesso Lambda per oggetti S3 invocano la funzione Lambda di oscuramento predefinita per rilevare e oscurare i dati PII recuperati da un'origine dati sottostante attraverso un punto di accesso S3 di supporto. Quindi, il punto di accesso Lambda per oggetti S3 restituisce il risultato oscurato all'applicazione.



Nel processo, la funzione Lambda preconstituita utilizza [Amazon Comprehend](#), un servizio di elaborazione del linguaggio naturale (NLP, Natural Language Processing), per acquisire variazioni nel modo in cui le PII sono rappresentate, indipendentemente dall'esistenza di PII nel testo (ad esempio in numeri o come combinazione di parole e numeri). Amazon Comprehend può anche utilizzare il contesto del testo per capire se un numero di 4 cifre è un PIN, gli ultimi quattro numeri di un numero di previdenza sociale (SSN) o un anno. Amazon Comprehend elabora qualsiasi file di testo in UTF-8 formato ed è in grado di proteggere le PII su larga scala senza compromettere la precisione. Per ulteriori informazioni, consulta [Cos'è Amazon Comprehend?](#) nella Guida per Developer di Amazon Comprehend.

Obiettivo

In questo tutorial, imparerai a utilizzare S3 Object Lambda con la funzione Lambda preconstituita `ComprehendPiiRedactionS3ObjectLambda`. Questa funzione utilizza Amazon Comprehend per rilevare entità PII. Oscurare quindi queste entità sostituendole con asterischi. Oscurando le PII, si nascondono i dati sensibili, cosa che può contribuire alla sicurezza e alla conformità.

Imparerai anche a utilizzare e configurare una AWS Lambda funzione predefinita in modo che funzioni insieme a S3 Object [AWS Serverless Application Repository](#) Lambda per una facile distribuzione.

Argomenti

- [Prerequisiti: creazione di un utente IAM con autorizzazioni](#)
- [Fase 1: Creazione di un bucket S3](#)
- [Fase 2: Caricamento di un file nel bucket S3](#)

- [Fase 3: Creazione di un punto di accesso S3](#)
- [Fase 4: Configurazione e implementazione di una funzione Lambda precostituita](#)
- [Fase 5: Creazione di un punto di accesso Lambda per oggetti S3](#)
- [Fase 6: Utilizzo del punto di accesso Lambda per oggetti S3 per recuperare il file oscurato](#)
- [Fase 7: pulire](#)
- [Fasi successive](#)

Prerequisiti: creazione di un utente IAM con autorizzazioni

Prima di iniziare questo tutorial, devi disporre di un AWS account a cui puoi accedere come AWS Identity and Access Management utente (utente IAM) con le autorizzazioni corrette.

Puoi creare un utente IAM per il tutorial. Per completare questo tutorial, l'utente IAM deve allegare le seguenti politiche IAM per accedere alle AWS risorse pertinenti ed eseguire azioni specifiche.

Note

Per semplicità, questo tutorial crea e utilizza un utente IAM. Dopo aver completato il tutorial, ricordati di [Eliminazione dell'utente IAM](#). Per l'uso in produzione, consigliamo di seguire le [best practice di sicurezza in IAM](#) disponibili nella Guida per l'utente di IAM. Come best practice, richiedi agli utenti di utilizzare la federazione con un gestore dell'identità digitale per accedere a AWS utilizzando credenziali temporanee. Un'ulteriore suggerimento derivante dalle best practice è richiedere ai carichi di lavoro di utilizzare credenziali temporanee con ruoli IAM per l'accesso ad AWS. Per informazioni sull'uso della creazione Centro identità AWS IAM di utenti con credenziali temporanee, consulta la Guida [introduttiva](#) nella Guida per l'Centro identità AWS IAM utente.

Per semplicità, questo tutorial utilizza policy di accesso completo. Per l'utilizzo in produzione, è consigliabile invece concedere solo le autorizzazioni minime necessarie per il caso d'uso, in conformità con le [best practice in fatto di sicurezza](#).

Il tuo utente IAM richiede le seguenti policy AWS gestite:

- [AmazonS3FullAccess](#)— Concede le autorizzazioni per tutte le azioni di Amazon S3, incluse le autorizzazioni per creare e utilizzare un Access Point Object Lambda.
- [AWS Lambda_FullAccess](#): concede le autorizzazioni per tutte le azioni Lambda.

- [AWSCloudFormationFullAccess](#)— Concede le autorizzazioni per tutte le azioni. AWS CloudFormation
- [IAMFullAccess](#)— Concede le autorizzazioni per tutte le azioni IAM.
- [IAMAccessAnalyzerReadOnlyAccess](#)— Concede le autorizzazioni per leggere tutte le informazioni di accesso fornite da IAM Access Analyzer.

Puoi allegare direttamente queste policy esistenti durante la creazione di un utente IAM. Per ulteriori informazioni su come creare un utente IAM, consulta [Creazione di utenti IAM \(console\)](#) nella Guida per l'utente di IAM.

Inoltre, l'utente IAM richiede una policy gestita dal cliente. Per concedere all'utente IAM le autorizzazioni per tutte le AWS Serverless Application Repository risorse e le azioni, è necessario creare una policy IAM e allegare la policy all'utente IAM.

Per creare e allegare una policy IAM a un utente IAM

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione sinistro, scegli Policy.
3. Scegli Crea policy.
4. Nella scheda Visual editor (Editor visivo), in Service (Servizio), seleziona Choose a Service (Scegli un servizio). Poi, scegli Serverless Application Repository.
5. In Actions (Operazioni), sotto Manual actions (Operazioni manuali), seleziona All Serverless Application Repository actions (serverlessrepo:*) (Tutte le operazioni Serverless Application Repository (serverlessrepo:*)) per questo tutorial.

Come best practice di sicurezza, dovresti concedere le autorizzazioni solo alle operazioni e alle risorse necessarie all'utente, in base al tuo caso d'uso. Per ulteriori informazioni, consulta [Best Practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

6. In Resources (Risorse), scegli All resources (Tutte le risorse) per questo tutorial.

Come best practice, è consigliabile definire le autorizzazioni solo per risorse specifiche in account specifici. In alternativa, puoi concedere un privilegio minimo utilizzando le chiavi di condizione. Per ulteriori informazioni, consulta [Assegnare il privilegio minimo](#) nella Guida per l'utente di IAM.

7. Scegliere Next: Tags (Successivo: Tag).

8. Scegliere Next:Review (Successivo: Rivedi).
9. Nella pagina Esamina la policy digita i valori per Nome (ad esempio, **tutorial-serverless-application-repository**) e Descrizione (facoltativa) per la policy che stai creando. Esaminare il riepilogo della policy per assicurarsi di aver concesso le autorizzazioni corrette e selezionare Create policy (Crea policy) per salvare la nuova policy.
10. Nel riquadro di navigazione a sinistra, seleziona Users (Utenti). Quindi, scegli l'utente IAM per questo tutorial.
11. Nella pagina Summary (Riepilogo) dell'utente scelto, scegli la scheda Permissions (Autorizzazioni), quindi scegli Add permissions (Aggiungi autorizzazioni).
12. In Grant permissions (Concedi autorizzazioni) scegli Attach existing policies directly (Collega direttamente le policy esistenti).
13. Seleziona la casella di controllo accanto alla policy creata (ad esempio, **tutorial-serverless-application-repository**) e quindi scegli Next: Review (Successivo: Rivedi).
14. In Permissions summary (Riepilogo delle autorizzazioni) esaminare il riepilogo per accertarti di aver allegato la policy desiderata. Quindi seleziona Add permissions (Aggiungi autorizzazioni).

Fase 1: Creazione di un bucket S3

Crea un bucket per archiviare i dati originali che intendi trasformare.

Note

I punti di accesso possono essere collegati a un'altra origine dati, come un volume Amazon FSx per OpenZFS, tuttavia questo tutorial utilizza un punto di accesso di supporto collegato a un bucket S3.

Per creare un bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Scegliere Create bucket (Crea bucket).

Viene visualizzata la pagina Create bucket (Crea bucket).

4. In Bucket name (Nome bucket), inserisci un nome per il bucket (ad esempio **tutorial-bucket**).

Per ulteriori informazioni sulle regole di denominazione del bucket in Amazon S3, consulta [Regole di denominazione dei bucket per uso generico](#).

5. Per Regione, scegli la Regione AWS dove desideri che il bucket risieda.

Per ulteriori informazioni sulla Regione del bucket, consulta [Panoramica dei bucket per uso generico](#).

6. In Block Public Access settings for this bucket (Blocca le impostazioni di accesso pubblico per questo bucket), mantieni le impostazioni predefinite (è abilitato Block all public access (Blocca tutto l'accesso pubblico)).

È consigliabile di lasciare abilitate tutte le impostazioni di blocco dell'accesso pubblico, a meno che non abbia bisogno di disattivarne una o più per il caso d'uso. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

7. Mantieni le impostazioni rimanenti impostate sui valori di default.

(Facoltativo) Se desideri configurare ulteriori impostazioni del bucket per il tuo caso d'uso specifico, consulta [Creazione di un bucket per uso generico](#).

8. Seleziona Crea bucket.

Fase 2: Caricamento di un file nel bucket S3

Carica un file di testo contenente dati PII noti di vari tipi, come nomi, informazioni bancarie, numeri di telefono e SSN, nel bucket S3 quali dati originali da cui oscurare i PII più avanti in questo tutorial.

Ad esempio, puoi caricare il seguente file `tutorial.txt`. Questo è un esempio di file di input di Amazon Comprehend.

```
Hello Zhang Wei, I am John. Your AnyCompany Financial Services,
LLC credit card account 1111-0000-1111-0008 has a minimum payment
of $24.53 that is due by July 31st. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account number XXXXXX1111 with the routing number XXXXX0000.
```

```
Your latest statement was mailed to 100 Main Street, Any City,
WA 98121.
```

```
After your payment is received, you will receive a confirmation
```

text message at 206-555-0100.

If you have questions about your bill, AnyCompany Customer Service is available by phone at 206-555-0199 or email at support@anycompany.com.

Per caricare un file in un bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) scegli il nome del bucket creato nella [Fase 1](#) (ad esempio, **tutorial-bucket**) in cui caricare il file.
4. Nella scheda Oggetti del bucket seleziona Carica.
5. Nella pagina Upload (Caricamento), sotto Files and Folders (File e cartelle) scegli Add Files (Aggiungi file).
6. Seleziona un file da caricare, quindi scegli Apri. Ad esempio, puoi caricare il file di esempio `tutorial.txt` menzionato in precedenza.
7. Scegli Carica.

Fase 3: Creazione di un punto di accesso S3

Per utilizzare un punto di accesso Lambda per oggetti S3 per accedere e trasformare i dati originali, devi creare un punto di accesso S3 e associarlo al bucket S3 creato nella [Fase 1](#). Il punto di accesso deve trovarsi nella Regione AWS stesso oggetto da trasformare.

Più avanti in questo tutorial, utilizzerai questo punto di accesso come punto di accesso di supporto per il tuo punto di accesso Lambda per oggetti.

Per creare un punto di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Access Points (Punti di accesso).
3. Nella pagina Punto di accesso, scegli Crea punto di accesso.
4. Nel campo Nome del punto di accesso, inserisci il nome (ad esempio, **tutorial-pii-access-point**) del punto di accesso.

Per ulteriori informazioni sulla denominazione dei punti di accesso, consulta [Regole di denominazione dei punti di accesso](#).

5. Nel campo Origine dati inserisci il nome del bucket creato nella [Fase 1](#) (ad esempio, **tutorial-bucket**). S3 allega quindi il punto di accesso a questo bucket.

(Facoltativo) Puoi scegliere Browse S3 (Sfoglia S3) per sfogliare e cercare i bucket nell'account. Se scegli Browse S3 (Sfoglia S3), scegli il bucket desiderato e scegli Choose path (Scegli percorso) per popolare il campo Bucket name (Nome bucket) con il nome del bucket.

6. In Network origin (Origine rete), scegli Internet.

Per ulteriori informazioni sulle origini della rete per i punti di accesso, consulta [Creazione di access point limitati a un cloud privato virtuale](#).

7. Tutte le impostazioni di blocco dell'accesso pubblico sono abilitate per impostazione predefinita per il punto di accesso. È consigliabile lasciare abilitato Block all public access (Blocca tutto l'accesso pubblico). Per ulteriori informazioni, consulta [Gestione dell'accesso pubblico ai punti di accesso per bucket per uso generico](#).

8. Per tutte le altre impostazioni del punto di accesso, mantieni i valori di default.

(Facoltativo) Puoi modificare le impostazioni del punto di accesso per supportare il caso d'uso. Per questo tutorial, ti consigliamo di mantenere le impostazioni di default.

(Facoltativo) Se è necessario gestire l'accesso al punto di accesso, puoi specificare una policy per il punto di accesso. Per ulteriori informazioni, consulta [Esempi di policy per i punti di accesso](#).

9. Scegli Crea punto di accesso.

Fase 4: Configurazione e implementazione di una funzione Lambda precostituita

Per oscurare i dati PII, configura e implementa la funzione AWS Lambda precostituita ComprehendPiiRedactionS3ObjectLambda per l'utilizzo con il punto di accesso Lambda per oggetti S3.

Per configurare e implementare la funzione Lambda

1. Accedi a Console di gestione AWS e visualizza la [ComprehendPiiRedactionS3ObjectLambda](#) funzione in. AWS Serverless Application Repository

2. In Application settings (Impostazioni applicazioni), sotto Application name (Nome applicazione), mantieni il valore di default (ComprehendPiiRedactionS3ObjectLambda) per questo tutorial.

(Facoltativo) Puoi inserire il nome che desideri assegnare a questa applicazione. Puoi eseguire questa operazione se prevedi di configurare più funzioni Lambda per esigenze di accesso diverse per lo stesso set di dati condiviso.

3. Per MaskCharacter, mantieni il valore predefinito (*). Il carattere maschera sostituisce ogni carattere nell'entità PII oscurata.
4. Per MaskMode, mantieni il valore predefinito (MASK). Il MaskMode valore specifica se l'entità PII viene oscurata con il MASK carattere o il valore. PII_ENTITY_TYPE
5. Per oscurare i tipi di dati specificati, per PiiEntityTypes, mantieni il valore predefinito ALL. Il PiiEntityTypes valore specifica i tipi di entità PII da considerare per la redazione.

Per ulteriori informazioni sull'elenco dei tipi di entità PII supportati, vedi [Detect Personally Identifiable Information \(PII\)](#) nella Guida per Developer di Amazon Comprehend.

6. Mantieni le impostazioni rimanenti impostate sui valori predefiniti.

(Facoltativo) Se desideri configurare impostazioni aggiuntive per il caso d'uso specifico, consulta la sezione File readme sul lato sinistro della pagina.

7. Selezionare la casella di controllo accanto a I acknowledge that this app creates custom IAM roles (Confermo che questa app crea ruoli IAM personalizzati).
8. Seleziona Implementa.
9. Nella pagina della nuova applicazione, sotto Resources (Risorse), scegli il Logical ID (ID logico) della funzione Lambda implementata per rivedere la funzione nella pagina della funzione Lambda.

Fase 5: Creazione di un punto di accesso Lambda per oggetti S3

Un punto di accesso Lambda per oggetti S3 offre la flessibilità di richiamare una funzione Lambda direttamente da una richiesta GET S3 in modo che la funzione possa oscurare i dati PII recuperati da un punto di accesso S3. Quando crei e configuri un punto di accesso Lambda per oggetti S3, devi specificare la funzione Lambda di oscuramento da richiamare e fornire il contesto dell'evento in formato JSON come parametri personalizzati utilizzabili da Lambda.

Il contesto dell'evento fornisce informazioni relative alla richiesta eseguita nell'evento inviato da S3 Object Lambda a Lambda. Per ulteriori informazioni su tutti i campi nel contesto dell'evento, consulta [Formato e utilizzo del contesto degli eventi](#).

Per creare un punto di accesso Lambda per oggetti S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Punti di accesso Lambda dell'oggetto.
3. Nella pagina Object Lambda Access Points (Punti di accesso Object Lambda), scegli Create Object Lambda Access Point (Crea punto di accesso Object Lambda).
4. In Nome del punto di accesso per le espressioni Lambda dell'oggetto immetti il nome che desideri utilizzare per il punto di accesso Lambda per oggetti (per esempio, **tutorial-pii-object-lambda-accesspoint**).
5. Per Punto di accesso di supporto, immetti o cerca il punto di accesso standard creato al [punto 3](#) (ad esempio, **tutorial-pii-access-point**), quindi seleziona Scegli punto di accesso di supporto.
6. Per le API S3, per recuperare oggetti dal bucket S3 per l'elaborazione della funzione Lambda, seleziona. GetObject
7. Per l'invocazione della funzione Lambda, si può scegliere una delle due opzioni seguenti per questa esercitazione.
 - Seleziona Scegli tra le funzioni nel tuo account, e scegli la funzione Lambda implementata nella [Fase 4](#) (ad esempio, **serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**) dall'elenco a discesa Funzione Lambda.
 - Scegli Enter ARN (Inserisci ARN), quindi inserisci l'Amazon Resource Name (ARN) della funzione Lambda creata nella [Fase 4](#).
8. In Lambda function version (Versione delle funzioni Lambda), scegli \$LATEST (l'ultima versione della funzione Lambda implementata nella [Fase 4](#)).
9. (Facoltativo) Se hai bisogno che la tua funzione Lambda riconosca ed elabori le richieste GET con intestazioni con intervalli e numeri di parte, seleziona Lambda function supports requests using range (La funzione Lambda supporta le richieste che utilizzano l'intervallo) e Lambda function supports requests using part numbers (La funzione Lambda supporta le richieste che utilizzano numeri di parte). Altrimenti, deseleziona queste due caselle di controllo.

Per ulteriori informazioni sull'utilizzo di intervalli o numeri di parte con Lambda per oggetti S3, consulta [Lavorare con Intervallo and Numero del pezzo headers](#).

10. (Facoltativo) In Payload - optional (Payload - facoltativo), aggiungi il testo JSON per fornire alla tua funzione Lambda ulteriori informazioni.

Un payload è un testo JSON opzionale che puoi fornire alla tua funzione Lambda come input per tutte le chiamate provenienti da uno specifico punto di accesso Lambda per oggetti S3. Per personalizzare il comportamento di più punti di accesso Lambda per oggetti che invocano la stessa funzione Lambda, puoi configurare i payload con parametri diversi, estendendo così la flessibilità della funzione stessa.

Per ulteriori informazioni sul payload, consulta [Formato e utilizzo del contesto degli eventi](#).

11. (Facoltativo) In Parametri di richiesta - facoltativo, scegli Disabilita o Abilita per aggiungere il monitoraggio Amazon S3 al punto di accesso Lambda per oggetti. Le metriche delle richieste vengono fatturate alla tariffa standard di Amazon. CloudWatch Per ulteriori informazioni, consulta [Prezzi di CloudWatch](#).

12. In Policy del punto di accesso per le espressioni Lambda dell'oggetto - opzionale mantieni l'impostazione predefinita.

(Facoltativo) Puoi impostare una policy delle risorse. Questa policy delle risorse fornisce all'API `GetObject` l'autorizzazione per utilizzare il punto di accesso Lambda per oggetti specificato.

13. Mantieni le impostazioni rimanenti sui valori di default, quindi scegli `Create Object Lambda Access Point` (Crea punto di accesso Object Lambda).

Fase 6: Utilizzo del punto di accesso Lambda per oggetti S3 per recuperare il file oscurato

Ora, S3 Object Lambda è pronto a oscurare i dati PII dal file originale.

Per utilizzare il punto di accesso Lambda per oggetti S3 per recuperare il file oscurato

Quando chiedi di recuperare un file tramite il punto di accesso Lambda per oggetti S3, esegui una chiamata API `GetObject` a Lambda per oggetti S3. S3 Object Lambda richiama la funzione Lambda per oscurare i dati PII e restituisce i dati trasformati come risposta alla chiamata API `GetObject` S3 standard.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Object Lambda Access Points (Punti di accesso Object Lambda).
3. Nella pagina Punti di accesso Lambda dell'oggetto scegli il punto di accesso Lambda per oggetti S3 creato nella [Fase 5](#) (ad esempio, **tutorial-pii-object-lambda-accesspoint**).

4. Nella scheda Oggetti del punto di accesso Lambda per oggetti S3, seleziona il file con lo stesso nome (ad esempio, tutorial.txt) di quello che hai caricato nel bucket S3 nella [Fase 2](#).

Questo file deve contenere tutti i dati trasformati.

5. Per visualizzare i dati trasformati, scegli Open (Apri) o Download (Scarica).

Dovresti visualizzare il file oscurato, come mostrato nell'esempio seguente.

```
Hello *****. Your AnyCompany Financial Services,
LLC credit card account ***** has a minimum payment
of $24.53 that is due by *****. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account ***** with the routing number *****.

Your latest statement was mailed to *****.
After your payment is received, you will receive a confirmation
text message at *****.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at ***** or
email at *****.
```

Fase 7: pulire

Se hai oscurato i tuoi dati tramite S3 Object Lambda solo come esercizio di apprendimento, elimina le AWS risorse che hai allocato in modo da non accumulare più addebiti.

Fasi secondarie

- [Eliminazione del punto di accesso Lambda per oggetti](#)
- [Eliminazione del punto di accesso S3](#)
- [Eliminazione della funzione Lambda](#)
- [Elimina il gruppo di CloudWatch log](#)
- [Eliminazione del file originale nel bucket S3 di origine](#)
- [Eliminazione del bucket S3 di origine](#)
- [Eliminazione del ruolo IAM per la funzione Lambda](#)
- [Eliminazione dei criteri gestiti dal cliente per l'utente IAM](#)
- [Eliminazione dell'utente IAM](#)

Eliminazione del punto di accesso Lambda per oggetti

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Object Lambda Access Points (Punti di accesso Object Lambda).
3. Nella pagina Punti di accesso Lambda dell'oggetto scegli il pulsante di opzione a sinistra del punto di accesso Lambda per oggetti S3 creato nella [Fase 5](#) (ad esempio, **tutorial-pii-object-lambda-accesspoint**).
4. Scegliere Elimina.
5. Conferma di voler eliminare il punto di accesso Lambda per oggetti inserendone il nome nel campo di testo che viene visualizzato, quindi scegli Elimina.

Eliminazione del punto di accesso S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Points (Punti di accesso).
3. Passa al punto di accesso creato nella [Fase 3](#) (ad esempio, **tutorial-pii-access-point**), quindi scegli il pulsante di opzione accanto al nome del punto di accesso.
4. Scegliere Elimina.
5. Conferma di voler eliminare il punto di accesso inserendone il nome nel campo di testo che viene visualizzato, quindi scegli Delete (Elimina).

Eliminazione della funzione Lambda

1. Nella AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>, scegli Funzioni nel riquadro di navigazione a sinistra.
2. Scegli la funzione creata nella [Fase 4](#) (ad esempio, **serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**).
3. Scegli Azioni, quindi Elimina.
4. Nella finestra di dialogo Delete function (Elimina funzione), scegli Delete (Elimina).

Elimina il gruppo di CloudWatch log

1. Aprire la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel pannello di navigazione a sinistra, scegli Log groups (Gruppi di log).
3. Individua il gruppo di registri il cui nome termina con la funzione Lambda creata nella [Fase 4](#) (ad esempio, **serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**).
4. Scegli Actions (Operazioni), quindi scegli Delete log group(s) (Elimina gruppi di registri).
5. Nella finestra di dialogo Delete log group(s) (Elimina gruppo/i di log) scegli Delete (Elimina).

Eliminazione del file originale nel bucket S3 di origine

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket name (Nome bucket) scegli il nome del bucket su cui hai caricato il file originale nella [Fase 2](#) (ad esempio, **tutorial-bucket**).
4. Seleziona la casella di controllo a sinistra del nome dell'oggetto da eliminare (ad esempio, `tutorial.txt`).
5. Scegliere Elimina.
6. Nella pagina Delete objects (Elimina oggetti), nella sezione Permanently delete objects? (Eliminare definitivamente gli oggetti?) conferma che desideri eliminare questo oggetto inserendo **permanently delete** nella casella di testo.
7. Scegliere Delete objects (Elimina oggetti).

Eliminazione del bucket S3 di origine

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) scegli il pulsante di opzione accanto al nome del bucket creato nella [Fase 1](#)(ad esempio,**tutorial-bucket**).
4. Scegliere Elimina.
5. Nella pagina Delete bucket (Elimina bucket) conferma che desideri eliminare il bucket inserendone il nome nel campo di testo e quindi scegli Delete bucket (Elimina bucket).

Eliminazione del ruolo IAM per la funzione Lambda

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione a sinistra, scegli Roles (Ruoli), quindi seleziona la casella di controllo accanto al nome del ruolo che desideri eliminare. Il nome del ruolo inizia con il nome della funzione Lambda implementata nella [Fase 4](#) (ad esempio, **serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**).
3. Scegliere Elimina.
4. Nella casella di dialogo Delete (Elimina), inserisci il nome del ruolo nel campo di inserimento del testo per confermare l'eliminazione. Quindi, scegli Elimina.

Eliminazione dei criteri gestiti dal cliente per l'utente IAM

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione sinistro, scegli Policy.
3. Nella pagina Policies (Policy) inserisci il nome della policy gestita dal cliente creata nei [Prerequisiti](#) (ad esempio, **tutorial-serverless-application-repository**) nella casella di ricerca per filtrare l'elenco di policy. Seleziona il pulsante di opzione accanto al nome della policy che desideri eliminare.
4. Scegli Azioni, quindi Elimina.
5. Conferma di voler eliminare questa policy inserendone il nome nel campo di testo che viene visualizzato, quindi scegli Delete (Elimina).

Eliminazione dell'utente IAM

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione a sinistra, scegli Users (Utenti), quindi seleziona la casella di controllo accanto al nome utente che desideri eliminare.
3. Scegliere Elimina.
4. Nella sezione Elimina **user name**? nella finestra di dialogo, inserisci il nome utente nel campo di immissione del testo per confermare l'eliminazione dell'utente. Scegliere Elimina.

Fasi successive

Dopo aver completato questo tutorial, puoi esplorare altri casi d'uso correlati:

- Puoi creare più punti di accesso Lambda per oggetti S3 e abilitarli con funzioni Lambda precostituite configurate in modo diverso per oscurare specifici tipi di PII a seconda delle esigenze aziendali di chi accede ai dati.

Ogni tipo di utente assume un ruolo IAM e ha accesso solo a un punto di accesso Lambda per oggetti S3 (gestito tramite policy IAM). Quindi, collega ogni funzione Lambda `ComprehendPiiRedactionS3ObjectLambda` configurata per un diverso caso d'uso di oscuramento a un diverso punto di accesso Lambda per oggetti S3. Per ogni punto di accesso Lambda per oggetti S3, puoi disporre di un punto di accesso S3 di supporto per leggere i dati da un bucket S3 che archivia il set di dati condiviso.

Per ulteriori informazioni su come creare una policy di bucket S3 che consenta agli utenti di leggere dal bucket solo tramite i punti di accesso S3, consulta [Configurazione delle policy IAM per l'utilizzo degli access point](#).

Per ulteriori informazioni su come concedere a un utente l'autorizzazione per accedere alla funzione Lambda, al punto di accesso S3 e al punto di accesso Lambda per oggetti S3, consulta [Configurazione delle policy IAM per i punti di accesso Lambda per oggetti](#).

- Puoi creare una funzione Lambda personalizzata e utilizzarla in S3 Object Lambda per soddisfare le tue esigenze specifiche relative ai dati.

Ad esempio, per esplorare vari valori di dati, puoi utilizzare S3 Object Lambda e la funzione Lambda personalizzata che utilizza ulteriori [funzionalità di Amazon Comprehend](#), come il riconoscimento delle entità, il riconoscimento delle frasi chiave, l'analisi del sentimento e la classificazione dei documenti, per elaborare i dati. Puoi anche utilizzare S3 Object Lambda insieme ad [Amazon Comprehend Medical](#), un servizio di HIPAA-eligible PNL, per analizzare ed estrarre dati in modo contestuale.

Per ulteriori informazioni su come trasformare i dati con S3 Object Lambda e sulla funzione Lambda personalizzata, consulta [Tutorial: trasformazione dei dati per l'applicazione con S3 Object Lambda](#).

Debug e risoluzione dei problemi di Lambda per oggetti S3

Note

A partire dal 7 novembre 2025, S3 Object Lambda è disponibile solo per i clienti esistenti che attualmente utilizzano il servizio e per alcuni partner Partner Network (APN). AWS Per funzionalità simili a Lambda per oggetti S3, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

Le richieste ai punti di accesso Amazon S3 Object Lambda possono comportare una nuova risposta di errore quando si verificano problemi con l'invocazione o l'esecuzione della funzione Lambda. Questi errori seguono lo stesso formato degli errori Amazon S3 standard. Per informazioni sugli errori di S3 Object Lambda, consulta la sezione [Elenco dei codici di errore di S3 Object Lambda](#) nei riferimenti all'API di Amazon Simple Storage Service.

Per ulteriori informazioni sul debug generale delle funzioni Lambda, consulta [Monitoraggio e risoluzione dei problemi delle applicazioni Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

Per informazioni sugli errori standard di Amazon S3, consulta la sezione [Risposte agli errori](#) nei riferimenti all'API di Amazon Simple Storage Service.

Puoi abilitare le metriche delle richieste in Amazon CloudWatch per i tuoi access point Object Lambda. Queste metriche possono essere utilizzate per monitorare le prestazioni operative del punto di accesso. È possibile abilitare le metriche delle richieste durante o dopo la creazione del punto di accesso Lambda per oggetti. Per ulteriori informazioni, consulta [Metriche di richiesta S3 Object Lambda in CloudWatch](#).

Puoi abilitare gli eventi di dati AWS CloudTrail per ottenere una registrazione più granulare sulle richieste effettuate ai punti di accesso Lambda per oggetti. Per ulteriori informazioni, consulta [Registrazione di eventi di dati per i percorsi](#) nella Guida per l'utente di AWS CloudTrail .

Per i tutorial su S3 Object Lambda, consulta quanto segue:

- [Tutorial: trasformazione dei dati per l'applicazione con S3 Object Lambda](#)
- [Tutorial: rilevamento e oscuramento dei dati PII con S3 Object Lambda e Amazon Comprehend](#)
- [Tutorial: utilizzo di S3 Object Lambda per aggiungere filigrane alle immagini in modo dinamico man mano che vengono recuperate](#)

Per ulteriori informazioni sui punti di accesso standard, consulta la sezione [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

Per informazioni sull'utilizzo di bucket, consulta [Panoramica dei bucket per uso generico](#). Per informazioni sull'utilizzo di oggetti, consulta [Panoramica degli oggetti di Amazon S3](#).

Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch

È possibile utilizzare Operazioni in batch S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. Le operazioni in batch S3 possono eseguire una singola operazione su elenchi di oggetti Amazon S3 specificati. Un solo processo può eseguire l'operazione specificata su miliardi di oggetti contenenti exabyte di dati. Amazon S3 tiene traccia dei progressi, invia notifiche e archivia un report dettagliato sul completamento di tutte le azioni, offrendo un'esperienza completamente gestita, verificabile e serverless. Puoi utilizzare S3 Batch Operations tramite la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Usa S3 Batch Operations per copiare oggetti, aggiornare la crittografia degli oggetti sul lato server e impostare i tag degli oggetti o gli elenchi di controllo degli accessi (ACL). È inoltre possibile avviare il ripristino degli oggetti da S3 Glacier Flexible Retrieval o richiamare una funzione per eseguire azioni personalizzate utilizzando gli oggetti. AWS Lambda Puoi eseguire queste operazioni su un elenco personalizzato di oggetti oppure utilizzare un report di Amazon S3 Inventory per generare facilmente liste di oggetti. Operazioni in batch Amazon S3 utilizza le stesse operazioni API di Amazon S3 già utilizzate con Amazon S3.

Note

Per ulteriori informazioni sull'uso della classe di storage Amazon S3 Express One Zone con i bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#). Per ulteriori informazioni sull'utilizzo delle Operazioni in batch con S3 Express One Zone e bucket di directory, consulta [Utilizzo di Operazioni in batch con i bucket di directory](#).

Nozioni di base sulle operazioni in batch S3

È possibile utilizzare Operazioni in batch S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. Le operazioni in batch S3 possono eseguire una singola operazione su elenchi di oggetti Amazon S3 specificati.

Terminologia

In questa sezione si utilizzano i termini manifesto, processo, operazione e attività, definiti come segue:

Manifesto

Un manifesto è un oggetto Amazon S3 che contiene le chiavi dell'oggetto su cui si desidera che Amazon S3 agisca. Se si desidera creare un processo di Operazioni in batch, è necessario fornire un manifesto. Il manifesto generato dall'utente deve contenere il nome del bucket, la chiave dell'oggetto e, facoltativamente, la versione dell'oggetto per ogni oggetto. Se si fornisce un manifesto generato dall'utente, deve essere sotto forma di un report di Inventario Amazon S3 o di un file CSV.

È anche possibile fare in modo che Amazon S3 generi automaticamente un manifesto in base ai criteri di filtro degli oggetti specificati durante la creazione del processo. Questa opzione è disponibile per i processi Batch Operations creati utilizzando la console Amazon S3 o per qualsiasi tipo di processo creato utilizzando AWS Command Line Interface (AWS CLI), AWS SDK o l'API REST di Amazon S3.

Processo

Un processo è l'unità di lavoro di base per le operazioni in batch S3. Un processo include tutte le informazioni necessarie per eseguire l'operazione specificata sugli oggetti elencati nel file manifest. Una volta fornite queste informazioni e richiesto l'inizio del processo, il processo esegue l'operazione specificata su ciascun oggetto del manifest.

Operazione

L'operazione è il tipo di [operazione](#) API, ad esempio la copia di oggetti, che desideri venga eseguita dal processo Batch Operations. Ogni processo esegue un singolo tipo di operazione in tutti gli oggetti specificati nel manifest.

Attività

Un'attività è l'unità di esecuzione per un processo. Un'attività rappresenta una singola chiamata a un'operazione Amazon S3 o AWS Lambda API per eseguire l'operazione del lavoro su un singolo oggetto. Nel corso del ciclo di vita di un processo, le operazioni in batch S3 creano un'unica attività per ogni oggetto specificato nel manifest.

Funzionamento di un processo Batch S3 Operations

Un processo è l'unità di lavoro di base per le operazioni in batch S3. Un processo include tutte le informazioni necessarie per eseguire l'operazione specificata su un elenco di oggetti. Per creare un processo, devi fornire alle operazioni in batch S3 un elenco di oggetti e specificare l'operazione da eseguire su tali oggetti. Per informazioni sulle operazioni in batch supportate da S3, consulta [Operazioni supportate dalle operazioni in batch S3](#).

Un processo batch esegue un'operazione specifica su ogni oggetto incluso nel suo manifesto. Un manifest elenca gli oggetti che si desidera elaborare con un processo batch e viene memorizzato come oggetto in un bucket. Puoi utilizzare report in formato CSV (comma-separated values, valori separati da virgola) [Catalogazione e analisi dei dati con Inventario S3](#) come manifest per semplificare la creazione di elenchi di oggetti di grandi dimensioni presenti in un bucket. È anche possibile specificare un manifest in un formato CSV semplice che consente di eseguire operazioni batch su un elenco personalizzato di oggetti contenuti in un singolo bucket.

Dopo aver creato un processo, Amazon S3 elabora l'elenco di oggetti nel manifest ed esegue l'operazione specificata su ogni oggetto. Durante l'esecuzione di un processo, puoi monitorarne lo stato a livello di programmazione o tramite la console Amazon S3. È anche possibile configurare un processo affinché generi un rapporto di completamento al termine della sua esecuzione. Il rapporto di completamento descrive i risultati di ciascuna attività eseguita dal processo. Per ulteriori informazioni sul monitoraggio dei processi, consulta [Gestione dei processi di operazioni in batch Amazon S3](#).

Operazioni in batch S3 prevede dei costi. Ti viene addebitato il costo della creazione dei processi Operazioni in batch, inclusi quelli che vengono annullati prima del completamento. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Per impostazione predefinita, i processi Operazioni in batch S3 possono elaborare fino a 4 miliardi di oggetti per tutte le operazioni. In particolare, i job Copy, Object Tagging, Object Lock, che richiamano una AWS Lambda funzione e Batch Replication, possono supportare fino a 20 miliardi di oggetti. È previsto un limite di 6 processi di replica in batch attivi per account. AWS Per iniziare a creare un processo Operazioni in batch S3, consulta [Creazione di un processo Operazioni in batch S3](#).

Tutorial su Operazioni in batch S3

I seguenti tutorial illustrano le procedure complete end-to-end per alcune operazioni in batch.

- [Tutorial: video con S3 Batch Operations Batch-transcoding](#)

Concessione di autorizzazioni per le operazioni in batch

Prima di creare ed eseguire processi operazioni in batch S3, è necessario concedere le autorizzazioni necessarie. Per creare un processo di operazioni in batch Amazon S3, è necessaria l'autorizzazione utente `s3:CreateJob`. La stessa entità che crea il job deve inoltre avere l'`iam:PassRole` autorizzazione a passare il ruolo AWS Identity and Access Management (IAM) specificato per il job a Batch Operations.

Nelle sezioni seguenti vengono fornite informazioni sulla creazione di un ruolo IAM e sul collegamento delle policy. Per informazioni generali sulla specifica delle risorse IAM, consulta [IAM JSON policy elements: Resource](#) nella IAM User Guide.

Argomenti

- [Creazione di un ruolo IAM di operazioni in batch S3](#)
- [Allegare policy di autorizzazione](#)

Creazione di un ruolo IAM di operazioni in batch S3

Perché Amazon S3 possa eseguire operazioni in batch S3 per tuo conto, occorre concedergli le opportune autorizzazioni. Concedi queste autorizzazioni tramite un ruolo AWS Identity and Access Management (IAM). Quando crei un job S3 Batch Operations, specifichi il ruolo IAM che desideri che il job utilizzi. Questo può essere un ruolo IAM esistente. Oppure, se utilizzi la console Amazon S3 per creare il job, può essere un ruolo IAM creato da Amazon S3 per te.

Se scegli di lasciare che Amazon S3 crei il ruolo IAM per te, crea e allega automaticamente politiche di fiducia e autorizzazioni al ruolo. La policy di fiducia consente al responsabile del servizio S3 Batch Operations (`batchoperations.s3.amazonaws.com`) di assumere il ruolo. La politica delle autorizzazioni consente tutte le azioni necessarie per l'esecuzione del job, in base alle impostazioni specificate per il job. Ad esempio, se configuri un processo per copiare oggetti da un bucket a un altro bucket del tuo Account AWS, la politica delle autorizzazioni consente azioni come `s3:GetObject` e `s3:PutObject`. È possibile rivedere le politiche di attendibilità e autorizzazioni per il ruolo prima di inviare il lavoro. Questa opzione è disponibile solo se utilizzi la console Amazon S3 per creare un job e lo configuri in modo da utilizzare un elenco di oggetti generato da S3 che utilizza filtri o si basa su una configurazione di replica. Dopo aver inviato il job, il ruolo IAM rimane nel tuo account. È quindi possibile utilizzarlo nuovamente per i lavori successivi che eseguono la stessa operazione o eliminarlo al termine dell'esecuzione del lavoro.

Se preferisci creare il ruolo IAM manualmente, gli esempi di policy in questa sezione possono aiutarti a creare il ruolo. Per ulteriori informazioni sulla creazione e la configurazione dei ruoli, consulta i ruoli [IAM](#) nella IAM User Guide. Per informazioni sulle autorizzazioni per le operazioni dell'API S3 per tipo di risorsa S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#). Per ulteriori esempi, consulta e [Controllo delle autorizzazioni per le operazioni in batch utilizzando i tag di processo](#) [Copia di oggetti mediante operazioni in batch S3](#)

Nelle policy IAM è inoltre possibile utilizzare le chiavi di condizione per filtrare le autorizzazioni di accesso per i processi di operazioni in batch Amazon S3. Per ulteriori informazioni e per un elenco completo delle chiavi di condizione specifiche per Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Policy di trust

Per consentire al principale del servizio di operazioni in batch S3 di assumere il ruolo IAM, collega la seguente policy di attendibilità al ruolo.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "batchoperations.s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Allegare policy di autorizzazione

A seconda del tipo di operazioni, puoi collegare una delle policy seguenti.

Prima di configurare le autorizzazioni, tieni presente quanto segue:

- A prescindere dall'operazione, Amazon S3 necessita delle autorizzazioni per leggere l'oggetto manifest dal bucket S3 e, facoltativamente, per scrivere un report nel bucket. Quindi, tutte le policy seguenti includono queste autorizzazioni.
- Per i manifest di report di Amazon S3 Inventory, S3 Batch Operations richiede l'autorizzazione per leggere l'oggetto manifest.json e tutti i file di dati CSV associati.
- Version-specific autorizzazioni come `s3:GetObjectVersion` quelle richieste solo quando si specifica l'ID di versione degli oggetti.
- Se stai eseguendo S3 Batch Operations su oggetti crittografati, il ruolo IAM deve avere accesso anche alle AWS KMS chiavi utilizzate per crittografarli.
- Se invii un manifesto del report di inventario crittografato con AWS KMS, la tua policy IAM deve includere le autorizzazioni `"kms:Decrypt"` e `"kms:GenerateDataKey"` per l'oggetto manifest.json e tutti i file di dati CSV associati.
- Se il job Batch Operations genera un manifest in un bucket con gli elenchi di controllo degli accessi (ACL) abilitati e si trova in un altro Account AWS, devi concedere l'`s3:PutObjectAcl` autorizzazione nella policy IAM del ruolo IAM configurato per il processo batch. Se non si include questa autorizzazione, il processo batch fallisce con l'errore `Error occurred when preparing manifest: Failed to write manifest`.

Copia oggetti: PutObject

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
```

```

        "s3:GetObjectTagging",
        "s3:ListBucket"
    ],
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
    ]
}
]
}

```

Sostituisci i tag degli oggetti: PutObjectTagging

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging",

```



```

        "s3:PutObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
    ]
  }
]
}

```

Elimina i tag degli oggetti: DeleteObjectTagging

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}

```

Sostituisci l'elenco di controllo degli accessi: PutObjectAcl

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",

```

```
    "s3:GetObjectVersion"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
  ]
}
]
```

Ripristina oggetti: RestoreObject

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:RestoreObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
  ]
}
```

Applica la conservazione Object Lock: PutObjectRetention

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetBucketObjectLockConfiguration",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectRetention",
        "s3:BypassGovernanceRetention"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],

```

```

        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
        ],
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
        ]
    }
]
}

```

Applica la conservazione legale di Object Lock: PutObjectLegalHold

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:PutObjectLegalHold",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ]
        }
    ]
}

```

```

    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
    ]
}
]
}

```

Replica oggetti esistenti: InitiateReplication con un manifest generato da S3

Usa questa policy se si utilizza e si memorizza un manifesto generato da S3. Per ulteriori informazioni sull'uso delle Operazioni in batch per replicare gli oggetti esistenti, consulta [Replica di oggetti esistenti con Replica in batch](#).

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:InitiateReplication"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Action": [
                "s3:GetReplicationConfiguration",
                "s3:PutInventoryConfiguration"
            ]
        }
    ]
}

```

```

    ],
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket"
    ]
},
{
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
    ],
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    ]
}
]
}

```

Replica oggetti esistenti: `InitiateReplication` con un manifesto utente

Usa questa policy se si utilizza un manifesto fornito dall'utente. Per ulteriori informazioni sull'uso delle Operazioni in batch per replicare gli oggetti esistenti, consulta [Replica di oggetti esistenti con Replica in batch](#).

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {

```

```

    "Action": [
      "s3:InitiateReplication"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    ]
  },
  {
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
    ]
  }
]
}

```

Checksum di calcolo: consenti **GetObject**, **GetObjectVersion**, e **RestoreObject** **PutObject**

Utilizza questa policy per utilizzare l'operazione Calcola il checksum con Operazioni in batch S3. Le autorizzazioni per **GetObject**, **GetObjectVersion** e **RestoreObject** sono necessarie per ottenere e leggere i byte dei dati archiviati. Sostituisci i segnaposto per l'input dell'utente con le informazioni appropriate. Per ulteriori informazioni su Calcola il checksum, consulta [Verifica dell'integrità degli oggetti per i dati a riposo in Amazon S3](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```



```

    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:RestoreObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket2/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket3/*"
    ]
}
]
}

```

Aggiorna la crittografia degli oggetti

È necessario allegare la seguente politica di autorizzazione per consentire a Batch Operations di leggere un manifesto, aggiornare il tipo di crittografia degli oggetti e scrivere un rapporto di completamento. Per utilizzare questa politica di autorizzazione, sostituiscila *user input placeholders* con le tue informazioni. Per ulteriori informazioni sull'utilizzo di questa operazione e sulle autorizzazioni da assegnare al ruolo utilizzato dal responsabile IAM, consulta [the section called “Aggiorna la crittografia degli oggetti”](#)

```

{
    "Version": "2012-10-17",

```

```

"Statement": [{
  "Sid": "S3BatchOperationsUpdateEncryption",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:UpdateObjectEncryption"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket-target",
    "arn:aws:s3:::amzn-s3-demo-bucket-target/*"
  ]
},
{
  "Sid": "S3BatchOperationsPolicyForManifestFile",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket-manifest/*"
  ]
},
{
  "Sid": "S3BatchOperationsPolicyForCompletionReport",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket-completion-report/*"
  ]
},
{
  "Sid": "S3BatchOperationsPolicyManifestGeneration",
  "Effect": "Allow",
  "Action": [
    "s3:PutInventoryConfiguration"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket-target"
  ]
}

```

```
    }
    {
      "Sid": "AllowKMSOperationsForS3BatchOperations",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/01234567-89ab-
cdef-0123-456789abcdef"
      ]
    }
  ]
}
```

Creazione di un processo di operazioni in batch S3

Con Operazioni in batch Amazon S3, puoi eseguire operazioni in batch su larga scala su un elenco di oggetti Amazon S3 specifici. In questa sezione vengono descritte le informazioni necessarie per creare un processo S3 Batch Operations e i risultati di una richiesta `CreateJob`. Fornisce inoltre istruzioni per creare un job Batch Operations utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java

Quando crei un job S3 Batch Operations, puoi richiedere un report di completamento per tutte le attività o solo per le attività fallite. Se almeno un'attività è stata richiamata correttamente, Operazioni in batch S3 genera un report per i processi che sono stati completati, che non sono andati a buon fine o che sono stati annullati. Per ulteriori informazioni, consulta [Esempi: report di completamento delle operazioni in batch S3](#).

Argomenti

- [Elementi della richiesta di un processo di operazioni in batch](#)
- [Specifica di un manifesto](#)
- [Generazione automatica di un elenco di oggetti e salvataggio come file manifesto](#)
- [Creazione di un file manifesto](#)
- [Utilizzo di un manifesto esistente](#)
- [Creazione di un processo](#)

- [Risposte di lavoro](#)

Elementi della richiesta di un processo di operazioni in batch

Per creare un processo di operazioni in batch S3, è necessario fornire le seguenti informazioni:

Operazione

Specifica l'operazione che vuoi far eseguire alle operazioni in batch S3 sugli oggetti nel manifest. Ogni tipo di operazione accetta parametri specifici di tale operazione. Con Operazioni in batch, puoi eseguire un'operazione in blocco ottenendo gli stessi risultati come se stessi eseguendo un'operazione alla volta su ciascun oggetto.

Manifesto

Un manifesto è un elenco di oggetti Amazon S3 che contiene le chiavi degli oggetti su cui si desidera che Amazon S3 agisca. Per specificare un manifesto per un processo Operazioni in batch, puoi utilizzare i seguenti metodi:

- Configura Operazioni in batch per generare un elenco di oggetti basato sui metadati specificati. Puoi salvare questo elenco come file manifesto e utilizzarlo quando crei il processo. Questa opzione è disponibile per qualsiasi tipo di processo creato utilizzando la console Amazon S3, gli AWS SDK o l'AWS CLI API REST di Amazon S3.
- Genera automaticamente un elenco di oggetti in base a una configurazione di replica esistente. Puoi salvare questo elenco come file manifesto e utilizzarlo nuovamente per processi futuri.
- Crea un nuovo file manifesto manualmente.
- Utilizza un manifesto esistente.

Note

- Indipendentemente da come si specificano gli oggetti da utilizzare, il manifesto deve essere archiviato in un bucket per uso generico. Operazioni in batch non è in grado di importare manifesti esistenti da bucket di directory, né salvare elenchi di oggetti generati come manifesti in bucket di directory. Gli oggetti descritti all'interno del manifesto, tuttavia, possono essere archiviati in bucket di directory. Per ulteriori informazioni, consulta [Directory buckets](#).
- Se gli oggetti nel manifesto si trovano in un bucket con versione, la specifica degli ID versione per gli oggetti indirizza Operazioni in batch a eseguire l'operazione su una

versione specifica. Se nessun ID versione è specificato, Operazioni in batch esegue l'operazione sulla versione più recente degli oggetti. Se il manifesto include un campo ID versione, è necessario fornire un ID versione per tutti gli oggetti del manifesto.

Per ulteriori informazioni, consulta [Specifica di un manifest](#).

Priorità

Utilizza le priorità del processo per indicarne la priorità rispetto agli altri processi in esecuzione sul tuo account. Numeri maggiori indicano una priorità più alta.

Le priorità del lavoro hanno un significato solo rispetto alle priorità stabilite per altri lavori nello stesso account e nella stessa regione. Pertanto puoi scegliere qualsiasi sistema di numerazione utile. Ad esempio, potrebbe essere necessario assegnare a tutti i processi Ripristina (RestoreObject) la priorità 1, a tutti i processi Copia (CopyObject) la priorità 2 e a tutti i processi Sostituisci liste di controllo degli accessi (ACL) (PutObjectAcl) la priorità 3.

Operazioni in batch S3 assegna la priorità ai processi in base ai numeri di priorità ma non è garantito un ordinamento rigoroso. Pertanto, si consiglia di non utilizzare le priorità dei processi per accertarsi che un processo inizi o termini prima di un altro. Per essere certo che l'ordine venga rigidamente rispettato, attendi che un processo sia terminato prima di iniziare quello successivo.

RoleArn

Specifica un ruolo AWS Identity and Access Management (IAM) per eseguire il job. Il ruolo IAM utilizzato deve disporre di autorizzazioni sufficienti per eseguire l'operazione specificata nel job. Ad esempio, per eseguire un processo CopyObject, il ruolo IAM deve disporre dell'autorizzazione `s3:GetObject` per il bucket di origine e dell'autorizzazione `s3:PutObject` per il bucket di destinazione. Il ruolo necessita anche delle autorizzazioni per leggere il manifesto e scrivere il report di completamento.

Il ruolo IAM può essere un ruolo esistente. Oppure, se utilizzi la console Amazon S3 per creare il job, può essere un ruolo IAM che Amazon S3 crea automaticamente per te. Per ulteriori informazioni, consulta [Concessione di autorizzazioni per le operazioni in batch](#).

Per ulteriori informazioni sui ruoli IAM, consulta [Ruoli IAM](#) nella Guida per l'utente di IAM. Per ulteriori informazioni sulle autorizzazioni di Amazon S3, consulta la sezione [Azioni di policy per Amazon S3](#).

 Note

I processi Operazioni in batch che eseguono azioni su bucket di directory richiedono autorizzazioni specifiche. Per ulteriori informazioni, consulta [AWS Identity and Access Management \(IAM\) for S3 Express One Zone](#).

Report

Specifica se desideri che le operazioni in batch S3 generino un report di completamento. Se richiedi un report di completamento, dovrai inserire i parametri per il report in questo elemento. Sono necessarie le seguenti informazioni:

- Il bucket in cui desideri archiviare il report

 Note

Il report deve essere archiviato in un bucket per uso generico. Operazioni in batch non può salvare report in bucket di directory. Per ulteriori informazioni, consulta [Directory buckets](#).

- Il formato del report
- Se desideri che il report includa i dettagli di tutte le attività o solo di quelle fallite
- Una stringa di prefisso (facoltativa)

Se il campo `CreateJob.Report.ExpectedBucketOwner` viene specificato, deve corrispondere al proprietario del bucket del report di completamento. Se non corrisponde, il processo non riesce.

 Note

I report di completamento sono sempre crittografati con crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3

Tag (opzionali)

È possibile etichettare e controllare l'accesso ai processi di Operazioni in batch S3 aggiungendo tag. Puoi utilizzare tag per identificare il responsabile del processo Operazioni in batch o

controllare in che modo gli utenti interagiscono con processi Operazioni in batch. La presenza dei tag dei lavori può consentire o limitare la capacità di un utente di cancellare un lavoro, attivare un lavoro in stato di conferma o cambiare il livello di priorità di un lavoro. Ad esempio, puoi concedere a un utente l'autorizzazione per richiamare l'operazione `CreateJob`, purché il processo venga creato con il tag `"Department=Finance"`.

È possibile creare lavori con tag ad essi associati e aggiungere tag ai lavori dopo averli creati.

Per ulteriori informazioni, consulta [the section called “Utilizzo dei tag”](#).

Descrizione (facoltativa)

Per tenere traccia e monitorare il processo, è anche possibile fornire una descrizione di un massimo di 256 caratteri. Amazon S3 include questa descrizione ogni volta che restituisce informazioni su un processo o visualizza i dettagli del processo nella console di Amazon S3. Puoi quindi ordinare e filtrare i processi con facilità in base alle descrizioni che hai assegnato loro. Le descrizioni non devono necessariamente essere univoche, quindi puoi utilizzarle come categorie (ad esempio, "Registro settimanale dei processi Copy") per aiutarti a tenere traccia dei gruppi di processi simili.

Specifica di un manifest

Un manifesto è un elenco di oggetti Amazon S3 che contiene le chiavi degli oggetti su cui si desidera che Amazon S3 agisca. Per specificare un manifesto per un processo Operazioni in batch, puoi utilizzare i seguenti metodi:

- Configura Operazioni in batch per generare un elenco di oggetti basato sui metadati specificati. Puoi salvare questo elenco come manifesto e utilizzarlo quando crei il processo. Questa opzione è disponibile per qualsiasi tipo di processo creato utilizzando la console Amazon S3, gli AWS SDK o l'AWS CLI API REST di Amazon S3.
- Genera automaticamente un elenco di oggetti in base a una configurazione di replica esistente. Puoi salvare questo elenco come manifesto e utilizzarlo nuovamente per processi futuri.
- Crea un nuovo file manifesto manualmente.
- Utilizza un manifesto esistente.

 Note

- Operazioni in batch Amazon S3 non supporta la generazione di elenchi di oggetti multi-Regione.
- Indipendentemente da come si specificano gli oggetti da utilizzare, il manifesto deve essere archiviato in un bucket per uso generico. Operazioni in batch non è in grado di importare manifesti esistenti da bucket di directory, né salvare elenchi di oggetti generati come manifesti in bucket di directory. Gli oggetti descritti all'interno del manifesto, tuttavia, possono essere archiviati in bucket di directory. Per ulteriori informazioni, consulta [Directory buckets](#).

Generazione automatica di un elenco di oggetti e salvataggio come file manifesto

Puoi utilizzare Amazon S3 per generare un elenco di oggetti automaticamente in base ai metadati specificati. Puoi salvare questo elenco come manifesto e utilizzarlo quando crei il processo. Questa opzione è disponibile per qualsiasi tipo di processo creato utilizzando la console Amazon S3, gli AWS SDK o l'API AWS CLI REST di Amazon S3.

Per generare automaticamente un elenco di oggetti e salvarlo come file manifesto, è necessario specificare i seguenti elementi come parte della richiesta di creazione del processo:

- Informazioni sul bucket contenente gli oggetti di origine, inclusi il proprietario del bucket e il nome della risorsa Amazon (ARN).
- Informazioni sull'output del manifesto, incluso un flag per creare un file manifesto, il proprietario del bucket di output, l'ARN, il prefisso, il formato del file e il tipo di crittografia.
- Criteri opzionali per filtrare gli oggetti in base alla data di creazione, al nome della chiave, alla dimensione, al tipo di crittografia, all'ARN della chiave KMS, alla chiave del bucket e alla classe di archiviazione. Nel caso di processi di replica, è anche possibile utilizzare i tag per filtrare gli oggetti.

Criteri di filtro degli oggetti

Per filtrare l'elenco degli oggetti da includere in un elenco di oggetti generato automaticamente, è possibile specificare i seguenti criteri. Per ulteriori informazioni, consulta [JobManifestGeneratorFilter](#) nella documentazione di riferimento delle API di Amazon S3.

CreatedAfter

Se fornito, il manifesto generato include solo oggetti del bucket di origine creati dopo questo periodo.

CreatedBefore

Se fornito, il manifesto generato include solo oggetti del bucket di origine creati prima di questo periodo.

EligibleForReplication

Se fornito, il manifesto generato include oggetti solo se sono idonei alla replica in base alla configurazione di replica sul bucket di origine.

KeyNameConstraint

Se fornito, il manifest generato include solo oggetti bucket di origine le cui chiavi oggetto corrispondono ai vincoli di stringa specificati per, e. `MatchAnySubstring` `MatchAnyPrefix` `MatchAnySuffix`

MatchAnySubstring— Se fornito, il manifesto generato include oggetti se la stringa specificata appare ovunque all'interno della stringa chiave dell'oggetto.

MatchAnyPrefix— Se fornito, il manifesto generato include oggetti se la stringa specificata appare all'inizio della stringa chiave dell'oggetto.

MatchAnySuffix— Se fornito, il manifesto generato include oggetti se la stringa specificata appare alla fine della stringa chiave dell'oggetto.

MatchAnyObjectEncryption

Se fornito, l'elenco di oggetti generato salvato come file manifesto include solo oggetti bucket di origine con il tipo di crittografia lato server indicato (SSE-S3,, SSE-KMS DSSE-KMS SSE-C, o). NOT-SSE Se si seleziona SSE-KMS o DSSE-KMS, facoltativamente, è possibile filtrare ulteriormente i risultati specificando una chiave KMS specifica ARN. Se si seleziona SSE-KMS, è anche possibile filtrare ulteriormente i risultati in base allo stato di attivazione di Bucket Key.

Note

Per migliorare le prestazioni di generazione dei manifesti quando si utilizza il `KmsKeyArn` filtro, utilizzatelo con altri filtri per i metadati degli oggetti, come `MatchAnyPrefix`, o. `CreatedAfter` `MatchAnyStorageClass`

MatchAnyStorageClass

Se fornito, il manifesto generato include solo oggetti del bucket di origine archiviati con la classe di archiviazione specificata.

ObjectReplicationStatuses

Se fornito, il manifesto generato include solo oggetti del bucket di origine che dispongono di uno degli stati di replica specificati.

ObjectSizeGreaterThanBytes

Se fornito, il manifesto generato include solo oggetti del bucket di origine la cui dimensione file è maggiore del numero di byte specificato.

ObjectSizeLessThanBytes

Se fornito, il manifesto generato include solo oggetti del bucket di origine la cui dimensione file è minore del numero di byte specificato.

Note

Non è possibile clonare la maggior parte dei processi che hanno generato automaticamente elenchi di oggetti che sono stati salvati come manifesti. I processi di replica batch possono essere clonati, tranne quando utilizzano i criteri di filtro del manifesto `KeyNameConstraint`, `MatchAnyStorageClass`, `ObjectSizeGreaterThanBytes` o `ObjectSizeLessThanBytes`.

La sintassi per specificare i criteri del manifesto varia a seconda del metodo utilizzato per creare il processo. Per alcuni esempi, consulta [Creazione di un processo](#).

Creazione di un file manifesto

Per creare un file manifesto manualmente, specificate la chiave dell'oggetto manifesto, l'ETag (tag di entità) e l'ID di versione opzionale in un elenco. CSV-formatted Il contenuto del manifesto deve essere URL-encoded.

Per impostazione predefinita, Amazon S3 utilizza automaticamente la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) per crittografare un manifesto caricato in un bucket Amazon S3. I manifesti che utilizzano la crittografia lato server con chiavi fornite dal cliente () non

sono supportati. SSE-C I manifesti che utilizzano la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS) sono supportati solo quando si utilizzano i report di inventario. CSV-formatted L'utilizzo di un manifesto creato manualmente con AWS KMS non è supportato.

Il manifest deve contenere il nome del bucket, la chiave dell'oggetto e, facoltativamente, la versione dell'oggetto per ciascun oggetto. Gli altri campi nel manifest non vengono utilizzati dalle operazioni in batch S3.

Note

Se gli oggetti nel manifesto si trovano in un bucket con versione, la specifica degli ID versione per gli oggetti indirizza Operazioni in batch a eseguire l'operazione su una versione specifica. Se nessun ID versione è specificato, Operazioni in batch esegue l'operazione sulla versione più recente degli oggetti. Se il manifesto include un campo ID versione, è necessario fornire un ID versione per tutti gli oggetti del manifesto.

Di seguito è riportato un manifest di esempio in formato CSV senza ID versione.

```
amzn-s3-demo-bucket1,objectkey1
amzn-s3-demo-bucket1,objectkey2
amzn-s3-demo-bucket1,objectkey3
amzn-s3-demo-bucket1,photos/jpgs/objectkey4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5
amzn-s3-demo-bucket1,object%20key%20with%20spaces
```

Di seguito è riportato un manifesto di esempio in formato CSV che include ID versione.

```
amzn-s3-demo-bucket1,objectkey1,PZ9ibn9D51P6p298B7S9_ceqx1n5EJ0p
amzn-s3-demo-bucket1,objectkey2,YY_ouuAJByNW1LRBfFMfxMge7XQWxMBF
amzn-s3-demo-bucket1,objectkey3,jbo9_jhdPEyB4Rim0xWS0kU0EoNrU_oI
amzn-s3-demo-bucket1,photos/jpgs/objectkey4,6EqlikJJxLTsHsnbZbSRffn24_eh5Ny4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5,imHf3FAiRsvBW_EHB8G0u.NHunH01gVs
amzn-s3-demo-bucket1,object%20key%20with%20spaces,9HkPvDaZY5MVbMhn6TMn1YTb5ArQAo3w
```

Utilizzo di un manifesto esistente

È possibile specificare un manifesto esistente per creare un processo Operazioni in batch utilizzando uno dei due formati seguenti:

- Rapporto di inventario Amazon S3: deve essere un rapporto di inventario CSV-formatted Amazon S3. Devi specificare il file `manifest.json` associato al report di inventario. Per ulteriori informazioni sui report di inventario, consulta [Catalogazione e analisi dei dati con Inventario S3](#). Se il rapporto di inventario include gli ID di versione, S3 Batch Operations opera sulle versioni specifiche degli oggetti.

Note

- S3 Batch Operations supporta i report di inventario CSV crittografati con SSE-KMS
 - Se invii un manifesto del report di inventario crittografato con SSE-KMS, la tua policy IAM deve includere le autorizzazioni relative all'`manifest.json` oggetto `"kms:Decrypt"` e `"kms:GenerateDataKey"` a tutti i file di dati CSV associati.
- File CSV: ogni riga nel file deve includere il nome del bucket, la chiave dell'oggetto e, facoltativamente, la versione dell'oggetto. Le chiavi degli oggetti devono essere URL-encoded, come mostrato negli esempi seguenti. Il manifest deve includere gli ID versione di tutti gli oggetti oppure ometterli per tutti gli oggetti. Per ulteriori informazioni sul formato CSV del manifesto, consulta [JobManifestSpec](#) nella Documentazione di riferimento delle API Amazon Simple Storage Service.

Note

S3 Batch Operations non supporta i file manifest CSV crittografati con SSE-KMS

Important

Quando si utilizza un manifesto creato manualmente e un bucket con versione, si consiglia di specificare gli ID versione per gli oggetti. Quando crei un processo, S3 Batch Operations analizza l'intero manifest prima di eseguire il processo. Tuttavia, non esegue una "snapshot" dello stato del bucket.

Poiché i manifesti possono contenere miliardi di oggetti, l'esecuzione dei processi potrebbe richiedere molto tempo, influenzando la versione di un oggetto su cui agisce il processo.

Supponi di sovrascrivere un oggetto con una nuova versione durante l'esecuzione di un processo e di non aver specificato un ID versione per tale oggetto. In questo caso, Amazon S3 esegue l'operazione sulla versione più recente dell'oggetto, non sulla versione

che esisteva al momento della creazione del processo. L'unico modo per evitare questo comportamento è specificare gli ID versione per gli oggetti elencati nel manifest.

Creazione di un processo

Puoi creare processi S3 Batch Operations utilizzando la console Amazon S3, AWS CLI, gli AWS SDK o l'API REST di Amazon S3.

Per ulteriori informazioni sulla creazione di una richiesta di processo, consulta la sezione [Elementi della richiesta di un processo di operazioni in batch](#).

Prerequisiti

Prima di creare un processo Operazioni in batch, conferma di aver configurato le autorizzazioni pertinenti. Per ulteriori informazioni, consulta [Concessione di autorizzazioni per le operazioni in batch](#).

Utilizzo della console S3

Come creare un processo Operazioni in batch utilizzando la console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegli Operazioni in batch nel pannello di navigazione sinistro della console Amazon S3.
3. Scegli Crea processo.
4. In Scegli regione e ambito, scegli e visualizza la AWS regione in cui desideri creare il tuo lavoro.

Note

Per le operazioni di copia, è necessario creare il processo nella stessa Regione del bucket di destinazione. Per tutte le altre operazioni, è necessario creare il processo nella stessa Regione degli oggetti del manifesto.

5. Per Ambito, specifica l'elenco di oggetti su cui agirà il processo Operazioni in batch.

In Elenco oggetti, puoi scegliere di generare un manifesto utilizzando un elenco di oggetti, generare un manifesto utilizzando una configurazione di replica o utilizzare un manifesto esistente.

- Se scegli Genera un elenco di oggetti, viene generato automaticamente un elenco di oggetti in base alla posizione di origine e ai metadati specificati. Puoi salvare questo elenco come manifesto e utilizzarlo nuovamente per processi futuri.

 Note

Per generare un elenco di oggetti, è necessario disporre dell'`s3:PutInventoryConfiguration` autorizzazione. Il bucket di origine deve essere un bucket per uso generico.

- Se scegli Usa un file manifesto esistente, puoi importare un elenco di oggetti da un manifesto esistente. Un manifesto è un report o un file CV di Inventario S3 che elenca gli oggetti specifici su cui desideri che Operazioni in batch agisca.
- Se scegli Usa una configurazione di replica, puoi generare automaticamente un elenco di oggetti in base a una configurazione di replica esistente. Puoi salvare questo elenco come manifesto e utilizzarlo nuovamente per processi futuri.

Per questo esempio, scegli Genera un elenco di oggetti.

6. Per Account di origine, scegli l'account proprietario degli oggetti di origine.
7. In Origine, inserisci il percorso dell'origine, ad esempio `s3://amzn-s3-demo-bucket`.
8. In Filtri oggetto, puoi utilizzare i filtri per filtrare in base a qualsiasi parte della chiave dell'oggetto o in base alla fine della chiave dell'oggetto. I Filtri chiave oggetto aiutano a rifinire l'elenco degli oggetti da utilizzare nel manifesto. Per Filtri dei metadati degli oggetti, scegli i filtri per definire ulteriormente l'ambito degli oggetti da includere nel manifesto.
9. In Scegli operazione scegli l'operazione che desideri eseguire su tutti gli oggetti elencati nel manifesto. Se il tuo manifesto fa riferimento a oggetti archiviati in un bucket di directory, usa solo le operazioni della funzione copy o invoke AWS Lambda. Tutte le altre operazioni non sono supportate.
10. Dopo aver selezionato un tipo di operazione, scegli Successivo.
11. Compila le informazioni per Configurare le opzioni aggiuntive.

Per le autorizzazioni, specifica il ruolo AWS Identity and Access Management (IAM) che desideri che il job utilizzi. Può essere un ruolo esistente o un ruolo che Amazon S3 crea automaticamente per te. Per ulteriori informazioni, consulta [Concessione di autorizzazioni per le operazioni in batch](#). Amazon S3 può creare il ruolo per te se hai configurato il job in modo da utilizzare un

elenco di oggetti generato da S3 con filtri o un elenco di oggetti basato su una configurazione di replica.

12. Al termine della configurazione delle opzioni aggiuntive, scegli Avanti.
13. Per Review (Revisione), verificare le impostazioni. Se è necessario apportare modifiche, scegliere Previous (Precedente). Altrimenti, puoi scegliere Invia lavoro.

Utilizzo di AWS CLI

Per creare il job Batch Operations con AWS CLI, scegliete uno dei seguenti esempi, a seconda che stiate specificando un manifesto esistente o generando un manifesto automaticamente.

Specify manifest

L'esempio seguente mostra come utilizzare il per AWS CLI creare un `S3PutObjectTagging` job S3 Batch Operations che agisca sugli oggetti elencati in un file manifest esistente.

Per creare un processo **S3PutObjectTagging** di Operazioni in batch specificando un manifesto

1. Utilizza i seguenti comandi per creare un ruolo AWS Identity and Access Management (IAM), quindi crea una policy IAM per assegnare le autorizzazioni pertinenti. Il ruolo e la policy seguenti concedono l'autorizzazione Amazon S3 per aggiungere tag degli oggetti, necessari per creare il processo in una fase successiva.
 - a. Utilizza il comando di esempio seguente per creare un ruolo IAM utilizzato da Operazioni in batch. Per utilizzare questo comando di esempio, sostituisci *S3BatchJobRole* con il nome che desideri assegnare al ruolo.

```
aws iam create-role \
  --role-name S3BatchJobRole \
  --assume-role-policy-document '{
    "Version": "2012-10-17"
    ,
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "batchoperations.s3.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
```

```
}'
```

Registra il nome della risorsa Amazon (ARN) del ruolo. Quando si crea un processo sarà necessario specificare l'ARN.

- b. Utilizza il comando di esempio seguente per creare una policy IAM con le autorizzazioni necessarie e collegala al ruolo IAM creato nella fase precedente. Per ulteriori informazioni sulle autorizzazioni necessarie, consulta [Concessione di autorizzazioni per le operazioni in batch](#).

 Note

I processi Operazioni in batch che eseguono azioni su bucket di directory richiedono autorizzazioni specifiche. Per ulteriori informazioni, consulta [AWS Identity and Access Management \(IAM\) for S3 Express One Zone](#).

Per utilizzare questo comando di esempio, sostituisci *user input placeholders* come segue:

- Sostituisci *S3BatchJobRole* con il nome del ruolo IAM. Assicurati che questo nome corrisponda al nome utilizzato in precedenza.
- Sostituisci *PutObjectTaggingBatchJobPolicy* con il nome che desideri assegnare alla policy IAM.
- Sostituisci *amzn-s3-demo-destination-bucket* con il nome del bucket contenente gli oggetti a cui desideri applicare i tag.
- Sostituisci *amzn-s3-demo-manifest-bucket* con il nome del bucket contenente il manifesto.
- Sostituisci *amzn-s3-demo-completion-report-bucket* con il nome del bucket a cui desideri venga consegnato il report di completamento.

```
aws iam put-role-policy \  
  --role-name S3BatchJobRole \  
  --policy-name PutObjectTaggingBatchJobPolicy \  
  --policy-document '{  
    "Version": "2012-10-17",  
    "Statement": [  
      {
```



```

    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketLocation"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetBucketLocation"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
    ]
}
]
}'

```

2. Utilizza il comando di esempio seguente per creare un processo S3PutObjectTagging.

Il file `manifest.csv` fornisce un elenco di valori di bucket e chiave di oggetto. Il processo applica i tag specificati agli oggetti identificati nel manifesto. ETag è l'ETag dell'oggetto `manifest.csv`, che è possibile ottenere dalla console di Amazon S3. Questa richiesta specifica il parametro `no-confirmation-required`, in modo da poter eseguire il processo senza doverlo confermare con il comando `update-job-status`. Per ulteriori informazioni, consulta [create-job](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni. Sostituisci *IAM-role* con l'ARN del ruolo IAM creato in precedenza.

```
aws s3control create-job \
  --region us-west-2 \
  --account-id acct-id \
  --operation '{"S3PutObjectTagging": { "TagSet": [{"Key": "keyOne",
    "Value": "ValueOne"}] }}' \
  --manifest '{"Spec":{"Format": "S3BatchOperations_CSV_20180820", "Fields":
    [{"Bucket", "Key"}], "Location": {"ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-
bucket/manifest.csv", "ETag": "60e460c9d1046e73f7dde5043ac3ae85"}}' \
  --report '{"Bucket": "arn:aws:s3:::amzn-s3-demo-
completion-report-bucket", "Prefix": "final-reports",
    "Format": "Report_CSV_20180820", "Enabled": true, "ReportScope": "AllTasks"}' \
  --priority 42 \
  --role-arn IAM-role \
  --client-request-token $(uuidgen) \
  --description "job description" \
  --no-confirmation-required
```

In risposta, Amazon S3 restituisce un ID processo, ad esempio, *00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c*). L'ID processo è necessario per identificare, monitorare e modificare il processo.

Generate manifest

Nell'esempio seguente viene illustrato come creare un processo Operazioni in batch S3 **S3DeleteObjectTagging** che genera automaticamente un manifesto in base ai criteri di filtro degli oggetti. Questi criteri includono la data di creazione, il nome della chiave, le dimensioni, la classe di archiviazione e i tag.

Per creare un processo **S3DeleteObjectTagging** di Operazioni in batch generando un manifesto

1. Usa i seguenti comandi per creare un ruolo AWS Identity and Access Management (IAM), quindi crea una policy IAM per assegnare le autorizzazioni. Il ruolo e la policy seguenti concedono l'autorizzazione Amazon S3 per eliminare tag di oggetti, necessari quando si crea il processo in una fase successiva.

a.

Utilizza il comando di esempio seguente per creare un ruolo IAM utilizzato da Operazioni in batch. Per utilizzare questo comando di esempio, sostituisci *S3BatchJobRole* con il nome che desideri assegnare al ruolo.

```
aws iam create-role \  
  --role-name S3BatchJobRole \  
  --assume-role-policy-document '{  
    "Version": "2012-10-17",  
    "Statement": [  
      {  
        "Effect": "Allow",  
        "Principal": {  
          "Service": "batchoperations.s3.amazonaws.com"  
        },  
        "Action": "sts:AssumeRole"  
      }  
    ]  
  }'
```

Registra il nome della risorsa Amazon (ARN) del ruolo. Quando si crea un processo sarà necessario specificare l'ARN.

b. Utilizza il comando di esempio seguente per creare una policy IAM con le autorizzazioni necessarie e collegala al ruolo IAM creato nella fase precedente. Per ulteriori informazioni sulle autorizzazioni necessarie, consulta [Concessione di autorizzazioni per le operazioni in batch](#).

 Note

I processi Operazioni in batch che eseguono azioni su bucket di directory richiedono autorizzazioni specifiche. Per ulteriori informazioni, consulta [AWS Identity and Access Management \(IAM\) for S3 Express One Zone](#).

Per utilizzare questo comando di esempio, sostituisci *user input placeholders* come segue:

- Sostituisci *S3BatchJobRole* con il nome del ruolo IAM. Assicurati che questo nome corrisponda al nome utilizzato in precedenza.

- Sostituisci *DeleteObjectTaggingBatchJobPolicy* con il nome che desideri assegnare alla policy IAM.
- Sostituisci *amzn-s3-demo-destination-bucket* con il nome del bucket contenente gli oggetti a cui desideri applicare i tag.
- Sostituisci *amzn-s3-demo-manifest-bucket* con il nome del bucket in cui desideri salvare il manifesto.
- Sostituisci *amzn-s3-demo-completion-report-bucket* con il nome del bucket a cui desideri venga inviato il report di completamento.

```
aws iam put-role-policy \  
  --role-name S3BatchJobRole \  
  --policy-name DeleteObjectTaggingBatchJobPolicy \  
  --policy-document '{  
    "Version": "2012-10-17",  
    "Statement": [  
      {  
        "Effect": "Allow",  
        "Action": [  
          "s3:DeleteObjectTagging",  
          "s3:DeleteObjectVersionTagging"  
        ],  
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"  
      },  
      {  
        "Effect": "Allow",  
        "Action": [  
          "s3:PutInventoryConfiguration"  
        ],  
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"  
      },  
      {  
        "Effect": "Allow",  
        "Action": [  
          "s3:GetObject",  
          "s3:GetObjectVersion",  
          "s3:ListBucket"  
        ],  
        "Resource": [  
          "arn:aws:s3:::amzn-s3-demo-manifest-bucket",  
          "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"  
        ]  
      }  
    ]  
  }'
```

```

    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
      "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
      "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    ]
  }
]
}'

```

2. Utilizza il comando di esempio seguente per creare il processo S3DeleteObjectTagging.

In questo esempio, i valori nella sezione `--report` specificano il bucket, il prefisso, il formato e l'ambito del report del processo che verrà generato. Nella sezione `--manifest-generator` vengono specificate le informazioni sul bucket di origine contenente gli oggetti su cui agirà il processo, informazioni sull'elenco di output del manifesto che verrà generato per il processo e i criteri di filtro per restringere l'ambito degli oggetti da includere nel manifesto in base a data di creazione, vincoli di nome, dimensioni e classe di archiviazione. Il comando specifica, inoltre, la priorità del processo, il ruolo IAM e la Regione AWS.

Per ulteriori informazioni, consulta [create-job](#) nella documentazione di riferimento dei comandi della AWS CLI.

Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni. Sostituisci *IAM-role* con l'ARN del ruolo IAM creato in precedenza.

```

aws s3control create-job \
  --account-id 012345678901 \
  --operation '{
    "S3DeleteObjectTagging": {}
  }' \
  --report '{
    "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
    "Prefix": "reports",

```

```

    "Format": "Report_CSV_20180820",
    "Enabled": true,
    "ReportScope": "AllTasks"
  }' \
--manifest-generator '{
  "S3JobManifestGenerator": {
    "ExpectedBucketOwner": "012345678901",
    "SourceBucket": "arn:aws:s3::amzn-s3-demo-source-bucket",
    "EnableManifestOutput": true,
    "ManifestOutputLocation": {
      "ExpectedManifestBucketOwner": "012345678901",
      "Bucket": "arn:aws:s3::amzn-s3-demo-manifest-bucket",
      "ManifestPrefix": "prefix",
      "ManifestFormat": "S3InventoryReport_CSV_20211130"
    },
    "Filter": {
      "CreatedAfter": "2023-09-01",
      "CreatedBefore": "2023-10-01",
      "KeyNameConstraint": {
        "MatchAnyPrefix": [
          "prefix"
        ],
        "MatchAnySuffix": [
          "suffix"
        ]
      },
      "ObjectSizeGreaterThanBytes": 100,
      "ObjectSizeLessThanBytes": 200,
      "MatchAnyStorageClass": [
        "STANDARD",
        "STANDARD_IA"
      ]
    }
  }
}' \
--priority 2 \
--role-arn IAM-role \
--region us-east-1

```

In risposta, Amazon S3 restituisce un ID processo, ad esempio, 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c). Questo ID processo è necessario per identificare, monitorare e modificare il processo.

Utilizzo di AWS SDK per Java

Per creare il tuo job Batch Operations con l' AWS SDK per Java, puoi scegliere tra due approcci a seconda che tu stia specificando un manifest esistente o generando un manifest automaticamente:

- Specifica manifesto esistente: crea un processo Operazioni in batch S3 (ad esempio `S3PutObjectTagging`) che agisce sugli oggetti elencati in un file manifesto esistente. Questo approccio richiede l'inserimento della posizione del manifesto, dell'ETag e delle specifiche di formato.
- Genera manifesto automaticamente: crea un processo Operazioni in batch S3 (ad esempio `s3PutObjectCopy`) che genera automaticamente un manifesto in base ai criteri di filtro degli oggetti, inclusi data di creazione, nome della chiave e vincoli di dimensione.

Entrambi gli approcci utilizzano il client `S3Control` per configurare le operazioni del processo, le specifiche del manifesto, i report del processo, i ruoli IAM e altri parametri del processo, inclusi i requisiti di priorità e conferma.

Per esempi di come creare processi S3 Batch Operations con l' AWS SDK per Java, consulta [Creare un processo batch per copiare oggetti](#) nell'API Reference di Amazon S3.

Utilizzo della REST API

È possibile utilizzare l'API REST per creare un processo di operazioni in batch. Per ulteriori informazioni, consulta [CreateJob](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Risposte di lavoro

Se la richiesta `CreateJob` ha esito positivo, Amazon S3 restituisce un ID processo. L'ID processo è un identificatore univoco che Amazon S3 genera automaticamente per permetterti di identificare il processo di operazioni in batch e di monitorarne lo stato.

Quando crei un lavoro tramite AWS SDK o API REST, puoi impostare S3 Batch Operations in modo che inizi l'elaborazione automatica del lavoro. AWS CLI Il processo viene eseguito appena è pronto anziché attendere in coda ad altri processi con priorità più alta.

Quando crei un processo con la console Amazon S3, devi rivedere i dettagli del processo e confermare che desideri eseguirlo prima che venga elaborato da Operazioni in batch. Se un processo rimane sospeso per più di 30 giorni, avrà esito negativo.

Operazioni supportate dalle operazioni in batch S3

È possibile utilizzare Operazioni in batch S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. Le operazioni in batch S3 possono eseguire una singola operazione su elenchi di oggetti Amazon S3 specificati. Un solo processo può eseguire l'operazione specificata su miliardi di oggetti contenenti exabyte di dati. Amazon S3 tiene traccia dei progressi, invia notifiche e archivia un report dettagliato sul completamento di tutte le azioni, offrendo un'esperienza completamente gestita, verificabile e serverless. Puoi utilizzare S3 Batch Operations tramite la console Amazon S3, AWS CLI, gli AWS SDK o l'API REST di Amazon S3.

Le operazioni in batch S3 supportano le operazioni seguenti:

Copia oggetti

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. L'operazione di copia di Operazioni in batch copia ogni oggetto specificato nel manifesto. Puoi copiare oggetti in un bucket nella stessa regione AWS o in un bucket in una regione diversa. S3 Batch Operations supporta la maggior parte delle opzioni disponibili tramite Amazon S3 per la copia di oggetti. Queste opzioni includono l'impostazione dei metadati degli oggetti, l'impostazione delle autorizzazioni e la modifica di una classe di storage di un oggetto.

È inoltre possibile utilizzare l'operazione Copia per copiare gli oggetti esistenti non crittografati e riscriverli nello stesso bucket degli oggetti crittografati. Per ulteriori informazioni, consulta [Crittografia di oggetti con le operazioni in batch di Amazon S3](#).

Quando esegui la copia degli oggetti puoi modificare l'algoritmo di checksum utilizzato per calcolare il checksum dell'oggetto. Se gli oggetti non hanno un checksum aggiuntivo calcolato, puoi anche aggiungerne uno specificando l'algoritmo di checksum che Amazon S3 deve utilizzare. Per ulteriori informazioni, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Per ulteriori informazioni sulla copia di oggetti in Amazon S3 e sui parametri richiesti e opzionali, consulta [Copia, spostamento e denominazione di oggetti](#) in questa guida e [CopyObject](#) in Riferimento API di Amazon Simple Storage Service.

Restrizioni e limitazioni

Quando si utilizza l'operazione di copia di Operazioni in batch, si applicano le seguenti restrizioni e limitazioni:

- Tutti gli oggetti di origine devono trovarsi in un bucket.

- Tutti gli oggetti di destinazione devono trovarsi in un bucket.
- È necessario disporre delle autorizzazioni di lettura per il bucket di origine e delle autorizzazioni di scrittura per il bucket di destinazione.
- Gli oggetti da copiare non possono avere dimensioni superiori a 5 GB.
- Se si tenta di copiare oggetti dalle classi Recupero flessibile S3 Glacier o S3 Glacier Deep Archive alla classe di storage S3 Standard, è necessario prima ripristinare tali oggetti. Per ulteriori informazioni, consulta [Ripristino di un oggetto archiviato](#).
- È necessario creare i processi di copia di Operazioni in batch nella Regione di destinazione, ovvero la Regione in cui si intende copiare gli oggetti.
- Tutte le CopyObject opzioni sono supportate ad eccezione dei controlli condizionali sui tag di entità (ETag) e della crittografia lato server con chiavi di crittografia fornite dal cliente (). SSE-C
- Se il bucket di destinazione non è aggiornato, si sovrascriveranno gli oggetti che hanno gli stessi nomi di chiave.
- Gli oggetti non sono necessariamente copiati nello stesso ordine in cui appaiono nel manifesto. Per i bucket con controllo delle versioni, se è importante mantenere l'ordine delle versioni correnti o non correnti, copiare prima tutte le versioni non correnti. Quindi, al termine del primo processo, copia le versioni correnti in un processo successivo.
- La copia di oggetti nella classe RRS (Reduced Redundancy Storage) non è supportata.
- Un singolo processo di copia Operazioni in batch può supportare un manifesto con un massimo di 20 miliardi di oggetti.

Copia di oggetti mediante operazioni in batch S3

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. È possibile utilizzare Operazioni in batch S3 per creare un processo di copia (CopyObject) per copiare oggetti all'interno dello stesso account o in un account di destinazione diverso.

Gli esempi seguenti mostrano come memorizzare e utilizzare un manifesto che si trova in un account diverso. Il primo esempio mostra come utilizzare Inventario Amazon S3 per consegnare il report di inventario all'account di destinazione e utilizzarlo durante la creazione del processo. Il secondo esempio mostra come utilizzare un manifesto di valori separati da virgole (CSV) nell'account di origine o di destinazione. Il terzo esempio mostra come utilizzare l'operazione Copy per abilitare S3 Bucket Keys per oggetti esistenti che sono stati crittografati utilizzando la crittografia lato server con chiavi (). AWS Key Management Service AWS KMS SSE-KMS

Esempi di operazioni di copia

- [Utilizzo di un report di inventario per copiare gli oggetti Account AWS](#)
- [Utilizzo di un manifesto CSV per copiare oggetti Account AWS](#)
- [Utilizzo di Batch Operations per abilitare S3 Bucket Keys per SSE-KMS](#)

Utilizzo di un report di inventario per copiare gli oggetti Account AWS

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. È possibile utilizzare Operazioni in batch S3 per creare un processo di copia (CopyObject) per copiare oggetti all'interno dello stesso account o in un account di destinazione diverso.

È possibile utilizzare Inventario Amazon S3 per creare un report di inventario e utilizzare il report stesso per creare un elenco (manifesto) di oggetti da copiare con Operazioni in batch S3. Per maggiori informazioni sull'utilizzo di un manifest CSV nell'account di origine o di destinazione, consulta [the section called “Utilizzo di un manifesto CSV per copiare oggetti Account AWS”](#).

L'inventario Amazon S3 genera inventari degli oggetti in un bucket. L'elenco risultante viene pubblicato in un file di output. Il bucket inventariato è chiamato bucket di origine, mentre il bucket dove viene memorizzato il file del rapporto di inventario è chiamato bucket di destinazione.

Il report di inventario di Amazon S3 può essere configurato per essere consegnato a un altro Account AWS. In questo modo, Operazioni in batch S3 può leggere il report di inventario quando il processo viene creato nell'account di destinazione.

Per ulteriori informazioni sui bucket di origine e di destinazione di Inventario Amazon S3, consulta [Bucket di origine e di destinazione](#).

Il modo più semplice per configurare un inventario è utilizzare la console Amazon S3, ma puoi anche utilizzare l'API REST di Amazon S3, AWS Command Line Interface (AWS CLI) o gli SDK. AWS

La procedura della console seguente contiene le fasi di livello elevato per la configurazione delle autorizzazioni per un processo di operazioni in batch S3. In questa procedura, si copiano gli oggetti da un account di origine a un account di destinazione, con il report di inventario archiviato nell'account di destinazione.

Per configurare Amazon S3 Inventory per bucket di origine e di destinazione di proprietà di account diversi

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Scegli (o crea) un bucket del manifesto di destinazione in cui archiviare il report di inventario. In questa procedura, l'account di destinazione è l'account che possiede sia il bucket manifest di destinazione sia il bucket in cui vengono copiati gli oggetti.
4. Configura un report di inventario per un bucket di origine. Per informazioni su come utilizzare la console per configurare un inventario o su come crittografare il file dell'elenco inventario, consulta [Configurazione di Amazon S3 Inventory](#).

Quando si configura il report di inventario, si specifica il bucket di destinazione in cui si desidera memorizzare l'elenco. Il rapporto di inventario per il bucket di origine viene pubblicato nel bucket di destinazione. In questa procedura, l'account di origine è l'account che possiede il bucket di origine.

Scegliere CSV come formato di output.

Quando si inseriscono le informazioni per il bucket di destinazione, scegliere Buckets in another account (Bucket in un altro account). Quindi inserire il nome del bucket manifest di destinazione. Facoltativamente, è possibile inserire l'ID account dell'account di destinazione.

Una volta salvata la configurazione dell'inventario, la console visualizza un messaggio simile al seguente:

Amazon S3 could not create a bucket policy on the destination bucket. Ask the destination bucket owner to add the following bucket policy to allow Amazon S3 to place data in that bucket.

La console visualizza quindi una policy di bucket che può essere usata per il bucket di destinazione.

5. Copiare la policy del bucket di destinazione visualizzata sulla console.
6. Nell'account di destinazione, aggiungere la policy di bucket copiata nel bucket manifesto di destinazione in cui è memorizzato il report di inventario.
7. Creare un ruolo nell'account di destinazione basato sulla policy di attendibilità delle operazioni in batch S3. Per ulteriori informazioni su questa policy di attendibilità, consulta [Policy di trust](#).

Per ulteriori informazioni sulla creazione di un ruolo, consulta [Creazione di un ruolo per delegare le autorizzazioni a Servizio AWS](#) nella Guida all'utente IAM.

Immetti un nome per il ruolo (il seguente esempio di ruolo utilizza il nome *BatchOperationsDestinationRoleCOPY*). Scegli il servizio S3, quindi scegli il caso d'uso Operazioni in batch S3, che applica la policy di attendibilità al ruolo.

Scegli quindi Crea policy per associare la seguente policy al ruolo. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectAnnotation",
        "s3:GetObjectVersionAnnotation"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
```

Il ruolo usa la policy per concedere l'autorizzazione `batchoperations.s3.amazonaws.com` per leggere il manifest nel bucket di destinazione. Inoltre, concede autorizzazioni a GET oggetti, elenchi di controllo degli accessi (ACL), tag, annotazioni e versioni nel bucket degli oggetti di origine e concede autorizzazioni a PUT oggetti, ACL, tag e versioni nel bucket degli oggetti di destinazione.

8. Nell'account di origine, crea una policy bucket per il bucket di origine che conceda al ruolo creato nel passaggio precedente le autorizzazioni per GET oggetti, ACL, tag, annotazioni e versioni nel bucket di origine. Questa fase consente alle operazioni in batch S3 di ottenere oggetti dal bucket di origine tramite il ruolo trusted.

Segue un esempio della policy di bucket per l'account di origine. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
      "Principal": {
        "AWS":
"arn:aws:iam::<111122223333>:role/BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectAnnotation",
        "s3:GetObjectVersionAnnotation"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

9. Una volta che il report di inventario è disponibile, crea un processo di copia (CopyObject) di Operazioni in batch S3 nell'account di destinazione e scegli il report di inventario dal bucket manifesto di destinazione. È necessario l'ARN del ruolo IAM creato nell'account di destinazione.

Per informazioni generali sulla creazione di un processo, consultare [Creazione di un processo di operazioni in batch S3](#).

Per informazioni sulla creazione di un processo tramite la console, consulta [Creazione di un processo di operazioni in batch S3](#).

Utilizzo di un manifesto CSV per copiare oggetti Account AWS

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. È possibile utilizzare Operazioni in batch S3 per creare un processo di copia (CopyObject) per copiare oggetti all'interno dello stesso account o in un account di destinazione diverso.

È possibile utilizzare un manifesto CSV memorizzato nell'account di origine per copiare gli oggetti su Account AWS con Operazioni in batch S3. Per utilizzare un report di Inventario S3 come manifesto, consulta [the section called “Utilizzo di un rapporto di inventario per copiare oggetti Account AWS”](#).

Per un esempio di formato CSV per i file manifesto, consulta [the section called “Creazione di un file manifesto”](#).

La procedura seguente mostra come impostare le autorizzazioni quando si utilizza un processo di Operazioni in batch S3 per copiare oggetti da un account di origine a un account di destinazione con un file manifesto CSV memorizzato nell'account di origine.

Per utilizzare un manifesto CSV per copiare oggetti Account AWS

1. Crea un ruolo AWS Identity and Access Management (IAM) nell'account di destinazione basato sulla politica di fiducia di S3 Batch Operations. In questa procedura, l'account di destinazione è l'account in cui vengono copiati gli oggetti.

Per ulteriori informazioni sulla policy di attendibilità, consultare [Policy di trust](#).

Per ulteriori informazioni sulla creazione di un ruolo, consulta [Creazione di un ruolo per delegare le autorizzazioni a Servizio AWS](#) nella Guida all'utente IAM.

Se si crea il ruolo tramite la console, inserire un nome per il ruolo (l'esempio seguente utilizza il nome *BatchOperationsDestinationRoleCOPY*). Scegli il servizio S3, quindi scegli il caso d'uso Operazioni in batch S3, che applica la policy di attendibilità al ruolo.

Scegli quindi Crea policy per associare la seguente policy al ruolo. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectAnnotation",
        "s3:GetObjectVersionAnnotation"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
```

Usando la policy, il ruolo concede l'autorizzazione `batchoperations.s3.amazonaws.com` per leggere il manifest nel bucket manifest di origine. Concede autorizzazioni per GET oggetti, elenchi di controllo degli accessi (ACL), tag, annotazioni e versioni nel bucket degli oggetti di

origine. Inoltre, concede le autorizzazioni a PUT per oggetti, ACL, tag e versioni nel bucket degli oggetti di destinazione.

2. Nell'account di origine, crea una policy di bucket per il bucket che contiene il manifesto per concedere al ruolo creato nel passaggio precedente le autorizzazioni per gli oggetti e le versioni di GET nel bucket del manifesto di origine.

Questo passaggio consente a Operazioni in batch S3 di leggere il manifesto utilizzando il ruolo di attendibilità. Applicare la policy di bucket al bucket che contiene il manifest.

Segue un esempio della policy di bucket da applicare al bucket manifest di origine. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceManifestRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:user/ConsoleUserCreatingJob",
          "arn:aws:iam::111122223333:role/BatchOperationsDestinationRoleCOPY"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    }
  ]
}
```

Questa policy inoltre concede le autorizzazioni per garantire a un utente della console che sta creando un processo nell'account di destinazione le stesse autorizzazioni nel bucket manifest di origine tramite la stessa policy di bucket.

3. Nell'account di origine, crea una policy di bucket per il bucket di origine che conceda al ruolo creato le autorizzazioni per oggetti GET, ACL, tag e versioni nel bucket degli oggetti di origine. Le operazioni in batch S3 possono quindi ottenere oggetti dal bucket di origine tramite il ruolo trusted.

Segue un esempio della policy di bucket per il bucket che contiene gli oggetti di origine. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<111122223333>:role/BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectAnnotation",
        "s3:GetObjectVersionAnnotation"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

4. Creare un processo di operazioni in batch S3 nell'account di destinazione. È necessario l'Amazon Resource Name (ARN) del ruolo creato nell'account di destinazione. Per ulteriori informazioni sulla creazione di un processo, consulta [Creazione di un processo di operazioni in batch S3](#).

Utilizzo di Batch Operations per abilitare S3 Bucket Keys per SSE-KMS

S3 Bucket Keys riduce il costo della crittografia lato server con AWS Key Management Service (AWS KMS) (SSE-KMS) diminuendo il traffico di richieste da Amazon S3 a AWS KMS. Per ulteriori

informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#) e [Configurazione del bucket per l'utilizzo di una chiave S3 Bucket per i nuovi oggetti SSE-KMS](#). Quando esegui un'CopyObjectoperazione utilizzando l'API REST, gli AWS SDK o AWS CLI, puoi abilitare o disabilitare una chiave S3 Bucket a livello di oggetto aggiungendo l'intestazione della richiesta con un valore `or. x-amz-server-side-encryption-bucket-key-enabled true false`

Quando si configura una chiave S3 Bucket per un oggetto utilizzando un'operazione CopyObject, Amazon S3 aggiorna solo le impostazioni per quell'oggetto. Le impostazioni della chiave del bucket S3 per il bucket di destinazione non vengono modificate. Se si invia una richiesta CopyObject per un oggetto crittografato AWS KMS a un bucket con S3 Bucket Keys abilitate, l'operazione a livello di oggetto utilizzerà automaticamente S3 Bucket Keys, a meno che non si disabilitino le chiavi nell'intestazione della richiesta. Se non specifichi una chiave bucket S3 per il tuo oggetto, Amazon S3 applica le impostazioni della chiave bucket S3 per il bucket di destinazione all'oggetto.

Per crittografare gli oggetti Amazon S3 esistenti, è possibile utilizzare Operazioni in batch S3. È possibile utilizzare l'operazione di copia delle operazioni in batch per copiare gli oggetti non crittografati esistenti e scrivere i nuovi oggetti crittografati nello stesso bucket. Per ulteriori informazioni, [consulta la sezione Crittografia degli oggetti con Amazon S3 Batch Operations nel blog di storage](#). AWS

Nell'esempio seguente, si utilizza l'operazione di copia Operazioni in batch per abilitare le chiavi bucket S3 per gli oggetti esistenti. Per ulteriori informazioni, consulta [the section called "Configurazione di una chiave bucket S3 per un oggetto"](#).

Argomenti

- [Considerazioni sull'utilizzo di Operazioni in batch S3 per crittografare gli oggetti con chiavi bucket S3 abilitate](#)
- [Prerequisiti](#)
- [Fase 1: Ottenimento dell'elenco di oggetti tramite Amazon S3 Inventory](#)
- [Fase 2: Filtro dell'elenco degli oggetti con S3 Select](#)
- [Fase 3: Impostazione ed esecuzione del processo di operazioni in batch S3](#)

Considerazioni sull'utilizzo di Operazioni in batch S3 per crittografare gli oggetti con chiavi bucket S3 abilitate

Quando si usa Operazioni in batch S3 per crittografare gli oggetti con chiavi bucket S3 abilitate, si devono considerare i seguenti problemi:

- Verranno addebitati i costi di processi, oggetti e richieste associati alla funzione Operazioni in batch Amazon S3, oltre ai costi associati all'operazione eseguita dalla funzione Operazioni in batch Amazon S3 per tuo conto, inclusi trasferimenti dati, richieste e altri addebiti. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).
- Se utilizzi un bucket con versioni, ogni processo di operazioni in batch S3 eseguito crea nuove versioni crittografate degli oggetti. Conserva anche le versioni precedenti configurate senza chiave di bucket S3. Per eliminare le versioni precedenti, imposta una policy di scadenza del ciclo di vita S3 per le versioni non correnti, come descritto in [Elementi della configurazione del ciclo di vita](#).
- L'operazione di copia crea nuovi oggetti con nuove date di creazione, che possono influire sulle operazioni del ciclo di vita, come ad esempio l'archiviazione. Se copi tutti gli oggetti nel bucket, tutte le nuove copie avranno date di creazione identiche o simili. Per identificare ulteriormente questi oggetti e creare regole del ciclo di vita diverse per vari sottoinsiemi di dati, è consigliabile utilizzare i tag oggetto.

Prerequisiti

Prima di configurare gli oggetti per l'utilizzo di una chiave S3 Bucket, consulta [Modifiche alla nota prima dell'abilitazione di una chiave bucket S3](#).

Per utilizzare questo esempio, è necessario disporre di almeno un bucket S3 per contenere i file di lavoro Account AWS e i risultati crittografati. È inoltre possibile trovare utile buona parte della documentazione esistente delle operazioni in batch S3, inclusi i seguenti argomenti:

- [Nozioni di base sulle operazioni in batch S3](#)
- [Creazione di un processo di operazioni in batch S3](#)
- [Operazioni supportate dalle operazioni in batch S3](#)
- [Gestione dei processi di operazioni in batch Amazon S3](#)

Fase 1: Ottenimento dell'elenco di oggetti tramite Amazon S3 Inventory

Per iniziare, identifica il bucket S3 che contiene gli oggetti da crittografare e recupera un elenco del suo contenuto. Un report di inventario di Amazon S3 è il modo più conveniente per farlo. Il report fornisce l'elenco degli oggetti di un bucket con i relativi metadati. In questo passaggio, il bucket di origine è il bucket inventariato e il bucket di destinazione è il bucket in cui si memorizza il file del report di inventario. Per ulteriori informazioni sui bucket di origine e di destinazione di Inventario Amazon S3, consulta [Catalogazione e analisi dei dati con Inventario S3](#).

Il modo più semplice per configurare un inventario consiste nell'utilizzare la Console di gestione AWS. Ma puoi anche usare l'API REST, AWS Command Line Interface (AWS CLI) o AWS gli SDK. Prima di seguire questi passaggi, assicurati di accedere alla console e di aprire la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/> Se si verificano errori di autorizzazione negata, aggiungi una policy bucket al bucket di destinazione. Per ulteriori informazioni, consulta [Concedere autorizzazioni per S3 Inventory e S3 Analytics](#).

Come ottenere un elenco di oggetti tramite Inventario S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket e seleziona un bucket contenente gli oggetti da crittografare.
3. Nella scheda Gestione, passa alla sezione Configurazioni di inventario e seleziona Crea configurazione di inventario.
4. Assegna un nome al tuo nuovo inventario, inserisci il nome del bucket S3 di destinazione e, facoltativamente, crea un prefisso di destinazione per Amazon S3 per assegnare gli oggetti in quel bucket.
5. Per Formato di output, seleziona CSV.
6. (Facoltativo) Nella sezione Campi aggiuntivi - facoltativi, seleziona Crittografia e tutti gli altri campi del report che ti interessano. Imposta la frequenza per le consegne del report su Giornaliero in modo che il primo report venga consegnato al bucket quanto prima.
7. Seleziona Crea per salvare la configurazione.

Amazon S3 può richiedere fino a 48 ore per consegnare il primo report, quindi controlla quando arriva. Dopo aver ricevuto il primo report, procedi alla fase successiva per filtrare i contenuti del report di Inventario S3. Se non desideri più ricevere report di inventario per questo bucket, elimina la configurazione dell'inventario S3. Altrimenti, Amazon S3 continua a consegnare i report su base giornaliera o settimanale.

Un elenco di inventari non è una singola visualizzazione point-in-time di tutti gli oggetti. Gli elenchi di inventario sono uno snapshot in sequenza di voci del bucket, che sono a consistenza finale (cioè, l'elenco potrebbe non includere oggetti aggiunti o eliminati di recente). La combinazione di inventario S3 e operazioni in batch S3 funziona meglio quando si lavora con oggetti statici o con un set di oggetti creato due o più giorni prima. Per lavorare con dati più recenti, utilizza l'operazione API [ListObjectsV2](#) (GET bucket) per costruire manualmente l'elenco di oggetti. Se necessario, ripeti la

procedura per i giorni successivi o finché il report di inventario non mostra lo stato desiderato per tutti gli oggetti.

Fase 2: Filtro dell'elenco degli oggetti con S3 Select

Dopo aver ricevuto il report di Inventario S3, è possibile filtrare il contenuto del report per elencare solo gli oggetti che non sono crittografati con chiavi bucket S3 abilitate. Se si desidera che tutti gli oggetti del bucket siano crittografati con S3 Bucket Keys abilitate, si può ignorare questo passaggio. Tuttavia, filtrando il report di Inventario S3 in questa fase si risparmia il tempo e la spesa di una nuova crittografia degli oggetti precedentemente crittografati con chiavi del bucket S3 abilitate.

Sebbene i passaggi seguenti mostrino come filtrare utilizzando [Amazon S3 Select](#), è possibile utilizzare anche [Amazon Athena](#). Per decidere quale strumento utilizzare, dai un'occhiata al file `manifest.json` del report di inventario S3. Questo file riporta il numero di file di dati associati a tale report. Se il numero è grande, usa Amazon Athena perché viene eseguito su più oggetti S3, mentre S3 Select funziona su un oggetto alla volta. Per ulteriori informazioni sull'utilizzo congiunto di Amazon S3 e Athena, consulta [Esecuzione di query sull'inventario Amazon S3 con Amazon Athena](#) «Utilizzo di Athena» nel post del blog di AWS storage [Encrypting objects with Amazon S3 Batch Operations](#).

Per filtrare il report di Inventario S3 utilizzando S3 Select

1. Apri il file `manifest.json` dal report di inventario e guarda la sezione `fileSchema` del JSON. Questa sezione informa la query che si esegue sui dati.

Il seguente JSON è un `manifest.json` file di esempio per un CSV-formatted inventario su un bucket con il controllo delle versioni abilitato. A seconda di come hai configurato il report di inventario, il manifest potrebbe apparire diverso.

```
{
  "sourceBucket": "batchoperationsdemo",
  "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
  "version": "2021-05-22",
  "creationTimestamp": "1558656000000",
  "fileFormat": "CSV",
  "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
BucketKeyStatus",
  "files": [
    {
      "key": "demoinv/batchoperationsdemo/DemoInventory/data/009a40e4-
f053-4c16-8c75-6100f8892202.csv.gz",
      "size": 72691,
```

```

    "MD5checksum": "c24c831717a099f0ebe4a9d1c5d3935c"
  }
]
}

```

Se il controllo delle versioni non è attivato nel bucket o se hai deciso di eseguire il report per le versioni più recenti, la `fileSchema` è `Bucket`, `Key` e `BucketKeyStatus`.

Se il controllo delle versioni è attivato, a seconda di come è stato impostato il report di inventario, il `fileSchema` può includere quanto segue: `Bucket`, `Key`, `VersionId`, `IsLatest`, `IsDeleteMarker`, `BucketKeyStatus`. Quindi presta attenzione alle colonne 1, 2, 3 e 6 quando esegui la query.

Per eseguire il processo, la funzionalità Operazioni in batch Amazon S3 richiede come input il bucket, la chiave e l'ID versione, oltre al campo in base al quale eseguire la ricerca, ovvero `BucketKeyStatus`. Il campo `VersionID` non è necessario, ma è utile specificare il campo `VersionID` quando si opera su un bucket con controllo delle versioni. Per ulteriori informazioni, consulta [Utilizzo di oggetti in un bucket che supporta la funzione Controllo delle versioni](#).

1. Individua i file di dati per il report di inventario. L'oggetto `manifest.json` riporta i file di dati in `files`.
2. Dopo aver individuato e selezionato il file di dati nella console S3, seleziona Operazioni quindi scegli Query con S3 Select.
3. Mantieni i valori preimpostati per CSV, virgola e GZIP e seleziona Successivo.
4. Per rivedere il formato del report dell'inventario prima di procedere, scegli Mostra anteprima file.
5. Immetti le colonne a cui fare riferimento nel campo SQL expression (Espressione SQL), quindi seleziona Run SQL (Esegui SQL). L'espressione seguente restituisce le colonne 1-3 per tutti gli oggetti senza chiave bucket S3 configurata.

```
select s._1, s._2, s._3 from s3object s where s._6 = 'DISABLED'
```

Di seguito sono riportati i risultati di esempio.

```

batchoperationsdemo,0100059%7Ethumb.jpg,lSrtIxksLu0R0ZkYPL.LhgD5caTYn6vu
batchoperationsdemo,0100074%7Ethumb.jpg,sd2M60g6Fdazoi6D5kNARIE7KzUibmHR
batchoperationsdemo,0100075%7Ethumb.jpg,TLYESLn1mXD5c4Bwi0IinqFrktddkoL
batchoperationsdemo,0200147%7Ethumb.jpg,amufzfMi_fEw0Rs99rxR_HrDF1E.13Y0
batchoperationsdemo,0301420%7Ethumb.jpg,9qGU2SEscL.C.c_sK89trmXYIwooABSh
batchoperationsdemo,0401524%7Ethumb.jpg,0RnEWNuB1QhHrrYAGFsZhbyvEYJ3DUor

```

```
batchoperationsdemo,200907200065HQ
%7Ethumb.jpg,d8LgvIVjbDR5mUVwW6pu9ahTfReyn5V4
batchoperationsdemo,200907200076HQ
%7Ethumb.jpg,XUT25d7.gK40u_GmnupdaZg3BVx2jN40
batchoperationsdemo,201103190002HQ
%7Ethumb.jpg,z.2sVRh0myqVi0BuIrngWlsRPQdb7q0S
```

7. Scarica i risultati, salvali in un formato CSV e caricali in Amazon S3 come elenco di oggetti per il processo di operazioni in batch S3.
8. Se disponi di più file manifest, esegui Query con S3 Select anche su quelli. A seconda delle dimensioni dei risultati, è possibile combinare gli elenchi ed eseguire un singolo processo di operazioni in batch S3 oppure eseguire ogni elenco come processo separato. Per decidere il numero di processi da eseguire, considera il [prezzo](#) dell'esecuzione di ciascun processo di Operazioni in batch S3.

Fase 3: Impostazione ed esecuzione del processo di operazioni in batch S3

Ora che si dispone di elenchi CSV filtrati di oggetti S3, è possibile avviare il processo di Operazioni in batch S3 per crittografare gli oggetti con chiavi bucket S3 abilitate.

Un processo fa riferimento collettivamente all'elenco (manifest) degli oggetti forniti, all'operazione eseguita e ai parametri specificati. Il modo più semplice per crittografare questo insieme di oggetti con le chiavi bucket S3 abilitate è utilizzare l'operazione Copia e specificare lo stesso prefisso di destinazione degli oggetti elencati nel manifesto. In un bucket non convertito, questa operazione sovrascrive gli oggetti esistenti. In un bucket con il controllo delle versioni attivato, questa operazione crea una versione più recente e crittografata degli oggetti.

Come parte della copia degli oggetti, specifica che Amazon S3 deve crittografare gli oggetti con crittografia. SSE-KMS Questo processo copia gli oggetti, quindi tutti gli oggetti mostreranno una data di creazione aggiornata al momento del completamento, indipendentemente da quando sono stati aggiunti originariamente ad Amazon S3. Specifica inoltre le altre proprietà per l'insieme di oggetti come parte del processo di operazioni in batch S3, inclusi i tag oggetto e la classe di archiviazione.

Fasi secondarie

- [Impostazione della policy IAM](#)
- [Impostazione del ruolo IAM nelle operazioni in batch](#)
- [Attivazione di S3 Bucket Keys per un bucket esistente](#)
- [Creazione di un processo di operazioni in batch S3](#)

- [Esecuzione del processo di operazioni in batch](#)

Impostazione della policy IAM

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione a sinistra, scegli Policy, quindi scegli Crea policy.
3. Selezionare la scheda JSON. Seleziona Modifica policy e aggiungi la policy IAM di esempio visualizzata nel seguente blocco di codice.

Dopo aver copiato l'esempio di policy nella [Console IAM](#), sostituisci quanto segue:

- a. Sostituisci *amzn-s3-demo-source-bucket* con il nome del bucket di origine da cui copiare gli oggetti.
- b. Sostituisci *amzn-s3-demo-destination-bucket* con il nome del bucket di destinazione in cui copiare gli oggetti.
- c. Sostituisci *amzn-s3-demo-manifest-bucket/manifest-key* con il nome del tuo oggetto manifesto.
- d. Sostituisci *amzn-s3-demo-completion-report-bucket* con il nome del bucket in cui si desidera salvare i report di completamento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyObjectsToEncrypt",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectVersionAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",

```



```

        "s3:GetObjectAnnotation",
        "s3:GetObjectVersionAnnotation"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    ]
},
{
    "Sid": "ReadManifest",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest-key"
},
{
    "Sid": "WriteReport",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
}
]
}

```

4. Scegliere Next: Tags (Successivo: Tag).
5. Aggiungi tutti i tag desiderati (facoltativo) e seleziona Successivo: Rivedi.
6. Aggiungi un nome per la policy, facoltativamente, una descrizione quindi scegli Crea policy.
7. Scegli Esamina policy e quindi Salva modifiche.
8. Una volta completata la policy per le operazioni in batch S3, la console ritorna alla pagina Policy di IAM. Filtra in base al nome della policy, scegli il pulsante a sinistra del nome della policy, seleziona Operazioni di policy e scegli Collega.

Per associare la nuova policy creata a un ruolo IAM, seleziona gli utenti, i gruppi o i ruoli appropriati nell'account e scegli Collega policy. In questo modo si ritorna alla console IAM.

Impostazione del ruolo IAM nelle operazioni in batch

1. Nella [Console IAM](#), nel riquadro di navigazione, scegli Ruoli, quindi scegli Crea ruolo.
2. Seleziona Servizio AWS, S3 e Operazioni in batch S3. Quindi scegliere Next: Permissions (Successivo: Autorizzazioni).
3. Inizia a inserire il nome della policy IAM che hai appena creato. Seleziona la casella di controllo in base al nome della policy quando viene visualizzata e scegli Successivo: Tag.
4. (Facoltativo) Aggiungi tag o mantieni vuoti i campi di chiave e valore per questo esercizio. Scegliere Next:Review (Successivo:Rivedi).
5. Specifica un nome per il ruolo e accetta la descrizione predefinita o aggiungine una personalizzata. Seleziona Create role (Crea ruolo).
6. Assicurati che l'utente che crea il processo disponga delle autorizzazioni riportate nell'esempio seguente.

Sostituisci *account-id* con il tuo ID Account AWS e *IAM-role-name* con il nome che prevedi di applicare al ruolo IAM che verrà creato nel passaggio della creazione del processo Operazioni in batch più avanti. Per ulteriori informazioni, consulta [Concessione di autorizzazioni per le operazioni in batch](#).

```
{
  "Sid": "AddIamPermissions",
  "Effect": "Allow",
  "Action": [
    "iam:GetRole",
    "iam:PassRole"
  ],
  "Resource": "arn:aws:iam::account-id:role/IAM-role-name"
}
```

Attivazione di S3 Bucket Keys per un bucket esistente

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket scegli il bucket per cui desideri abilitare una chiave bucket S3.
3. Scegliere Properties (Proprietà).
4. In Default encryption (Crittografia di default), scegliere Edit (Modifica).

5. In Tipo di crittografia, puoi scegliere tra chiavi gestite da Amazon S3 (SSE-S3) e AWS Key Management Service chiave (SSE-KMS).
6. Se hai scelto AWS Key Management Service key (SSE-KMS), in AWS KMS key, puoi specificare la AWS KMS chiave tramite una delle seguenti opzioni.
 - Per effettuare una selezione in un elenco di chiavi KMS disponibili, seleziona Scegli tra le chiavi AWS KMS . Nell'elenco di chiavi disponibili, scegli una chiave KMS di crittografia simmetrica nella stessa regione del bucket. Nell'elenco vengono visualizzate sia la chiave AWS gestita (aws/s3) che la chiave gestita dal cliente.
 - Per inserire l'ARN della chiave KMS, scegli Inserisci la AWS KMS chiave ARN, quindi inserisci la chiave ARN del tuo KMS nel campo visualizzato.
 - Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.
7. In Chiave bucket, seleziona Abilita quindi scegli Salva modifiche.

Ora che la chiave del bucket S3 è abilitata a livello di bucket, gli oggetti caricati, modificati o copiati in questo bucket ereditano questa configurazione di crittografia per impostazione predefinita. Sono inclusi anche gli oggetti copiati tramite la funzionalità Operazioni in batch Amazon S3.

Creazione di un processo di operazioni in batch S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione seleziona Operazioni in batch, quindi scegli Crea processo.
3. Seleziona la regione in cui si trovano i tuoi oggetti e scegli CSV come tipo manifest.
4. Specifica il percorso o passare al file manifest CSV creato in precedenza dai risultati di S3 Select (o Athena). Se il manifest contiene ID versione, seleziona tale casella. Scegli Avanti.
5. Seleziona Copia e scegli il bucket di destinazione della copia. Puoi mantenere la crittografia lato server disattivata. Finché nella destinazione del bucket sono abilitate le chiavi bucket S3, l'operazione di copia applica le chiavi bucket S3 al bucket di destinazione.
6. (Facoltativo) Scegli una classe di archiviazione e gli altri parametri come desiderato. I parametri specificati in questo passaggio si applicano a tutte le operazioni eseguite sugli oggetti riportati nel manifest. Scegli Avanti.
7. Per configurare la crittografia lato server, completa la seguente procedura:
 - a. Nella sezione Server-side Crittografia, scegli una delle seguenti opzioni:

- Per conservare le impostazioni relative ai bucket per la crittografia predefinita degli oggetti lato server durante l'archiviazione in Amazon S3, scegli Non specificare una chiave di crittografia. Finché nella destinazione del bucket sono abilitate le chiavi bucket S3, l'operazione di copia applica la chiave bucket S3 al bucket di destinazione.

 Note

Se la policy di bucket per la destinazione specificata richiede la crittografia degli oggetti prima di archivarli in Amazon S3, è necessario specificare una chiave di crittografia. In caso contrario, la copia degli oggetti nella destinazione avrà esito negativo.

- Per crittografare gli oggetti prima di archivarli in Amazon S3, scegli Specifica una chiave di crittografia.
- b. In Impostazioni di crittografia, se scegli Specifica una chiave di crittografia, devi scegliere Usa le impostazioni del bucket di destinazione per la crittografia predefinita o Ignora le impostazioni del bucket di destinazione per la crittografia predefinita.
 - c. Se scegli Ignora le impostazioni del bucket di destinazione per la crittografia predefinita, dovrai configurare le seguenti impostazioni di crittografia.
 - i. In Tipo di crittografia, devi scegliere le chiavi gestite da Amazon S3 (SSE-S3) o AWS Key Management Service la chiave (SSE-KMS). SSE-S3 utilizza uno dei più potenti cifrari a blocchi: Advanced Encryption Standard () a 256 bit per crittografare ogni oggetto. AES-256 SSE-KMS ti offre un maggiore controllo sulla tua chiave. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#) e [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#).
 - ii. Se scegli AWS Key Management Service key (SSE-KMS), in AWS KMS key, puoi specificarlo AWS KMS key tramite una delle seguenti opzioni.
 - Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS keys, quindi scegli una chiave KMS di crittografia simmetrica nella stessa regione del bucket. Nell'elenco vengono visualizzate sia la chiave AWS gestita (aws/s3) che la chiave gestita dal cliente.
 - Per inserire l'ARN della chiave KMS, scegli Inserisci la AWS KMS chiave ARN e inserisci la tua chiave KMS ARN nel campo visualizzato.

- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.
- iii. In Chiave bucket scegli Abilita. L'operazione di copia applica una chiave bucket S3 al bucket di destinazione.
8. Assegna al processo una descrizione (o mantieni quella predefinita), impostane il livello di priorità, scegli un tipo di report e specifica il Percorso di destinazione del report di completamento.
 9. Nella sezione Autorizzazioni, assicurati di scegliere il ruolo IAM delle operazioni in batch definito in precedenza. Scegli Avanti.
 10. In Rivedi, verificare le impostazioni. Se è necessario apportare modifiche, seleziona Precedente. Dopo aver confermato le impostazioni delle operazioni in batch, seleziona Crea processo.

Per ulteriori informazioni, consulta [Creazione di un processo di operazioni in batch S3](#).

Esecuzione del processo di operazioni in batch

La procedura guidata di configurazione ti riporta automaticamente alla sezione Operazioni in batch S3 della console di Amazon S3. Le transizioni del tuo nuovo processo dallo stato Nuovo allo stato Preparazione in corso indicano come inizia il processo S3. Durante lo stato Preparazione in corso, S3 legge il manifest del processo, controlla la presenza di errori e calcola il numero di oggetti.

1. Scegli il pulsante Aggiorna nella console di Amazon S3 per verificare lo stato di avanzamento. A seconda delle dimensioni del manifest, la lettura può richiedere minuti o ore.
2. Dopo che S3 ha terminato la lettura del manifest del processo, il processo passa allo stato In attesa di conferma. Scegli il pulsante di opzione a sinistra dell'ID processo, quindi seleziona Esegui processo.
3. Controlla le impostazioni del processo e scegli Esegui processo.

Dopo l'inizio dell'esecuzione del processo, puoi scegliere il pulsante di aggiornamento per verificarne l'avanzamento tramite la vista del pannello di controllo della console o selezionando il processo specifico.

4. Una volta completato il processo, puoi visualizzare il numero di oggetti con stato Riuscito e Non riuscito per confermare che tutto è stato eseguito come previsto. Se hai abilitato i report del processo, controlla la causa esatta di eventuali operazioni non riuscite nel report.

Puoi anche eseguire questi passaggi utilizzando gli AWS SDK o AWS CLI l'API REST di Amazon S3. Per ulteriori informazioni sul monitoraggio dello stato del processo e dei report sul completamento, consulta [Monitoraggio dei rapporti sullo stato e sul completamento dei processi](#).

Per esempi che mostrano l'operazione di copia con i tag utilizzando il comando AWS CLI and AWS SDK per Java, consulta. [Creazione di un processo Batch Operations con tag di processo utilizzati per l'etichettatura](#)

Calcolo dei checksum

È possibile utilizzare Operazioni in batch S3 con l'operazione Calcola il checksum per eseguire calcoli del checksum di oggetti archiviati in Amazon S3 a riposo. L'operazione Calcola il checksum calcola i checksum degli oggetti che puoi utilizzare per convalidare l'integrità dei dati senza scaricare o ripristinare oggetti per i dati archiviati. È possibile utilizzare l'operazione Calcola il checksum per calcolare i checksum di tipi di checksum compositi e di oggetti completi, per tutti gli algoritmi di checksum supportati.

Con l'operazione Calcola il checksum, è possibile elaborare miliardi di oggetti tramite una singola richiesta di processo. Questa operazione in batch è compatibile con tutte le classi di archiviazione S3, indipendentemente dalla dimensione dell'oggetto. Per creare un processo di checksum di calcolo, utilizza la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Quando si [abilita la registrazione dei log degli accessi al server](#), è anche possibile ricevere voci di log relative al processo Calcola il checksum. L'operazione Calcola il checksum emette eventi del log di accesso al server separati dopo aver completato i calcoli del checksum. Queste voci di log seguono il [formato standard di registrazione dei log degli accessi al server S3](#) e includono campi come il tipo di operazione, il timestamp, i [codici di errore](#) e l'ID del processo Calcola il checksum associato. Questa registrazione dei log fornisce un audit trail delle attività di verifica del checksum eseguite sugli oggetti, consentendo di monitorare e verificare le operazioni di integrità dei dati.

Note

L'operazione Compute checksum non supporta la crittografia lato server con oggetti crittografati con chiavi di crittografia fornite dal cliente (). SSE-C Tuttavia, è possibile utilizzare l'operazione Compute checksum con oggetti crittografati utilizzando la crittografia lato server con chiavi gestite S3 (), la [crittografia lato server con \(\). SSE-S3](#) AWS Key Management

Service DSSE-KMS Assicuratevi di aver [concesso le AWS KMS autorizzazioni](#) appropriate per eseguire l'operazione Compute checksum.

Per iniziare a utilizzare l'operazione Calcola il checksum utilizzando Operazioni in batch puoi procedere in questi modi:

- Crea un nuovo file manifesto manualmente.
- Utilizza un manifesto esistente.
- Configura Operazioni in batch per generare automaticamente un manifesto in base ai criteri di filtro degli oggetti [specificati quando si crea il processo](#).

Quindi, invia la richiesta di processo Calcola il checksum e monitorane lo stato. Al termine del processo Calcola il checksum, ricevi automaticamente un report di completamento nel bucket di destinazione specificato. Questo report di completamento contiene informazioni sul checksum di ogni oggetto presente nel bucket, consentendoti di verificare la coerenza dei dati. Per ulteriori informazioni su come utilizzare questo report per esaminare il processo, consulta [Monitoraggio dei rapporti sullo stato e sul completamento dei processi](#).

Per ulteriori informazioni sulle funzionalità di Calcola il checksum e su come utilizzare Calcola il checksum nella console, consulta [Verifica dell'integrità degli oggetti per i dati a riposo in Amazon S3](#). Per informazioni su come inviare richieste REST all'operazione Calcola il checksum, consulta [DescribeJob](#) e [CreateJob](#) nella Guida di riferimento delle API di Amazon S3.

Le sezioni seguenti spiegano come iniziare a utilizzare l'operazione Calcola il checksum con Operazioni in batch S3.

Argomenti

- [Operazioni in batch S3 Calcola il checksum considerazioni](#)
- [Report di completamento di Operazioni in batch S3](#)

Operazioni in batch S3 Calcola il checksum considerazioni

Prima di utilizzare l'operazione Calcola il checksum, esamina il seguente elenco di considerazioni:

- Se il manifesto include un campo ID versione, è necessario fornire un ID versione per tutti gli oggetti del manifesto. Se l'ID versione non è specificato, la richiesta Calcola il checksum esegue l'operazione sulla versione più recente dell'oggetto.
- Per ricevere i dettagli dell'operazione Calcola il checksum nei [log di accesso al server](#), è necessario innanzitutto [abilitare la registrazione dei log di accesso al server](#) nel bucket di origine e specificare un bucket di destinazione per archiviare i log. Il bucket di destinazione deve esistere anche nello stesso bucket Regione AWS e nel bucket di Account AWS origine. Dopo aver configurato la registrazione dei log degli accessi al server, l'operazione Calcola il checksum genera i [record di log](#) che includono campi standard come il tipo di operazione, il codice di stato HTTP, i [codici di errore S3](#), i timestamp e l'ID del processo Calcola il checksum associato. L'operazione Calcola il checksum viene eseguita in modo asincrono. Di conseguenza, le [voci di log](#) utilizzano un ID del processo Calcola il checksum, anziché l'ID della richiesta.
- La generazione del report può richiedere fino a qualche ora per gli oggetti archiviati.
- Per le seguenti classi di archiviazione S3 Glacier, il completamento del processo Calcola il checksum può richiedere fino a una settimana:
 - S3 Glacier Flexible Retrieval
 - S3 Glacier Deep Archive
- Per i bucket in cui verrà scritto il report di completamento, è necessario utilizzare la [condizione di proprietario del bucket](#) quando si esegue l'operazione Calcola il checksum. Se il proprietario del bucket effettivo non corrisponde al proprietario del bucket previsto per la richiesta di processo inviata, il processo ha esito negativo. Per l'elenco delle operazioni S3 che non supportano la condizione di proprietario del bucket, consulta [Restrizioni e limitazioni](#).

Report di completamento di Operazioni in batch S3

Quando crei un processo Calcola il checksum, puoi richiedere il report di completamento di Operazioni in batch S3. Questo file CSV mostra gli oggetti, i codici di esito positivo o negativo, gli output e le descrizioni. Per ulteriori informazioni sul monitoraggio dei processi e sui report di completamento, consulta [Report di completamento](#).

Elimina tutti i tag oggetto

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. L'operazione Elimina tutti i tag oggetto rimuove tutti i set di tag oggetto Amazon S3 correntemente associati agli oggetti riportati nel manifesto. Operazioni in batch S3 non supporta l'eliminazione dei tag dagli oggetti mantenendo anche altri tag.

Se gli oggetti nel manifest si trovano in un bucket con versione, puoi rimuovere i set di tag da una versione specifica di un oggetto. A tal fine, è necessario specificare un ID di versione per ogni oggetto del manifesto. Se non includi un ID versione per un oggetto, S3 Batch Operations rimuoverà il set di tag dall'ultima versione di ogni oggetto. Per ulteriori informazioni sui manifest di Batch Operations, consulta [Specifica di un manifest](#).

Per ulteriori dettagli sull'etichettatura degli oggetti, consulta [Etichettare i tuoi oggetti](#) in questa guida e [PutObjectTagging](#), [GetObjectTagging](#), e [DeleteObjectTagging](#) in Riferimento API di Amazon Simple Storage Service.

 Warning

L'esecuzione di questo processo rimuove tutti i set di tag oggetto in ogni oggetto elencato nel manifest.

Per utilizzare la console per creare un processo di eliminazione di tutti i tag degli oggetti, consulta [Creazione di un processo di operazioni in batch S3](#).

Restrizioni e limitazioni

Quando si utilizza Operazioni in batch per eliminare i tag da un oggetto, si applicano le seguenti restrizioni e limitazioni:

- Il ruolo AWS Identity and Access Management (IAM) specificato per eseguire il job deve disporre delle autorizzazioni per eseguire l'operazione Amazon S3 sottostante. `DeleteObjectTagging` Per ulteriori informazioni, consulta [DeleteObjectTagging](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).
- Operazioni in batch S3 utilizza l'operazione [DeleteObjectTagging](#) di Amazon S3 per rimuovere i set di tag da ogni oggetto del manifesto. Tutte le restrizioni e le limitazioni che si applicano all'operazione sottostante si applicano anche ai processi Operazioni in batch S3.
- Un singolo processo di eliminazione dei tag dagli oggetti può supportare un manifesto con un massimo di 20 miliardi di oggetti.

Invoke AWS Lambda funzione

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. L'operazione `Invoke AWS Lambda function Batch Operations` avvia AWS

Lambda funzioni per eseguire azioni personalizzate sugli oggetti elencati in un manifesto. Questa sezione descrive come creare una funzione Lambda da utilizzare con le operazioni in batch Amazon S3 e come creare un processo per richiamare la funzione. Il processo di S3 Batch Operations utilizza l'operazione LambdaInvoke per eseguire una funzione Lambda su ogni oggetto elencato in un manifesto.

Puoi lavorare con S3 Batch Operations utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3. Per ulteriori informazioni sull'utilizzo di Lambda, consulta [Nozioni di base su AWS Lambda](#) nella Guida per Developer di AWS Lambda .

Le sezioni seguenti spiegano come iniziare a utilizzare le operazioni in batch S3 con Lambda.

Argomenti

- [Utilizzo di Lambda con Operazioni in batch](#)
- [Creazione di una funzione Lambda da utilizzare con le operazioni in batch S3](#)
- [Creazione di un processo di operazioni in batch Amazon S3 che richiama una funzione Lambda](#)
- [Fornitura di informazioni a livello di task nei manifesti Lambda](#)
- [Tutorial su Operazioni in batch S3](#)

Utilizzo di Lambda con Operazioni in batch

Quando si utilizza S3 Batch Operations con AWS Lambda, è necessario creare nuove funzioni Lambda appositamente per l'utilizzo con S3 Batch Operations. Non puoi riutilizzare funzioni basate su eventi Amazon S3 esistenti con le operazioni in batch S3. Le funzioni evento possono solo ricevere messaggi, non possono restituirli. Le funzioni Lambda utilizzate con le operazioni in batch S3 devono accettare e restituire messaggi. Per ulteriori informazioni sull'utilizzo di Lambda con gli eventi Amazon S3, consulta [Using AWS Lambda with Amazon S3](#) nella Developer Guide. AWS Lambda

Devi creare un processo di operazioni in batch Amazon S3 che richiama la funzione Lambda. Il processo esegue la stessa funzione Lambda su tutti gli oggetti elencati nel manifesto. Puoi controllare quali versioni della funzione Lambda utilizzare durante l'elaborazione degli oggetti nel manifesto. Le operazioni in batch S3 supportano Amazon Resource Name (ARN) non qualificati, alias e versioni specifiche. Per ulteriori informazioni, consulta [Introduzione al controllo delle AWS Lambda versioni](#) nella Developer Guide. AWS Lambda

Se fornisci il processo di operazioni in batch Amazon S3 con una funzione ARN che utilizza un alias o il qualificatore \$LATEST e aggiorni la versione cui questi puntano, le operazioni in batch S3 iniziano a

chiamare la nuova versione della funzione Lambda. Ciò può essere utile quando desideri aggiornare la parte di funzionalità durante un processo di grandi dimensioni. Se non si desidera che Operazioni in batch S3 modifichi la versione utilizzata, fornisci la versione specifica nel parametro `FunctionARN` quando crei il processo.

Un singolo AWS Lambda processo con S3 Batch Operations può supportare un manifesto con un massimo di 20 miliardi di oggetti.

Utilizzo di Lambda e Operazioni in batch con i bucket di directory

I bucket di directory sono un tipo di bucket Amazon S3 progettato per carichi di lavoro o applicazioni critiche dal punto di vista delle prestazioni che richiedono una latenza costante a una cifra al millisecondo. Per ulteriori informazioni, consulta [Directory buckets](#).

Esistono requisiti speciali per l'uso di Operazioni in batch per invocare funzioni Lambda che agiscono sui bucket della directory. Ad esempio, è necessario strutturare la richiesta Lambda utilizzando uno schema JSON aggiornato e specificare [InvocationSchemaVersion](#) 2.0 (non 1.0) quando si crea il processo. Questo schema aggiornato consente di specificare coppie chiave-valore opzionali per [UserArguments](#), che puoi utilizzare per modificare determinati parametri delle funzioni Lambda esistenti. Per ulteriori informazioni, consulta [Automatizzare l'elaborazione degli oggetti nei bucket di directory Amazon S3 con S3 Batch Operations e AWS Lambda](#) nello Storage Blog. AWS

Codici di risposta e dei risultati

Operazioni in batch S3 invoca la funzione Lambda con una o più chiavi, ognuna delle quali è associata a un `TaskID`. Operazioni in batch S3 si aspetta un codice risultato per chiave dalle funzioni Lambda. Tutti gli ID dei task inviati nella richiesta che non vengono restituiti con un codice di risultato per chiave riceveranno il codice di risultato dal campo `treatMissingKeysAs`. `treatMissingKeysAs` è un campo di richiesta opzionale e ha come valore predefinito `TemporaryFailure`. La tabella seguente contiene gli altri possibili codici di risultato e valori per il campo `treatMissingKeysAs`.

Codice di risposta	Descrizione
Succeeded	L'attività si è conclusa normalmente. Se hai richiesto un rapporto di completamento del processo, la stringa di risultato dell'attività viene inclusa nel rapporto.

Codice di risposta	Descrizione
TemporaryFailure	Nell'attività si è verificato un errore temporaneo e verrà reindirizzata prima del completamento del processo. La stringa risultante viene ignorata. Se questo è l'ultimo reindirizzamento, il messaggio di errore viene incluso nel rapporto finale.
PermanentFailure	Nell'attività si è verificato un errore permanente. Se hai richiesto un rapporto di completamento del processo, l'attività viene contrassegnata come Failed e include la stringa del messaggio di errore. Le stringhe risultanti da attività non riuscite vengono ignorate.

Creazione di una funzione Lambda da utilizzare con le operazioni in batch S3

Questa sezione fornisce esempi di autorizzazioni AWS Identity and Access Management (IAM) da utilizzare con la funzione Lambda. Contiene anche una funzione Lambda di esempio da utilizzare con le operazioni in batch S3. Se non hai mai creato una funzione Lambda prima, consulta [Tutorial: Using AWS Lambda with Amazon S3](#) nella Developer Guide. AWS Lambda

Devi creare funzioni Lambda specifiche da utilizzare con le operazioni in batch S3. Non è possibile riutilizzare le funzioni Lambda esistenti basate su eventi di Amazon S3, perché le funzioni Lambda utilizzate per Operazioni in batch S3 devono accettare e restituire campi di dati speciali.

Important

AWS Lambda le funzioni scritte in Java accettano una [RequestHandler](#) o più interfacce [RequestStreamHandler](#) handler. Tuttavia, per supportare il formato di richiesta e risposta di S3 Batch Operations, è AWS Lambda necessaria l'`RequestStreamHandler` interfaccia per la serializzazione e la deserializzazione personalizzate di una richiesta e risposta. Questa interfaccia consente a Lambda di passare un `InputStream` e `OutputStream` al metodo Java `handleRequest`

Assicurati di specificare l'interfaccia `RequestStreamHandler` quando utilizzi funzioni Lambda con le operazioni in batch S3. Se utilizzi un'interfaccia `RequestHandler`, il

processo batch non riuscirà restituendo il messaggio "Invalid JSON returned in Lambda payload" (JSON non valido restituito nel payload Lambda) nel report di completamento. Per ulteriori informazioni, consulta [Interfacce Handler](#) nella Guida per l'utente di AWS Lambda .

Autorizzazioni IAM di esempio

Di seguito sono riportati alcuni esempi delle autorizzazioni IAM necessarie per utilizzare una funzione Lambda con le operazioni in batch S3.

Example– Policy di trust delle operazioni in batch S3

Di seguito è riportato un esempio di policy di trust che puoi utilizzare per il ruolo IAM in Batch Operations. Questo ruolo IAM viene specificato quando crei il processo e concede a Batch Operations l'autorizzazione per assumere il ruolo IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "batchoperations.s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Example– Policy IAM Lambda

Di seguito è riportato un esempio di policy IAM che fornisce alle operazioni in batch S3 l'autorizzazione per richiamare la funzione Lambda e leggere il manifest di input.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BatchOperationsLambdaPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "lambda:InvokeFunction"
      ],
      "Resource": "*"
    }
  ]
}
```

Richiesta e risposta di esempio

Questa sezione fornisce esempi di richiesta e risposta per la funzione Lambda.

Example Richiesta

Di seguito è riportato un esempio JSON di richiesta per la funzione Lambda.

```
{
  "invocationSchemaVersion": "1.0",
  "invocationId": "YXNkbGZqYWVmaBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "job": {
    "id": "f3cc4f60-61f6-4a2b-8a21-d07600c373ce"
  },
  "tasks": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "s3Key": "customerImage1.jpg",
      "s3VersionId": "1",
      "s3BucketArn": "arn:aws:s3:us-east-1:0123456788:amzn-s3-demo-bucket1"
    }
  ]
}
```

```
}
```

Example Risposta

Di seguito è riportato un esempio JSON di risposta per la funzione Lambda.

```
{
  "invocationSchemaVersion": "1.0",
  "treatMissingKeysAs" : "PermanentFailure",
  "invocationId" : "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "results": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "resultCode": "Succeeded",
      "resultString": "[\"Mary Major\", \"John Stiles\"]"
    }
  ]
}
```

Funzione Lambda di esempio per le operazioni in batch S3

Nell'esempio seguente Python Lambda rimuove un contrassegno di eliminazione da un oggetto con versione.

Come mostrato nell'esempio, le chiavi di operazioni in batch S3 sono codificate in formato URL. Per utilizzare Amazon S3 con altri AWS servizi, è importante decodificare tramite URL la chiave trasmessa da S3 Batch Operations.

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)
logger.setLevel("INFO")

s3 = boto3.client("s3")

def lambda_handler(event, context):
    """
    Removes a delete marker from the specified versioned object.
```

```

:param event: The S3 batch event that contains the ID of the delete marker
               to remove.
:param context: Context about the event.
:return: A result structure that Amazon S3 uses to interpret the result of the
         operation. When the result code is TemporaryFailure, S3 retries the
         operation.
"""
# Parse job parameters from Amazon S3 batch operations
invocation_id = event["invocationId"]
invocation_schema_version = event["invocationSchemaVersion"]

results = []
result_code = None
result_string = None

task = event["tasks"][0]
task_id = task["taskId"]

try:
    obj_key = parse.unquote_plus(task["s3Key"], encoding="utf-8")
    obj_version_id = task["s3VersionId"]
    bucket_name = task["s3BucketArn"].split(":")[-1]

    logger.info(
        "Got task: remove delete marker %s from object %s.", obj_version_id,
obj_key
    )

    try:
        # If this call does not raise an error, the object version is not a delete
        # marker and should not be deleted.
        response = s3.head_object(
            Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
        )
        result_code = "PermanentFailure"
        result_string = (
            f"Object {obj_key}, ID {obj_version_id} is not " f"a delete marker."
        )

        logger.debug(response)
        logger.warning(result_string)
    except ClientError as error:
        delete_marker = error.response["ResponseMetadata"]["HTTPHeaders"].get(
            "x-amz-delete-marker", "false"

```



```

    )
    if delete_marker == "true":
        logger.info(
            "Object %s, version %s is a delete marker.", obj_key,
obj_version_id
        )
        try:
            s3.delete_object(
                Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
            )
            result_code = "Succeeded"
            result_string = (
                f"Successfully removed delete marker "
                f"{obj_version_id} from object {obj_key}."
            )
            logger.info(result_string)
        except ClientError as error:
            # Mark request timeout as a temporary failure so it will be
retried.

            if error.response["Error"]["Code"] == "RequestTimeout":
                result_code = "TemporaryFailure"
                result_string = (
                    f"Attempt to remove delete marker from "
                    f"object {obj_key} timed out."
                )
                logger.info(result_string)
            else:
                raise
        else:
            raise ValueError(
                f"The x-amz-delete-marker header is either not "
                f"present or is not 'true'."
            )
    except Exception as error:
        # Mark all other exceptions as permanent failures.
        result_code = "PermanentFailure"
        result_string = str(error)
        logger.exception(error)
    finally:
        results.append(
            {
                "taskId": task_id,
                "resultCode": result_code,
                "resultString": result_string,

```

```

    }
  )
  return {
    "invocationSchemaVersion": invocation_schema_version,
    "treatMissingKeysAs": "PermanentFailure",
    "invocationId": invocation_id,
    "results": results,
  }
}

```

Creazione di un processo di operazioni in batch Amazon S3 che richiama una funzione Lambda

Quando crei un processo di operazioni in batch Amazon S3 per richiamare una funzione Lambda, devi fornire gli elementi seguenti:

- ARN della funzione Lambda, che può includere l'alias della funzione o un numero specifico di versione
- Ruolo IAM con l'autorizzazione per richiamare la funzione
- Il parametro dell'operazione LambdaInvokeFunction

Per ulteriori informazioni sulla creazione di un processo di operazioni in batch Amazon S3, consulta [Creazione di un processo di operazioni in batch S3](#) e [Operazioni supportate dalle operazioni in batch S3](#).

L'esempio seguente crea un processo di Operazioni in batch S3 che invoca una funzione Lambda utilizzando l'interfaccia AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```

aws s3control create-job
  --account-id account-id
  --operation '{"LambdaInvoke": { "FunctionArn": "arn:aws:lambda:region:account-id:function:LambdaFunctionName" } }'
  --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":["Bucket","Key"],"Location":{"ObjectArn":"arn:aws:s3::amzn-s3-demo-manifest-bucket","ETag":"ManifestETag"}}}'
  --report '{"Bucket":"arn:aws:s3::amzn-s3-demo-bucket","Format":"Report_CSV_20180820","Enabled":true,"Prefix":"ReportPrefix","ReportScope":"AllObjects"}'
  --priority 2

```

```
--role-arn arn:aws:iam::account-id:role/BatchOperationsRole  
--region region  
--description "Lambda Function"
```

Fornitura di informazioni a livello di task nei manifesti Lambda

Quando utilizzi AWS Lambda le funzioni con S3 Batch Operations, potresti aver bisogno di dati aggiuntivi per accompagnare ogni attività o tasto su cui viene operato. Ad esempio, si potrebbe voler fornire sia una chiave dell'oggetto di origine che una chiave dell'oggetto nuovo. La funzione Lambda può quindi copiare la chiave di origine in un nuovo bucket S3 con un nuovo nome. Per impostazione predefinita, Operazioni in batch consente di specificare solo il bucket di destinazione e un elenco di chiavi di origine nel manifesto di input del processo. Gli esempi seguenti descrivono come includere dati aggiuntivi nel manifesto, in modo da poter eseguire funzioni Lambda più complesse.

Per specificare i parametri per chiave nel manifesto di S3 Batch Operations da utilizzare nel codice della funzione Lambda, usa il seguente formato JSON. URL-encoded Il campo key viene passato alla funzione Lambda come se fosse una chiave oggetto Amazon S3. Tuttavia, può essere interpretato dalla funzione Lambda per contenere altri valori o più chiavi, come mostrato negli esempi seguenti.

Note

Il numero massimo di caratteri per il campo key nel manifest è 1.024.

Example- Manifesto che sostituisce le "chiavi Amazon S3" con stringhe JSON

La URL-encoded versione deve essere fornita a S3 Batch Operations.

```
amzn-s3-demo-bucket,{"origKey": "object1key", "newKey": "newObject1Key"}  
amzn-s3-demo-bucket,{"origKey": "object2key", "newKey": "newObject2Key"}  
amzn-s3-demo-bucket,{"origKey": "object3key", "newKey": "newObject3Key"}
```

Example— Manifesto URL-encoded

Questa URL-encoded versione deve essere fornita a S3 Batch Operations. La URL-encoded versione non funzionante non funziona.

```
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object1key%22%2C%20%22newKey%22%3A%20%22newObject1Key%22%7D
```

```
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object2key%22%2C%20%22newKey%22%3A%20%22newObject2Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object3key%22%2C%20%22newKey%22%3A%20%22newObject3Key%22%7D
```

Example– Funzione Lambda con formato manifest che scrive i risultati nel report del processo

Questo esempio di URL-encoded manifesto contiene chiavi oggetto delimitate da pipe per l'analisi della seguente funzione Lambda.

```
amzn-s3-demo-bucket,object1key%7Clower
amzn-s3-demo-bucket,object2key%7Cupper
amzn-s3-demo-bucket,object3key%7Creverse
amzn-s3-demo-bucket,object4key%7Cdelete
```

Questa funzione Lambda mostra come analizzare un'attività delimitata da barra verticale e codificata nel manifesto di Operazioni in batch S3. L'attività indica quale operazione di revisione viene applicata all'oggetto specificato.

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)
logger.setLevel("INFO")

s3 = boto3.resource("s3")

def lambda_handler(event, context):
    """
    Applies the specified revision to the specified object.

    :param event: The Amazon S3 batch event that contains the ID of the object to
                  revise and the revision type to apply.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation.
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
```

```
invocation_schema_version = event["invocationSchemaVersion"]

results = []
result_code = None
result_string = None

task = event["tasks"][0]
task_id = task["taskId"]
# The revision type is packed with the object key as a pipe-delimited string.
obj_key, revision = parse.unquote_plus(task["s3Key"], encoding="utf-8").split("|")
bucket_name = task["s3BucketArn"].split(":")[-1]

logger.info("Got task: apply revision %s to %s.", revision, obj_key)

try:
    stanza_obj = s3.Bucket(bucket_name).Object(obj_key)
    stanza = stanza_obj.get()["Body"].read().decode("utf-8")
    if revision == "lower":
        stanza = stanza.lower()
    elif revision == "upper":
        stanza = stanza.upper()
    elif revision == "reverse":
        stanza = stanza[::-1]
    elif revision == "delete":
        pass
    else:
        raise TypeError(f"Can't handle revision type '{revision}'.")

    if revision == "delete":
        stanza_obj.delete()
        result_string = f"Deleted stanza {stanza_obj.key}."
    else:
        stanza_obj.put(Body=bytes(stanza, "utf-8"))
        result_string = (
            f"Applied revision type '{revision}' to " f"stanza {stanza_obj.key}."
        )

    logger.info(result_string)
    result_code = "Succeeded"
except ClientError as error:
    if error.response["Error"]["Code"] == "NoSuchKey":
        result_code = "Succeeded"
        result_string = (
            f"Stanza {obj_key} not found, assuming it was deleted "
```

```
        f"in an earlier revision."
    )
    logger.info(result_string)
else:
    result_code = "PermanentFailure"
    result_string = (
        f"Got exception when applying revision type '{revision}' "
        f"to {obj_key}: {error}."
    )
    logger.exception(result_string)
finally:
    results.append(
        {
            "taskId": task_id,
            "resultCode": result_code,
            "resultString": result_string,
        }
    )
return {
    "invocationSchemaVersion": invocation_schema_version,
    "treatMissingKeysAs": "PermanentFailure",
    "invocationId": invocation_id,
    "results": results,
}
```

Tutorial su Operazioni in batch S3

I seguenti tutorial illustrano le procedure complete end-to-end per alcune operazioni in batch con Lambda. In questa esercitazione si apprende come impostare Operazioni in batch per invocare una funzione Lambda per la transcodifica in batch dei video memorizzati in un bucket di origine S3. La funzione Lambda chiama a transcodificare i video. AWS Elemental MediaConvert

- [Tutorial: video con S3 Batch Operations Batch-transcoding](#)

Sostituisci tutti i tag oggetto

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. L'operazione Sostituisci tutti i tag dell'oggetto sostituisce i tag dell'oggetto su

ogni oggetto elencato nel manifesto. Un tag di oggetto è una coppia chiave-valore di stringhe che si può usare per memorizzare metadati su un oggetto.

Per creare un processo di sostituzione di tutti i tag degli oggetti, si fornisce un set di tag da applicare. S3 Batch Operations applica lo stesso set di tag a ogni oggetto. Il set di tag fornito sostituisce tutti i set di tag già associati agli oggetti nel manifesto. Operazioni in batch S3 non supporta l'aggiunta di tag agli oggetti mantenendo anche i tag esistenti.

Se gli oggetti nel manifesto si trovano in un bucket con versione, dovrai applicare il set di tag alle versioni specifiche di ogni oggetto. Per farlo, specifica un ID di versione per ogni oggetto del manifesto. Se non si include un ID di versione per alcun oggetto, Operazioni in batch S3 applica il set di tag alla versione più recente di ogni oggetto. Per ulteriori informazioni sui manifesti delle operazioni in batch, consulta [Specifica di un manifesto](#).

Per maggiori informazioni sull'etichettatura degli oggetti, consulta [Etichettare i tuoi oggetti](#) in questa guida e consulta [PutObjectTagging](#), [GetObjectTagging](#), e [DeleteObjectTagging](#) in Riferimento API di Amazon Simple Storage Service.

Per utilizzare la console per creare un processo di sostituzione di tutti i tag degli oggetti, consulta [Creazione di un processo di operazioni in batch S3](#).

Restrizioni e limitazioni

Quando si utilizza Operazioni in batch per sostituire i tag degli oggetti, si applicano le seguenti restrizioni e limitazioni:

- Il ruolo AWS Identity and Access Management (IAM) specificato per eseguire il job Batch Operations deve disporre delle autorizzazioni per eseguire l'operazione sottostante.
[PutObjectTagging](#) Per ulteriori informazioni sulle autorizzazioni richieste, consulta la sezione [PutObjectTagging](#) in Riferimento API di Amazon Simple Storage Service.
- Operazioni in batch S3 utilizza l'operazione [PutObjectTagging](#) di Amazon S3 per applicare i tag a ogni oggetto del manifesto. Tutte le restrizioni e le limitazioni che si applicano all'operazione sottostante si applicano anche ai processi Operazioni in batch S3.
- Un unico processo di sostituzione di tutti i tag degli oggetti può supportare un manifesto con un massimo di 20 miliardi di oggetti.

Sostituzione della lista di controllo degli accessi (ACL)

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. L'operazione Sostituisci lista di controllo degli accessi (ACL) sostituisce le liste di controllo degli accessi (ACL) per ogni oggetto elencato nel manifesto. Utilizzando le ACL, è possibile definire chi può accedere a un oggetto e quali azioni può eseguire.

Note

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne nelle circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Con le ACL disabilitate, puoi utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Operazioni in batch S3 supporta le liste ACL personalizzate definite dall'utente e le liste ACL predefinite che Amazon S3 fornisce con un set di autorizzazioni di accesso predefinite.

Se gli oggetti nel manifest si trovano in un bucket con versione, devi applicare le liste di controllo degli accessi alle versioni specifiche di ogni oggetto. Per farlo, specifica un ID di versione per ogni oggetto del manifesto. Se non si include un ID di versione per un oggetto, Operazioni in batch S3 applica l'ACL alla versione più recente dell'oggetto.

Per ulteriori informazioni sulle ACL in Amazon S3, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

Blocco dell'accesso pubblico di S3

Se si desidera limitare l'accesso pubblico a tutti gli oggetti di un bucket, si consiglia di utilizzare Blocco dell'accesso pubblico Amazon S3 invece di utilizzare Operazioni in batch S3 per applicare le ACL. Il blocco dell'accesso pubblico può limitare l'accesso pubblico a livello di bucket o di account grazie a una sola semplice operazione con effetto rapido. Questo comportamento rende Blocco dell'accesso pubblico Amazon S3 una scelta migliore quando l'obiettivo è controllare l'accesso pubblico a tutti gli oggetti in un bucket o in un account. Utilizza Operazioni in batch S3 solo quando è necessario applicare una lista ACL personalizzata a ogni oggetto del manifesto. Per ulteriori informazioni sul blocco dell'accesso pubblico di S3, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

S3 Object Ownership

Se gli oggetti nel manifesto si trovano in un bucket che utilizza l'impostazione Proprietario del bucket applicato per la proprietà degli oggetti, l'operazione di sostituzione della lista di controllo degli accessi (ACL) può specificare solo le ACL degli oggetti che garantiscono il pieno controllo al proprietario del bucket. In questo caso, l'operazione Replace access control list (ACL) non può concedere le autorizzazioni ACL dell'oggetto ad altri o a gruppi. Account AWS Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Restrizioni e limitazioni

Quando si utilizza Operazioni in batch per sostituire le ACL, si applicano le seguenti restrizioni e limitazioni:

- Il ruolo AWS Identity and Access Management (IAM) specificato per eseguire il job Replace access control list (ACL) deve disporre delle autorizzazioni per eseguire l'operazione Amazon S3 sottostante. PutObjectAcl Per ulteriori informazioni sulle autorizzazioni richieste, consulta la sezione [PutObjectAcl](#) in Riferimento API di Amazon Simple Storage Service.
- S3 Batch Operations utilizza l'operazione PutObjectAcl di Amazon S3 per applicare la lista ACL specificata a ogni oggetto nel manifest. Pertanto, tutte le restrizioni e le limitazioni che si applicano all'operazione sottostante PutObjectAcl si applicano anche ai processi di Operazioni in batch S3 di sostituzione della lista di controllo degli accessi (ACL).
- Un singolo processo di sostituzione della lista di controllo degli accessi può supportare un manifesto con un massimo di 20 miliardi di oggetti.

Ripristino di oggetti con operazioni in batch

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. L'operazione Ripristino avvia le richieste di ripristino per gli oggetti Amazon S3 archiviati elencati nel manifesto. Prima di potervi accedere in tempo reale, i seguenti oggetti archiviati devono essere ripristinati:

- Oggetti archiviati nelle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive
- Oggetti archiviati tramite la classe di Intelligent-Tiering storage S3 nei livelli Archive Access o Deep Archive Access

L'utilizzo di un'operazione di ripristino ([S3InitiateRestoreObjectOperation](#)) nel processo di Operazioni in batch S3 comporta una richiesta a `RestoreObject` per ogni oggetto specificato nel manifesto.

 Important

Il processo di ripristino avvia solo la richiesta di ripristino degli oggetti. S3 Batch Operations riporta il processo come completo per ogni oggetto dopo l'avvio della richiesta per quell'oggetto. Amazon S3 non aggiorna il processo né ti informa in altro modo quando gli oggetti sono stati ripristinati. Tuttavia, puoi utilizzare le notifiche di eventi S3 per ricevere notifiche quando gli oggetti sono disponibili in Amazon S3. Per ulteriori informazioni, consulta [Notifiche di eventi Amazon S3](#).

Quando si crea un processo di ripristino, sono disponibili i seguenti argomenti:

ExpirationInDays

Questo argomento specifica per quanto tempo l'oggetto di S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive rimane disponibile in Amazon S3. I processi di ripristino che hanno come obiettivo gli oggetti Recupero flessibile S3 Glacier e S3 Glacier Deep Archive richiedono l'impostazione di `ExpirationInDays` a 1 o superiore.

 Important

Non impostare `ExpirationInDays` durante la creazione di processi operativi di ripristino destinati agli oggetti dei livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access. Gli oggetti nei livelli di accesso agli Intelligent-Tiering archivi S3 non sono soggetti alla scadenza del ripristino, pertanto la specificazione `ExpirationInDays` comporta un errore di richiesta. `RestoreObject`

GlacierJobTier

Amazon S3 può ripristinare gli oggetti utilizzando uno dei tre diversi livelli di recupero: EXPEDITED, STANDARD e BULK. Tuttavia, S3 Batch Operations supporta solo i livelli di recupero STANDARD e BULK. Per ulteriori informazioni sulle differenze tra i livelli di recupero, consulta [Informazioni sulle opzioni di recupero dall'archivio](#).

Per ulteriori informazioni sui prezzi per ogni livello, consulta la sezione Richieste e recupero dati nella [pagina dei prezzi di Amazon S3](#).

Differenze durante il ripristino da S3 Glacier e S3 Intelligent-Tiering

Il ripristino dei file archiviati dalle classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive è diverso dal ripristino dei file dalla classe di storage S3 nei livelli Archive Access o Deep Archive Access. Intelligent-Tiering

- Quando esegui il ripristino da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, viene creata una copia temporanea dell'oggetto. Amazon S3 elimina questa copia dopo che il valore specificato nell'argomento `ExpirationInDays` è trascorso. Dopo aver eliminato questa copia temporanea, dovrai inviare una richiesta di ripristino aggiuntiva per accedere all'oggetto.
- Quando ripristini oggetti S3 archiviati, non specifichi l'argomento `ExpirationInDays`. Quando ripristini un oggetto dai livelli S3 Intelligent-Tiering Archive Access o Deep Archive Access, l'oggetto torna al livello S3 Frequent Access. Intelligent-Tiering Dopo un minimo di 90 giorni consecutivi senza accesso, l'oggetto passa automaticamente al livello Accesso archivio. Dopo un minimo di 180 giorni consecutivi senza accesso, l'oggetto passa automaticamente al livello Accesso archivio approfondito.
- I job Batch Operations possono essere eseguiti sugli oggetti delle classi di storage S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive o sugli oggetti dei livelli di storage S3 Archive Access e Deep Archive Access Intelligent-Tiering. Le operazioni in batch non possono operare su entrambi i tipi di oggetti archiviati nello stesso processo. Per ripristinare oggetti di entrambi i tipi, devi creare processi Batch Operations separati.

Ripristini sovrapposti

Se il processo [S3InitiateRestoreObjectOperation](#) tenta di ripristinare un oggetto che è già in fase di ripristino, Operazioni in batch S3 procede come segue.

L'operazione di ripristino dell'oggetto riesce se una di queste condizioni restituisce true:

- Confrontato alla richiesta di ripristino già in corso, il valore `ExpirationInDays` del processo è uguale e il relativo valore `GlacierJobTier` è più veloce.
- La richiesta di ripristino precedente è già stata completata e l'oggetto è attualmente disponibile. In questo caso, le operazioni in batch aggiornano la data di scadenza dell'oggetto ripristinato in modo che corrisponda al valore `ExpirationInDays` specificato nella richiesta di ripristino in corso.

L'operazione di ripristino dell'oggetto non riesce se una o più delle seguenti condizioni restituisce true:

- La richiesta di ripristino già in corso non è ancora stata completata e la durata del ripristino per questo processo (specificata dal valore `ExpirationInDays`) è diversa dalla durata del ripristino specificata nella richiesta in corso.
- Il livello di ripristino per questo processo (specificato dal valore `GlacierJobTier`) è uguale o più lento del livello di ripristino specificato nella richiesta di ripristino in corso.

Limitazioni

I processi `S3InitiateRestoreObjectOperation` hanno le seguenti limitazioni:

- Devi creare il processo nella stessa regione degli oggetti archiviati.
- Operazioni in batch S3 non supporta il livello di recupero `EXPEDITED`.
- Un singolo processo di ripristino di Operazioni in batch può supportare un manifesto con un massimo di 4 miliardi di oggetti.

Per ulteriori informazioni sul ripristino degli oggetti, consulta [Ripristino di un oggetto archiviato](#).

Aggiorna la crittografia degli oggetti

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. L'operazione Batch [UpdateObjectEncryption](#) Operations aggiorna il tipo di crittografia lato server di più di un oggetto Amazon S3 con una singola richiesta. Una singola `UpdateObjectEncryption` operazione può supportare un manifesto con un massimo di 20 miliardi di oggetti.

L'`UpdateObjectEncryption` operazione è supportata per tutte le classi di storage Amazon S3 supportate da bucket generici. È possibile utilizzare l'`UpdateObjectEncryption` operazione per modificare gli oggetti crittografati dalla [crittografia lato server con chiavi gestite da Amazon S3 \(SSE-S3\)](#) a chiavi [AWS Key Management Service \(\) \(AWS KMS\)](#) o per applicare le chiavi bucket [SSE-KMS S3](#). Puoi anche utilizzare l'`UpdateObjectEncryption` operazione per modificare la chiave KMS gestita dal cliente utilizzata per crittografare i dati in modo da rispettare gli standard personalizzati di rotazione delle chiavi.

Quando si crea un job Batch Operations, è possibile generare un elenco di oggetti in base alla posizione di origine e ai criteri di filtro specificati. È possibile utilizzare il

MatchAnyObjectEncryption filtro per generare un elenco di oggetti dal bucket che si desidera aggiornare e includere nel manifest. L'elenco degli oggetti generato include solo gli oggetti bucket di origine con il tipo di crittografia lato server indicato. Se si seleziona SSE-KMS, è possibile filtrare ulteriormente i risultati specificando uno stato specifico di attivazione di KMS Key ARN e Bucket Key. Per ulteriori informazioni, consulta [JobManifestGeneratorFilter](#) e [SSEKMSFilter in Amazon S3API Reference](#).

Restrizioni e considerazioni

Quando si utilizza l'operazione Batch UpdateObjectEncryption Operations, si applicano le seguenti restrizioni e considerazioni:

- L'UpdateObjectEncryptionoperazione non supporta oggetti non crittografati o oggetti crittografati con crittografia lato server a doppio livello con AWS KMS keys (DSSE-KMS) o chiavi di crittografia fornite dal cliente (). SSE-C Inoltre, non è possibile specificare il tipo di richiesta di crittografia. SSE-S3 UpdateObjectEncryption
- È possibile utilizzare l'UpdateObjectEncryptionoperazione per aggiornare gli oggetti nei bucket in cui è abilitato il controllo delle versioni di S3. Per aggiornare il tipo di crittografia di una particolare versione, è necessario specificare un ID di versione nella richiesta. UpdateObjectEncryption Se non si specifica l'ID di versione, la UpdateObjectEncryption richiesta agisce sulla versione corrente dell'oggetto. Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [the section called “Conservazione più versioni degli oggetti”](#).
- L'UpdateObjectEncryptionoperazione ha esito negativo su qualsiasi oggetto a cui è applicata una modalità di conservazione S3 Object Lock o un blocco legale. Se un oggetto ha un periodo di conservazione in modalità governativa o un blocco legale, è necessario rimuovere lo stato Object Lock sull'oggetto prima di emettere la richiesta. UpdateObjectEncryption Non è possibile utilizzare l'UpdateObjectEncryptionoperazione con oggetti a cui è applicato un periodo di conservazione in modalità di conformità Object Lock. Per ulteriori informazioni sul blocco degli oggetti S3, consulta [the section called “Blocco degli oggetti”](#).
- UpdateObjectEncryptionle richieste sui bucket di origine con la replica in tempo reale abilitata non avvieranno eventi di replica nel bucket di destinazione. Se desideri modificare il tipo di crittografia degli oggetti nei bucket di origine e di destinazione, devi avviare UpdateObjectEncryption richieste separate sugli oggetti nei bucket di origine e di destinazione.
- Per impostazione predefinita, tutte le UpdateObjectEncryption richieste che specificano una chiave KMS gestita dal cliente sono limitate alle chiavi KMS di proprietà del proprietario del bucket. Account AWS Se stai utilizzando AWS Organizations, puoi richiedere la possibilità di

utilizzare account di AWS KMS keys proprietà di altri membri all'interno della tua organizzazione contattando. Supporto AWS

- Se utilizzi S3 Batch Replication per replicare set di dati in più regioni e in precedenza il tipo di crittografia lato server era aggiornato dal SSE-S3 al SSE-KMS, potresti aver bisogno di autorizzazioni aggiuntive. Nel bucket della regione di origine, è necessario disporre delle autorizzazioni `kms:decrypt`. Quindi, avrai bisogno delle `kms:encrypt` autorizzazioni `kms:decrypt` e per il bucket nella regione di destinazione.
- Fornisci un ARN completo della chiave KMS nella tua richiesta. `UpdateObjectEncryption` Non puoi utilizzare un nome alias o un alias ARN. Puoi determinare l'ARN completo della chiave KMS nella console AWS KMS o utilizzando l'API AWS KMS. `DescribeKey`
- Per migliorare le prestazioni di generazione di manifesti quando usi il `KmsKeyArn` filtro, utilizza questo filtro insieme ad altri filtri di metadati degli oggetti. Ad esempio, è possibile combinarlo `KmsKeyArn` con `MatchAnyPrefix` o `MatchAnyStorageClass` quando si genera automaticamente un manifesto in S3 Batch Operations. `CreatedAfter`

Per ulteriori informazioni su `UpdateObjectEncryption`, consultare [the section called "Aggiornamento della crittografia"](#).

Autorizzazioni richieste

Per eseguire l'`UpdateObjectEncryption` operazione, aggiungi la seguente policy AWS Identity and Access Management (IAM) al tuo principale IAM (utente, ruolo o gruppo). Per utilizzare questa policy, *amzn-s3-demo-bucket* sostituiscila con il nome del bucket che contiene gli oggetti per i quali desideri aggiornare la crittografia. Sostituisci *amzn-s3-demo-manifest-bucket* con il nome del bucket che contiene il tuo manifest e sostituisci *amzn-s3-demo-completion-report-bucket* con il nome del bucket in cui desideri archiviare il rapporto di completamento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3BatchOperationsUpdateEncryption",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:UpdateObjectEncryption"
      ],
    },
  ],
}
```

```

    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket-target"
        "arn:aws:s3:::amzn-s3-demo-bucket-target-target/*"
    ]
},
{
    "Sid": "S3BatchOperationsPolicyForManifestFile",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket-manifest/*"
    ]
},
{
    "Sid": "S3BatchOperationsPolicyForCompletionReport",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket-completion-report/*"
    ]
},
{
    "Sid": "S3BatchOperationsPolicyManifestGeneration",
    "Effect": "Allow",
    "Action": [
        "s3:PutInventoryConfiguration"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket-target"
    ]
},
{
    "Sid": "AllowKMSOperationsForS3BatchOperations",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",

```

```
        "kms:ReEncrypt*",
      ],
      "Resource": [
        "arn:aws:kms:us-  
east-1:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"
      ]
    }
  ]
}
```

Per la politica di fiducia e la politica delle autorizzazioni da collegare al ruolo IAM che il responsabile del servizio S3 Batch Operations assume per eseguire i lavori Batch Operations per tuo conto, vedi e. [the section called “Concessione di autorizzazioni”](#) [the section called “Aggiorna la crittografia degli oggetti”](#)

Creazione di un job Batch Operations per aggiornare la crittografia degli oggetti

Per aggiornare il tipo di crittografia lato server di più di un oggetto Amazon S3 con una singola richiesta, puoi utilizzare S3 Batch Operations. Puoi utilizzare S3 Batch Operations tramite la console Amazon S3, AWS Command Line Interface (AWS CLI) AWS SDK o l'API REST di Amazon S3.

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano installati e configurati AWS CLI . Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

In alternativa, puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Example 1 — Creare un processo Batch Operations che aggiorni gli oggetti crittografati partendo da un unico processo AWS KMS key a un'altra chiave KMS

L'esempio seguente mostra come creare un job S3 Batch Operations che aggiorna le impostazioni di crittografia per più oggetti nel bucket generico. Questo comando crea un processo che modifica gli oggetti crittografati con una AWS Key Management Service (AWS KMS) chiave per utilizzare una chiave KMS diversa. Questo job inoltre genera e salva un manifesto degli oggetti interessati e crea un report dei risultati. Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate.


```
aws s3control create-job --account-id account-id \
--no-confirmation-required \
--operation '{"S3UpdateObjectEncryption": { "ObjectEncryption": { "SSEKMS":
{ "KMSKeyArn": "KMS-key-ARN-to-apply", "BucketKeyEnabled": false } } } }' \
--report '{ "Enabled": true, "Bucket": "report-bucket-ARN", "Format":
"Report_CSV_20180820", "Prefix": "report", "ReportScope": "AllTasks" }' \
--manifest-generator '{ "S3JobManifestGenerator": { "ExpectedBucketOwner":
"account-id", "SourceBucket": "source-bucket-ARN", "EnableManifestOutput": true,
"ManifestOutputLocation": { "Bucket": "manifest-bucket-ARN", "ManifestFormat":
"S3InventoryReport_CSV_20211130", "ManifestPrefix": "manifest-prefix" }, "Filter":
{ "MatchAnyObjectEncryption": [{ "SSEKMS": { "KmsKeyArn": "kms-key-ARN-to-
match" } } ] } } }' \
--priority 1 \
--role-arn batch-operations-role-ARN
```

Per ottenere prestazioni ottimali, si consiglia di utilizzare il KmsKeyArn filtro insieme ad altri filtri per i metadati degli oggetti, ad esempio MatchAnyPrefix, CreatedAfter o. MatchAnyStorageClass

Example 2 — Creare un processo Batch Operations che SSE-S3 aggiorni gli oggetti crittografati in SSE-KMS

L'esempio seguente mostra come creare un job S3 Batch Operations che aggiorna le impostazioni di crittografia per più oggetti nel bucket generico. Questo comando crea un processo che modifica gli oggetti crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) per utilizzare invece la crittografia lato server con AWS Key Management Service () keys ().AWS KMS SSE-KMS Questo job inoltre genera e salva un manifesto degli oggetti interessati e crea un report dei risultati. Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control create-job --account-id account-id \
--no-confirmation-required \
--operation '{"S3UpdateObjectEncryption": { "ObjectEncryption": { "SSEKMS":
{ "KMSKeyArn": "KMS-key-ARN-to-apply", "BucketKeyEnabled": false } } } }' \
--report '{ "Enabled": true, "Bucket": "report-bucket-ARN", "Format":
"Report_CSV_20180820", "Prefix": "report", "ReportScope": "AllTasks" }' \
--manifest-generator '{ "S3JobManifestGenerator": { "ExpectedBucketOwner":
"account-id", "SourceBucket": "source-bucket-ARN", "EnableManifestOutput": true,
"ManifestOutputLocation": { "Bucket": "manifest-bucket-ARN", "ManifestFormat":
"S3InventoryReport_CSV_20211130", "ManifestPrefix": "manifest-prefix" }, "Filter": {
"MatchAnyObjectEncryption": [{ "SSES3": {} } ] } } }' \
--priority 1 \
```

```
--role-arn batch-operations-role-ARN
```

Per ottenere prestazioni ottimali, si consiglia di utilizzare il KmsKeyArn filtro insieme ad altri filtri per i metadati degli oggetti, ad esempio MatchAnyPrefix, CreatedAfter o MatchAnyStorageClass.

Conservazione Blocco oggetto S3

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. È possibile utilizzare l'operazione di conservazione Object Lock per applicare le date di conservazione agli oggetti utilizzando la modalità di governance o la modalità di conformità. Queste modalità di conservazione applicano livelli di protezione diversi. È possibile applicare entrambe le modalità di conservazione a qualsiasi versione di oggetto. Le date di conservazione, ad esempio per un blocco di carattere legale, impediscono di sovrascrivere o eliminare un oggetto. Amazon S3 memorizza la data di conservazione specificata nei metadati dell'oggetto e protegge la versione specificata dell'oggetto fino alla scadenza del periodo di conservazione.

È possibile utilizzare Operazioni in batch S3 con Object Lock per gestire le date di conservazione di più oggetti Amazon S3 contemporaneamente. Si specifica l'elenco degli oggetti di destinazione nel manifesto e si invia il manifesto a Operazioni in batch per il completamento. Per ulteriori informazioni, consulta del blocco oggetti S [the section called “Periodi di conservazione”](#).

Il processo di operazioni in batch Amazon S3 con date di conservazione viene eseguito fino al completamento, all'annullamento o al raggiungimento di uno stato di errore. Si consiglia di utilizzare la conservazione di Operazioni in batch S3 e S3 Object Lock per aggiungere, modificare o rimuovere la data di conservazione per più oggetti con un'unica richiesta.

Le operazioni in batch verificano che sia abilitato il blocco oggetti nel bucket prima di elaborare qualsiasi chiave nel manifest. Per eseguire le operazioni e la convalida, Batch Operations necessita delle s3:PutObjectRetention autorizzazioni s3:GetBucketObjectLockConfiguration and in un ruolo AWS Identity and Access Management (IAM) per consentire a Batch Operations di chiamare Object Lock per conto dell'utente. Per ulteriori informazioni, consulta [the section called “Considerazioni su Object Lock”](#).

Per informazioni sull'uso di questa operazione con la REST API, consulta S3PutObjectRetention nell'operazione [CreateJob](#) in Riferimento API di Amazon Simple Storage Service.

Per un AWS Command Line Interface (AWS CLI) esempio di utilizzo di questa operazione, vedere [the section called “Utilizzo di Operazioni in batch con la conservazione Object Lock”](#) Per un AWS SDK per Java esempio, vedere [the section called “Utilizzo di Operazioni in batch con la conservazione Object Lock”](#).

Restrizioni e limitazioni

Quando si utilizza Operazioni in batch per applicare i periodi di conservazione Object Lock, si applicano le seguenti restrizioni e limitazioni:

- Operazioni in batch S3 non apporta modifiche a livello di bucket.
- Le funzioni Controllo Versioni e Blocco oggetti S3 devono essere configurati nel bucket in cui viene eseguito il processo.
- Tutti gli oggetti elencati nel manifesto devono trovarsi nello stesso bucket.
- L'operazione funziona sulla versione più recente dell'oggetto, a meno che non venga specificata esplicitamente una versione nel manifest.
- Per utilizzare un processo di conservazione Object Lock è necessario disporre dell'autorizzazione `s3:PutObjectRetention` nel proprio ruolo IAM.
- L'autorizzazione IAM `s3:GetBucketObjectLockConfiguration` è necessaria per confermare che Object Lock sia abilitato per il bucket S3 su cui si sta eseguendo il processo.
- È possibile estendere solo il periodo di conservazione degli oggetti a cui sono applicate le date di conservazione in modalità COMPLIANCE e questo periodo di conservazione non può essere ridotto.
- Un singolo processo di conservazione di S3 Object Lock può supportare un manifesto con un massimo di 20 miliardi di oggetti.

Blocco di carattere legale del blocco oggetti S3

È possibile utilizzare Operazioni in batch Amazon S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. È possibile utilizzare l'operazione di Blocco legale Object Lock per inserire un blocco legale su una versione dell'oggetto. Analogamente all'impostazione di un periodo di conservazione, un blocco a di carattere legale impedisce che una versione di un oggetto venga sovrascritta o eliminata. Tuttavia, un blocco legale non ha un periodo di conservazione associato e rimane in vigore finché non viene rimosso.

Puoi utilizzare S3 Batch Operations con il blocco oggetti per aggiungere blocchi di carattere legale a molti oggetti Amazon S3 contemporaneamente. A tale scopo, specificare un elenco di oggetti di destinazione nel manifesto e inviare tale elenco a Operazioni in batch. Il processo di Operazioni in batch S3 Blocco legale Object Lock viene eseguito fino al completamento, all'annullamento o al raggiungimento di uno stato di errore.

Operazioni in batch S3 verifica che Object Lock sia abilitato sul bucket S3 prima di elaborare qualsiasi oggetto nel manifesto. Per eseguire le operazioni sugli oggetti e la convalida a

livello di bucket, S3 Batch Operations necessita del ruolo `s3:PutObjectLegalHold` and `s3:GetBucketObjectLockConfiguration` in un ruolo AWS Identity and Access Management (IAM). Queste autorizzazioni consentono a Operazioni in batch S3 di chiamare S3 Object Lock per conto dell'utente.

Quando si crea un processo Operazioni in batch S3 per rimuovere un blocco legale, è sufficiente specificare `Off` come stato di blocco legale. Per ulteriori informazioni, consulta [the section called "Considerazioni su Object Lock"](#).

Per informazioni su come utilizzare questa operazione con la REST API di Amazon S3, consulta `S3PutObjectLegalHold` nell'operazione [CreateJob](#) in Riferimento API di Amazon Simple Storage Service.

Per un esempio di utilizzo di questa operazione, consulta [Utilizzo di AWS SDK per Java](#).

Restrizioni e limitazioni

Quando si utilizza Operazioni in batch per applicare o rimuovere un blocco legale Object Lock, si applicano le seguenti restrizioni e limitazioni:

- Operazioni in batch S3 non apporta modifiche a livello di bucket.
- Tutti gli oggetti elencati nel manifest devono trovarsi nello stesso bucket.
- Le funzioni Controllo versioni e Blocco oggetti S3 devono essere configurati nel bucket in cui viene eseguito il processo.
- L'operazione di Blocco legale Object Lock funziona sulla versione più recente dell'oggetto, a meno che non sia specificata esplicitamente una versione nel manifesto.
- L'autorizzazione `s3:PutObjectLegalHold` è necessaria nel proprio ruolo IAM per aggiungere o rimuovere un blocco legale dagli oggetti.
- L'autorizzazione IAM `s3:GetBucketObjectLockConfiguration` è necessaria per confermare che S3 Object Lock è abilitato per il bucket S3 in cui viene eseguito il processo.
- Un singolo processo di blocco legale di S3 Object Lock può supportare un manifesto con un massimo di 20 miliardi di oggetti.
- [Copia oggetti](#)
- [Calcolo dei checksum](#)
- [Elimina tutti i tag oggetto](#)

- [Invoke AWS Lambda funzione](#)
- [Sostituisci tutti i tag oggetto](#)
- [Sostituzione della lista di controllo degli accessi \(ACL\)](#)
- [Ripristino di oggetti con operazioni in batch](#)
- [Aggiorna la crittografia degli oggetti](#)
- [Replica di oggetti esistenti con Replica in batch](#)
- [Conservazione Blocco oggetto S3](#)
- [Blocco di carattere legale del blocco oggetti S3](#)

Gestione dei processi di operazioni in batch Amazon S3

Amazon S3 fornisce un valido set di strumenti che consentono di gestire i processi di operazioni in batch S3 dopo la loro creazione. Questa sezione descrive le operazioni che puoi utilizzare per gestire e tracciare i tuoi lavori utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3.

Argomenti

- [Utilizzo della console Amazon S3 per gestire i processi S3 Batch Operations](#)
- [Elenchi di processi](#)
- [Visualizzazione dettagli processo](#)
- [Assegnazione della priorità dei processi](#)

Utilizzo della console Amazon S3 per gestire i processi S3 Batch Operations

Puoi gestire i processi S3 Batch Operations utilizzando la console. Ad esempio, puoi:

- Visualizzare i processi attivi e in coda
- Verifica lo stato di un lavoro
- Modificare la priorità di un processo
- Confermare ed eseguire un processo
- Clonazione di un processo
- Annullamento di un processo

Gestione di Batch Operations tramite la console

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Operazioni in batch.
3. Scegli il lavoro che desideri gestire.

Elenchi di processi

Puoi recuperare un elenco dei tuoi processi di operazioni in batch Amazon S3. L'elenco fornisce informazioni sui lavori non ancora terminati e sui lavori terminati negli ultimi 90 giorni. Per ogni lavoro, l'elenco include dettagli quali l'ID del lavoro, la descrizione, la priorità, lo stato corrente e il numero di attività completate e non riuscite.

Puoi filtrare l'elenco dei processi in base allo stato. Se recuperi l'elenco utilizzando la console, puoi anche cercare i lavori per descrizione o ID e filtrarli per. Regione AWS

Ottieni un elenco di offerte di **lavoro attivo e complete**

L' AWS CLI esempio seguente ottiene un elenco Active di Complete lavori. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control list-jobs \  
  --region us-west-2 \  
  --account-id account-id \  
  --job-statuses '["Active","Complete"]' \  
  --max-results 20
```

Per ulteriori informazioni ed esempi, consulta [list-jobs](#) nel Riferimento ai comandi AWS CLI .

Visualizzazione dettagli processo

Se desideri più informazioni su un job di Amazon S3 Batch Operations rispetto a quelle che puoi recuperare elencando i lavori, puoi visualizzare tutti i dettagli relativi a un singolo job. Puoi visualizzare i dettagli dei lavori non ancora terminati o dei lavori terminati negli ultimi 90 giorni. Oltre alle informazioni restituite in un elenco di lavori, i dettagli di un singolo lavoro includono informazioni come:

- I parametri dell'operazione.

- Dettagli sul manifesto.
- Informazioni sul rapporto di completamento, se ne hai configurato uno al momento della creazione del lavoro.
- L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) assegnato per eseguire il job.

Visualizzando i dettagli di un singolo processo, puoi accedere all'intera configurazione del processo. Per visualizzare i dettagli di un processo, puoi utilizzare la console Amazon S3 o AWS Command Line Interface (AWS CLI).

Ottenere la descrizione di un processo Operazioni in batch Amazon S3 nella console Amazon S3

Per visualizzare una descrizione del processo Operazioni in batch utilizzando la console

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Operazioni in batch.
3. Scegli l'ID del processo specifico per visualizzarne i dettagli.

Ottieni una descrizione del lavoro di S3 Batch Operations nel AWS CLI

Nell'esempio seguente viene recuperata la descrizione di un processo Operazioni in batch Amazon S3 tramite la AWS CLI. Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control describe-job \  
--region us-west-2 \  
--account-id account-id \  
--job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

Per ulteriori informazioni ed esempi, consulta [describe-job](#) nel Riferimento ai comandi AWS CLI .

Assegnazione della priorità dei processi

È possibile assegnare a ogni processo Operazioni in batch Amazon S3 una priorità numerica, che può essere un numero intero positivo. Operazioni in batch S3 assegna la priorità ai processi in base alla priorità assegnata. I processi con priorità superiore (o un valore numero più alto per il parametro

di priorità) vengono valutati per primi. La priorità viene determinata in ordine decrescente, ad esempio a una coda di processi con valore di priorità 10 viene assegnata una preferenza di pianificazione rispetto a una coda di processi con valore di priorità 1.

È possibile modificare la priorità di un processo mentre è in esecuzione. Se invii un nuovo processo con una priorità più alta mentre un processo è in esecuzione, il processo di priorità inferiore può essere sospeso per consentire l'esecuzione del processo con priorità più alta.

La modifica della priorità di un processo non influisce sulla velocità di elaborazione del processo.

Note

Operazioni in batch S3 assegna le priorità dei processi secondo il principio del miglior tentativo. Sebbene i processi con priorità più alta abbiano generalmente la precedenza su quelli con priorità più bassa, Amazon S3 non garantisce un ordine rigoroso dei processi.

Utilizzo della console S3

Come aggiornare la priorità dei processi nella console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Operazioni in batch.
3. Scegli il processo specifico che desideri gestire.
4. Scegli Actions (Operazioni). Nell'elenco a discesa, scegli Update priority (Aggiorna priorità).

Utilizzo di AWS CLI

L'esempio seguente aggiorna la priorità del processo utilizzando il comando AWS CLI. Un numero più alto indica una priorità di esecuzione più alta. Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control update-job-priority \  
  --region us-west-2 \  
  --account-id account-id \  
  --priority 98 \  
  --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```


Utilizzo di AWS SDK per Java

Per aggiornare la priorità di un job S3 Batch Operations utilizzando l' AWS SDK per Java, puoi utilizzare il client S3Control per modificare la priorità di esecuzione del job, che determina l'ordine in cui i job vengono elaborati rispetto agli altri job in coda.

Per ulteriori informazioni sulla priorità dei processi, consulta [Assegnazione della priorità dei processi](#).

Per esempi di come aggiornare la priorità dei job con l' AWS SDK per Java, consulta [Aggiornare la priorità di un job](#) batch nell'API Reference di Amazon S3.

Monitoraggio dei rapporti sullo stato e sul completamento dei processi

Con le operazioni in batch S3 è possibile visualizzare e aggiornare lo stato del processo, aggiungere notifiche e registrazione, tenere traccia degli errori di processo e generare report di completamento.

Argomenti

- [Stati del processo](#)
- [Aggiornamento dello stato del processo](#)
- [Notifiche e registrazione](#)
- [Tracciamento dei fallimenti dei processi](#)
- [Rapporti di completamento](#)
- [Esempi: monitoraggio di un processo S3 Batch Operations in Amazon EventBridge tramite AWS CloudTrail](#)
- [Esempi: report di completamento delle operazioni in batch S3](#)

Stati del processo

Una volta creato e avviato, un processo passa attraverso una serie di stati. La tabella seguente descrive gli stati e le possibili transizioni tra di essi.

Stato	Descrizione	Transizioni
New	Quando viene creato, un processo è nello stato New.	Un processo passa automaticamente allo stato Preparing quando Amazon S3 inizia a elaborare l'oggetto manifest.

Stato	Descrizione	Transizioni
Preparing	Amazon S3 sta elaborando l'oggetto manifest e altri parametri allo scopo di configurare ed eseguire il processo.	<p>Un processo passa automaticamente allo stato Ready quando Amazon S3 termina l'elaborazione del manifest e di altri parametri. Il processo è quindi pronto per iniziare a eseguire l'operazione specificata sugli oggetti elencati nel manifesto.</p> <p>Se il processo richiede una conferma prima dell'esecuzione, ad esempio quando si crea un processo mediante la console Amazon S3, il processo passa dallo stato <code>Preparing</code> allo stato <code>Suspended</code>. Rimane nello stato <code>Suspended</code> finché non confermi di eseguirlo.</p>

Stato	Descrizione	Transizioni
Suspended	Il processo richiede una conferma, ma l'utente non ha ancora confermato di volerlo eseguire. La conferma viene richiesta solo per i processi creati mediante la console Amazon S3. Un processo creato con la console entra nello stato Suspended subito dopo Preparing . Dopo aver confermato l'esecuzione del processo e quando il processo passa allo stato Ready, non torna mai allo stato Suspended .	Una volta confermata l'esecuzione del processo, lo stato cambia in Ready.
Ready	Amazon S3 è pronto per iniziare l'esecuzione delle operazioni richieste sugli oggetti.	Un processo passa automaticamente allo stato Active quando Amazon S3 inizia a eseguirlo. La quantità di tempo durante il quale un processo rimane nello stato Ready dipende dalla presenza o meno di processi con priorità più alta già in esecuzione e dal tempo necessario per completare questi processi.

Stato	Descrizione	Transizioni
Active	Amazon S3 sta eseguendo un'operazione richiesta sugli oggetti elencati nel manifest. Mentre un processo è in corsoActive, puoi monitorarne l'avanzamento utilizzando la console Amazon S3 o l'DescribeJob operazione tramite l'API REST o gli SDK AWS CLI. AWS	Un processo esce dallo stato Active quando non esegue più operazioni sugli oggetti. Questo comportamento può avvenire automaticamente, ad esempio quando un processo viene completato con successo o fallisce. Questo comportamento può anche verificarsi in seguito ad azioni dell'utente, come l'annullamento di un processo. Lo stato successivo del processo dipende dal motivo della transizione.
Pausing	Il processo sta passando allo stato Paused da un altro stato.	Un processo passa automaticamente allo stato Paused al termine della fase Pausing.
Paused	Un processo può passare allo stato Paused se si invia un altro processo con priorità più alta mentre il processo corrente è in esecuzione.	Un processo Paused torna automaticamente allo stato Active quando i processi con priorità più alta che ne stanno bloccando l'esecuzione vengono completati, sospesi o hanno esito negativo.
Completing	Il processo sta passando allo stato Complete da un altro stato.	Un processo passa automaticamente allo stato Complete al termine della fase Completing .

Stato	Descrizione	Transizioni
Complete	Il processo ha terminato l'esecuzione dell'operazione richiesta su tutti gli oggetti elencati nel manifest. Per ogni oggetto, l'operazione potrebbe aver avuto esito positivo o negativo. Se il processo è stato configurato in modo da generare un rapporto di completamento, tale rapporto sarà disponibile non appena il processo sarà passato allo stato Complete.	Complete è uno stato terminale. Una volta che un processo raggiunge Complete, non passa a nessun altro stato.
Cancelling	Il processo sta passando allo stato Cancelled .	Un processo passa automaticamente allo stato Cancelled al termine della fase Cancelling .
Cancelled	L'utente ha richiesto l'annullamento del processo e Operazioni in batch S3 ha annullato il processo con successo. Il processo non invierà nuove richieste ad Amazon S3.	Cancelled è uno stato terminale. Dopo che un processo ha raggiunto Cancelled , il processo non passerà a nessun altro stato.
Failing	Il processo sta passando allo stato Failed.	Un processo passa automaticamente allo stato Failed al termine della fase Failing.

Stato	Descrizione	Transizioni
Failed	Il processo ha avuto esito negativo e non è più in esecuzione. Per ulteriori informazioni sugli errori dei processi, consulta Tracciamento dei fallimenti dei processi .	Failed è uno stato terminale. Dopo che un processo ha raggiunto Failed, non passerà a nessun altro stato.

Aggiornamento dello stato del processo

I seguenti AWS SDK per Java esempi AWS CLI aggiornano lo stato di un job Batch Operations. Per ulteriori informazioni sull'utilizzo della console Amazon S3 per gestire i processi di Operazioni in batch, consulta [Utilizzo della console Amazon S3 per gestire i processi S3 Batch Operations](#).

Utilizzo di AWS CLI

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le informazioni appropriate.

- Se non si è specificato il parametro `--no-confirmation-required` nel comando `create-job`, il processo rimane in uno stato di sospensione finché non si conferma il processo impostando lo stato su Ready. Amazon S3 rende quindi il processo idoneo per l'esecuzione.

```
aws s3control update-job-status \  
  --region us-west-2 \  
  --account-id 123456789012 \  
  --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \  
  --requested-job-status 'Ready'
```

- Annullare il processo impostandone lo stato su Cancelled.

```
aws s3control update-job-status \  
  --region us-west-2 \  
  --account-id 123456789012 \  
  --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \  
  --status-update-reason "No longer needed" \  
  --requested-job-status Cancelled
```

Utilizzo di AWS SDK per Java

Per esempi di come aggiornare lo stato di un processo con l' AWS SDK per Java, consulta [Aggiornare lo stato di un processo batch](#) nell'API Reference di Amazon S3.

Notifiche e registrazione

Oltre a richiedere i report di completamento, è possibile acquisire, rivedere e verificare l'attività di Operazioni in batch tramite AWS CloudTrail. Poiché Operazioni in batch utilizza le operazioni dell'API Amazon S3 esistenti per eseguire le attività, queste ultime emettono gli stessi eventi che emetterebbero se fossero chiamate direttamente. Pertanto, è possibile monitorare e registrare l'avanzamento del processo e di tutte le sue attività utilizzando gli stessi strumenti e processi di notifica, registrazione e auditing già utilizzati con Amazon S3. Per ulteriori informazioni, consulta gli esempi nelle sezioni seguenti.

Note

Batch Operations genera sia eventi di gestione che di dati CloudTrail durante l'esecuzione del lavoro. Il volume di questi eventi varia in base al numero di chiavi presenti nel manifesto di ogni processo. Per ulteriori informazioni, consulta la [pagina](#) CloudTrail dei prezzi, che include esempi di come i prezzi variano in base al numero di percorsi configurati nel tuo account. Per informazioni su come configurare e registrare gli eventi in base alle tue esigenze, consulta [Creazione del primo trail](#) nella Guida per l'utente di AWS CloudTrail .

Per ulteriori informazioni sugli eventi Amazon S3, consulta [Notifiche di eventi Amazon S3](#).

Tracciamento dei fallimenti dei processi

Se si verifica un problema con un processo di operazioni in batch Amazon S3 che ne impedisce l'esecuzione, ad esempio non riesce a leggere il manifest specificato, il processo non riesce. Quando un processo non riesce, genera uno o più codici o motivi di errore. Operazioni in batch S3 memorizza i codici di errore e i motivi con il processo, in modo da poterli visualizzare richiedendo i dettagli del processo. Se è stato richiesto un rapporto di completamento per il processo, deve contenere anche i codici e i motivi di errore.

Per impedire che i processi eseguano un numero elevato di operazioni non riuscite, Amazon S3 impone una soglia di errore attività su ogni processo di operazioni in batch S3. Quando un processo ha eseguito almeno 1.000 task, Amazon S3 monitora il tasso di fallimento dei task. Se, in qualsiasi momento, la percentuale di errore (il numero di attività non andate a buon fine espresso come

proporzione del numero totale di attività eseguite) supera il 50%, il lavoro non riesce. Se il processo non riesce perché ha superato la soglia di errore attività, è possibile identificare la causa degli errori. È ad esempio possibile che nel manifest siano stati involontariamente inclusi alcuni oggetti che non esistono nel bucket specificato. Dopo aver risolto gli errori, è possibile inviare nuovamente il processo.

Note

Operazioni in batch S3 opera in modo asincrono e i task non vengono necessariamente eseguiti nell'ordine in cui gli oggetti sono elencati nel manifesto. Pertanto non puoi utilizzare l'ordinamento del manifest per determinare quali attività degli oggetti sono riuscite e quali no. Puoi invece esaminare il rapporto di completamento del lavoro (se ne hai richiesto uno) o visualizzare i registri degli AWS CloudTrail eventi per determinare l'origine degli errori.

Rapporti di completamento

Quando crei un processo, puoi richiedere un rapporto di completamento. Finché Operazioni in batch S3 invoca con successo almeno un'attività, Amazon S3 genera un report di completamento dopo che il processo ha terminato l'esecuzione delle attività, è fallito o è stato annullato. Puoi configurare il rapporto di completamento per includere tutte le attività o solo quelle non riuscite.

Il report di completamento include la configurazione del processo, lo stato e le informazioni per ogni attività, tra cui la chiave dell'oggetto e la versione, lo stato, i codici di errore e le descrizioni di eventuali errori. I report di completamento offrono un modo semplice per visualizzare i risultati delle attività in un formato consolidato, senza ulteriori operazioni di configurazione. I report di completamento sono crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Per un esempio di report di completamento, consulta [Esempi: report di completamento delle operazioni in batch S3](#).

Se non configuri un rapporto di completamento, puoi comunque monitorare e verificare il lavoro e le relative attività utilizzando CloudTrail Amazon. CloudWatch Per ulteriori informazioni, consulta i seguenti argomenti:

Argomenti

- [Esempi: monitoraggio di un processo S3 Batch Operations in Amazon EventBridge tramite AWS CloudTrail](#)
- [Esempi: report di completamento delle operazioni in batch S3](#)

Esempi: monitoraggio di un processo S3 Batch Operations in Amazon EventBridge tramite AWS CloudTrail

L'attività dei processi di operazioni in batch Amazon S3 viene registrata in forma di eventi in AWS CloudTrail. Puoi creare una regola personalizzata in Amazon EventBridge e inviare questi eventi alla risorsa di notifica di destinazione di tua scelta, come Amazon Simple Notification Service (Amazon SNS).

Note

Amazon EventBridge è il modo preferito per gestire i tuoi eventi. Amazon CloudWatch Events e Amazon EventBridge sono lo stesso servizio e la stessa API di base, ma EventBridge offrono più funzionalità. Modifiche apportate in una delle due CloudWatch o EventBridge visualizzate in ciascuna console. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).

Esempi di monitoraggio

- [Eventi S3 Batch Operations registrati in CloudTrail](#)
- [EventBridge regola per il monitoraggio degli eventi di lavoro di S3 Batch Operations](#)

Eventi S3 Batch Operations registrati in CloudTrail

Quando viene creato un job Batch Operations, viene registrato come JobCreated evento in CloudTrail. Durante l'esecuzione, il processo cambia stato durante l'elaborazione e vengono registrati altri JobStatusChanged eventi CloudTrail. È possibile visualizzare questi eventi sulla [console CloudTrail](#). Per ulteriori informazioni CloudTrail, consultare la Guida [AWS CloudTrail per l'utente](#).

Note

Vengono registrati solo status-change gli eventi del job di S3 Batch Operations. CloudTrail

Example— Evento di completamento del lavoro di S3 Batch Operations registrato da CloudTrail

```
{  
  "eventVersion": "1.05",
```

```

"userIdentity": {
  "accountId": "123456789012",
  "invokedBy": "s3.amazonaws.com"
},
"eventTime": "2020-02-05T18:25:30Z",
"eventSource": "s3.amazonaws.com",
"eventName": "JobStatusChanged",
"awsRegion": "us-west-2",
"sourceIPAddress": "s3.amazonaws.com",
"userAgent": "s3.amazonaws.com",
"requestParameters": null,
"responseElements": null,
"eventID": "f907577b-bf3d-4c53-b9ed-8a83a118a554",
"readOnly": false,
"eventType": "AwsServiceEvent",
"recipientAccountId": "123412341234",
"serviceEventDetails": {
  "jobId": "d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
  "jobArn": "arn:aws:s3:us-west-2:181572960644:job/d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
  "status": "Complete",
  "jobEventId": "b268784cf0a66749f1a05bce259804f5",
  "failureCodes": [],
  "statusChangeReason": []
}
}

```

EventBridge regola per il monitoraggio degli eventi di lavoro di S3 Batch Operations

L'esempio seguente mostra come creare una regola in Amazon EventBridge per acquisire gli eventi S3 Batch Operations registrati da un target AWS CloudTrail a tua scelta.

Per fare ciò, crei una regola seguendo tutti i passaggi descritti in [Creazione di EventBridge regole che reagiscono agli eventi](#). È possibile incollare la seguente policy personalizzata di modello di eventi delle operazioni in batch S3, se applicabile, e scegliere il servizio di destinazione desiderato.

Policy personalizzata di modello di eventi delle operazioni in batch S3

```

{
  "source": [
    "aws.s3"
  ],
  "detail-type": [

```

```

    "AWS Service Event via CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "s3.amazonaws.com"
    ],
    "eventName": [
      "JobCreated",
      "JobStatusChanged"
    ]
  }
}

```

Gli esempi seguenti sono due eventi Batch Operations inviati ad Amazon Simple Queue Service (Amazon SQS) da una EventBridge regola di evento. Un processo di operazioni in batch attraversa molti stati diversi durante l'elaborazione (New, Preparing, Active e così via), quindi è possibile ricevere diversi messaggi per ogni processo.

Example— JobCreated evento di esempio

```

{
  "version": "0",
  "id": "51dc8145-541c-5518-2349-56d7dffdf2d8",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.s3",
  "account": "123456789012",
  "time": "2020-02-27T15:25:49Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "11112223334444",
      "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-27T15:25:49Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobCreated",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "eventID": "7c38220f-f80b-4239-8b78-2ed867b7d3fa",
    "readOnly": false,

```

```

    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
      "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
      "status": "New",
      "jobEventId": "f177ff24f1f097b69768e327038f30ac",
      "failureCodes": [],
      "statusChangeReason": []
    }
  }
}

```

Example— JobStatusChanged evento di completamento del lavoro

```

{
  "version": "0",
  "id": "c8791abf-2af8-c754-0435-fd869ce25233",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.s3",
  "account": "123456789012",
  "time": "2020-02-27T15:26:42Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "1111222233334444",
      "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-27T15:26:42Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "eventID": "0238c1f7-c2b0-440b-8dbd-1ed5e5833afb",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
      "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",

```

```
    "status": "Complete",
    "jobEventId": "51f5ac17dba408301d56cd1b2c8d1e9e",
    "failureCodes": [],
    "statusChangeReason": []
  }
}
```

Esempi: report di completamento delle operazioni in batch S3

Quando crei un processo di operazioni in batch S3, è possibile richiedere un report di completamento per tutte le attività o solo per le attività non andate a buon fine. Se almeno un'attività è stata invocata correttamente, le operazioni in batch S3 generano un report per i processi che sono stati completati, che non sono andati a buon fine o che sono stati annullati.

Il rapporto di completamento contiene informazioni aggiuntive per ogni attività, inclusi il nome della chiave e la versione dell'oggetto, lo stato, i codici di errore e le descrizioni degli errori. La descrizione degli errori per ogni attività non andata a buon fine può essere utilizzata per diagnosticare problemi durante la creazione del lavoro, come le autorizzazioni. Per i processi Calcola il checksum, il report di completamento contiene i valori di checksum per ogni oggetto.

Note

I report di completamento sono sempre crittografati con chiavi gestite da Amazon S3 (SSE-S3).

Example— file dei risultati Top-level manifesto

Il file `manifest.json` di primo livello contiene le posizioni di tutti i rapporti andati a buon fine e (se il processo conteneva errori) la posizione dei rapporti non andati a buon fine, come mostrato nel seguente esempio.

```
{
  "Format": "Report_CSV_20180820",
  "ReportCreationDate": "2019-04-05T17:48:39.725Z",
  "Results": [
    {
      "TaskExecutionStatus": "succeeded",
      "Bucket": "my-job-reports",
      "MD5Checksum": "83b1c4cbe93fc893f54053697e10fd6e",

```

```
      "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/
results/6217b0fab0de85c408b4be96aeaca9b195a7daa5.csv"
    },
    {
      "TaskExecutionStatus": "failed",
      "Bucket": "my-job-reports",
      "MD5Checksum": "22ee037f3515975f7719699e5c416eaa",
      "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/results/
b2ddad417e94331e9f37b44f1faf8c7ed5873f2e.csv"
    }
  ],
  "ReportSchema": "Bucket, Key, VersionId, TaskStatus, ErrorCode, HTTPStatusCode,
ResultMessage"
}
```

Report sulle attività andate a buon fine

I report sulle attività andate a buon fine contengono i seguenti dati relativi alle attività completate correttamente:

- Bucket
- Key
- VersionId
- TaskStatus
- ErrorCode
- HTTPStatusCode
- ResultMessage

Report sulle attività non andate a buon fine

I report sulle attività non andate a buon fine contengono le seguenti informazioni per tutte le attività non completate:

- Bucket
- Key
- VersionId
- TaskStatus
- ErrorCode

- HTTPStatusCode
- ResultMessage

Example- Report sulle attività della funzione Lambda

Nel seguente esempio, la funzione Lambda ha copiato correttamente l'oggetto Amazon S3 in un altro bucket. La risposta di Amazon S3 restituita viene passata alle operazioni in batch S3 e quindi viene scritta nel report di completamento finale.

```
amzn-s3-demo-bucket1,image_17775,,succeeded,200,,{"u'CopySourceVersionId':
'xVR78haVK1RnurYofbTfYr3ufYbktF8h', u'CopyObjectResult': {u'LastModified':
datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()), u'ETag':
'""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
200, 'RetryAttempts': 0, 'HostId': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn00GoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'RequestId': '3ED5852152014362', 'HTTPHeaders':
{'content-length': '234', 'x-amz-id-2': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn00GoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'x-amz-copy-source-version-id':
'xVR78haVK1RnurYofbTfYr3ufYbktF8h', 'server': 'AmazonS3', 'x-amz-request-id':
'3ED5852152014362', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT', 'content-type':
'application/xml'}}}

amzn-s3-demo-bucket1,image_17763,,succeeded,200,,{"u'CopySourceVersionId':
'6Hj0USim4Wj6BTcbxToXW44pSZ.40pwq', u'CopyObjectResult': {u'LastModified':
datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()),
u'ETag': '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata':
{'HTTPStatusCode': 200, 'RetryAttempts': 0, 'HostId': 'GiCZNYr8LHd/
Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'RequestId':
'1BC9F5B1B95D7000', 'HTTPHeaders': {'content-length': '234', 'x-amz-id-2':
'GiCZNYr8LHd/Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'x-
amz-copy-source-version-id': '6Hj0USim4Wj6BTcbxToXW44pSZ.40pwq', 'server': 'AmazonS3',
'x-amz-request-id': '1BC9F5B1B95D7000', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT',
'content-type': 'application/xml'}}}

amzn-s3-demo-bucket1,image_17860,,succeeded,200,,{"u'CopySourceVersionId':
'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', u'CopyObjectResult': {u'LastModified':
datetime.datetime(2019, 4, 5, 17, 35, 40, tzinfo=tzlocal()), u'ETag':
'""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
200, 'RetryAttempts': 0, 'HostId': 'F9ooZ0gpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'RequestId': '8D9CA56A56813DF3', 'HTTPHeaders':
{'content-length': '234', 'x-amz-id-2': 'F9ooZ0gpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'x-amz-copy-source-version-id':
'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', 'server': 'AmazonS3', 'x-amz-request-id':
'8D9CA56A56813DF3', 'date': 'Fri, 05 Apr 2019 17:35:40 GMT', 'content-type':
'application/xml'}}}
```

Il seguente rapporto di esempio mostra un caso in cui la AWS Lambda funzione è scaduta, causando il superamento della soglia di errore da parte dei guasti. Viene quindi contrassegnata come `PermanentFailure`.

```
amzn-s3-demo-bucket1,image_14975,,failed,200,PermanentFailure,"Lambda returned
function error: {"errorMessage":"2019-04-05T17:35:21.155Z 2845ca0d-38d9-4c4b-
abcf-379dc749c452 Task timed out after 3.00 seconds"}"
amzn-s3-demo-bucket1,image_15897,,failed,200,PermanentFailure,"Lambda returned
function error: {"errorMessage":"2019-04-05T17:35:29.610Z 2d0a330b-de9b-425f-
b511-29232fde5fe4 Task timed out after 3.00 seconds"}"
amzn-s3-demo-bucket1,image_14819,,failed,200,PermanentFailure,"Lambda returned
function error: {"errorMessage":"2019-04-05T17:35:22.362Z fcf5efde-74d4-4e6d-b37a-
c7f18827f551 Task timed out after 3.00 seconds"}"
amzn-s3-demo-bucket1,image_15930,,failed,200,PermanentFailure,"Lambda returned
function error: {"errorMessage":"2019-04-05T17:35:29.809Z 3dd5b57c-4a4a-48aa-8a35-
cbf027b7957e Task timed out after 3.00 seconds"}"
amzn-s3-demo-bucket1,image_17644,,failed,200,PermanentFailure,"Lambda
returned function error: {"errorMessage":"2019-04-05T17:35:46.025Z
10a764e4-2b26-4d8c-9056-1e1072b4723f Task timed out after 3.00 seconds"}"
amzn-s3-demo-bucket1,image_17398,,failed,200,PermanentFailure,"Lambda returned
function error: {"errorMessage":"2019-04-05T17:35:44.661Z 1e306352-4c54-4eba-
aee8-4d02f8c0235c Task timed out after 3.00 seconds"}"
```

Example- Report sulle attività Calcola il checksum

Nell'esempio seguente, l'operazione Calcola il checksum ha calcolato correttamente il checksum per l'oggetto caricato mentre era a riposo. La risposta restituita da Amazon S3 viene passata nuovamente a Operazioni in batch S3 e quindi viene scritta nel report di completamento finale:

```
amzn-s3-demo-bucket1,s3-standard-1mb-test-
object,,succeeded,200,,{"checksum_base64":"bS9T0Q\u003d
\u003d","etag":"3c3c1813042989094598e4b57ecbdc82","checksumAlgorithm":"CRC32","checksums"
```

Il seguente report di esempio mostra cosa succede quando un'operazione Calcola il checksum non riesce, con conseguente report sull'attività non andata a buon fine:

```
amzn-s3-demo-bucket1,image_14975,,failed,200,PermanentFailure,"error details:
{"failureMessage":"Task 2845ca0d-38d9-4c4b-abcf-379dc749c452 SSE-C encryption type
is not supported for this operation", "errorCode": "400"}"
amzn-s3-demo-bucket1,image_14975,,failed,200,PermanentFailure,"error details:
{"failureMessage":"Task 2845ca0d-38d9-4c4b-abcf-379dc749c452 Key not found",
"errorCode": "404"}"
```



```
amzn-s3-demo-bucket1,image_14975,,failed,200,PermanentFailure,"error details:
{""failureMessage"":""Task 2845ca0d-38d9-4c4b-abcfc3-379dc749c452 Internal server error,
please retry", ""errorCode"": "500"}"
```

Controllo dei lavori di accesso ed etichettatura mediante tag

È possibile etichettare e controllare l'accesso ai processi di operazioni in batch Amazon S3 aggiungendo tag. I tag possono essere utilizzati per identificare chi è responsabile di un processo di operazioni in batch. La presenza dei tag dei lavori può consentire o limitare la capacità di un utente di cancellare un lavoro, attivare un lavoro in stato di conferma o cambiare il livello di priorità di un lavoro. È possibile creare processi con tag collegati e aggiungere tag ai processi dopo la loro creazione. Ogni tag è una coppia chiave-valore che può essere inclusa quando si crea il lavoro o si aggiorna in un secondo momento.

Warning

Assicurati che i tuoi tag non contengano informazioni riservate o dati personali.

Considera il seguente esempio di tag: supponiamo che desideri che il reparto Finanze crei un processo Batch Operations. È possibile scrivere una policy AWS Identity and Access Management (IAM) che consenta a un utente di richiamare `CreateJob`, a condizione che il job venga creato con il `Department` tag assegnato al valore `Finance`. Inoltre, è possibile allegare tale policy a tutti gli utenti membri del dipartimento Finanze.

Continuando con questo esempio, è possibile scrivere una policy che consenta a un utente di aggiornare la priorità di qualsiasi lavoro con i tag desiderati o annullare qualsiasi lavoro con tali tag. Per ulteriori informazioni, consulta [the section called “Controllo delle autorizzazioni”](#).

È possibile aggiungere tag a nuovi processi di operazioni in batch Amazon S3 al momento della loro creazione o a processi esistenti.

Sono valide le seguenti limitazioni sui tag:

- È possibile associare fino a 50 tag a un lavoro purché abbiano chiavi tag univoche.
- Una chiave di tag può essere composta da un massimo di 128 caratteri Unicode e i valori di tag possono essere composti da un massimo di 256 caratteri Unicode.
- La chiave e i valori fanno distinzione tra maiuscole e minuscole.

Per ulteriori informazioni sulle restrizioni relative ai tag, consulta [Restrizioni relative ai User-Defined tag](#) nella Guida per l'utente per la Gestione costi e fatturazione AWS.

Operazioni API correlate al tagging dei processi di operazioni in batch Amazon S3

Amazon S3 supporta le seguenti operazioni API specifiche del tagging dei processi di operazioni in batch Amazon S3:

- [GetJobTagging](#) - Restituisce il set di tag associato a un processo di Operazioni in batch.
- [PutJobTagging](#) - Sostituisce il set di tag associato a un processo. La gestione di tag dei processi di operazioni in batch Amazon S3 mediante questa operazione API prevede due scenari distinti:
 - Il processo non ha tag - È possibile aggiungere una serie di etichette a un processo (il processo non ha tag precedenti).
 - Il processo ha un insieme di tag esistenti - Per modificare l'insieme di tag esistente, è possibile sostituirlo completamente o apportare modifiche all'interno dell'insieme di tag esistente, recuperando l'insieme di tag esistente con [GetJobTagging](#), modificare quel set di tag e utilizzare questa azione API per sostituire il set di tag con quello modificato.

Note

Se invii questa richiesta con un set di tag vuoto, le operazioni in batch S3 eliminano il set di tag esistenti sull'oggetto. Se si utilizza questo metodo, viene addebitato un costo per una richiesta di livello 1 (PUT). Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per eliminare i tag esistenti per il processo Batch Operations, l'operazione `DeleteJobTagging` è da preferire perché ottiene lo stesso risultato senza incorrere in addebiti.

- [DeleteJobTagging](#) - Elimina il set di tag associato a un processo di Operazioni in batch.

Creazione di un processo Batch Operations con tag di processo utilizzati per l'etichettatura

È possibile etichettare e controllare l'accesso ai processi di Operazioni in batch Amazon S3 aggiungendo dei tag. I tag possono essere utilizzati per identificare chi è responsabile di un processo di operazioni in batch. È possibile creare lavori con tag ad essi associati e aggiungere tag ai lavori dopo la creazione. Per ulteriori informazioni, consulta [the section called "Utilizzo dei tag"](#).

Utilizzo di AWS CLI

L'AWS CLI esempio seguente crea un S3PutObjectCopy job S3 Batch Operations utilizzando i tag del job come etichette per il job.

1. Selezionare l'operazione o OPERATION da far eseguire al processo di operazioni in batch e scegliere il proprio TargetResource.

```
read -d '' OPERATION <<EOF
{
  "S3PutObjectCopy": {
    "TargetResource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  }
}
EOF
```

2. Identificare il lavoro TAGS che si desidera per il lavoro. In questo caso, si applicano due tag department e FiscalYear, con i valori Marketing e 2020 rispettivamente.

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
]
EOF
```

3. Specificare MANIFEST per il processo di operazioni in batch.

```
read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "EXAMPLE_S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
}
```

```

"Location": {
  "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/example_manifest.csv",
  "ETag": "example-5dc7a8bfb90808fc5d546218"
}
}
EOF

```

4. Configurare REPORT per il processo di operazioni in batch.

```

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Example_Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/copy-with-replace-metadata",
  "ReportScope": "AllTasks"
}
EOF

```

5. Eseguire l'operazione create-job per creare il processo di operazioni in batch con input impostati nelle fasi precedenti.

```

aws \
  s3control create-job \
    --account-id 123456789012 \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'}/" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn arn:aws:iam::123456789012:role/batch-operations-role \
    --tags "${TAGS//$'\n'}/" \
    --client-request-token "$(uuidgen)" \
    --region us-west-2 \
    --description "Copy with Replace Metadata";

```

Utilizzo di AWS SDK per Java

Per creare un processo S3 Batch Operations con tag utilizzando l' AWS SDK per Java, è possibile utilizzare il client S3Control per configurare i parametri del lavoro, tra cui la posizione del manifesto, le operazioni del lavoro, le impostazioni di reporting e i tag per scopi di organizzazione e tracciamento.

Per esempi di come creare processi S3 Batch Operations con tag utilizzando l' AWS SDK per Java, consulta [Creare un lavoro batch per copiare oggetti](#) nell'API Reference di Amazon S3.

Eliminazione dei tag da un processo S3 Batch Operations

È possibile utilizzare questi esempi per eliminare i tag da un processo di Operazioni in batch Amazon S3.

Utilizzo di AWS CLI

Nell'esempio seguente vengono eliminati i tag da un processo di operazioni in batch tramite la AWS CLI.

```
aws \
  s3control delete-job-tagging \
  --account-id 123456789012 \
  --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
  --region us-east-1
```

Eliminare i tag di processo di un processo di operazioni in batch

Per eliminare i tag di un job S3 Batch Operations utilizzando l' AWS SDK per Java, puoi utilizzare il client S3Control con l'ID del job per rimuovere tutti i tag associati al job batch operations.

Per esempi di come eliminare i tag di lavoro con l' AWS SDK per Java, consulta [Eliminare i tag da un lavoro batch](#) nell'API Reference di Amazon S3.

Aggiunta di tag di processo a un processo di Operazioni in batch esistente

È possibile utilizzare l'operazione API [PutJobTagging](#) per aggiungere tag ai processi esistenti di Operazioni in batch Amazon S3. Per maggiori informazioni, consulta i seguenti esempi.

Utilizzo di AWS CLI

Di seguito è riportato un esempio di utilizzo di `s3control put-job-tagging` per aggiungere tag al processo di Operazioni in batch S3 tramite AWS CLI. Per utilizzare gli esempi, sostituisci i caratteri *user input placeholders* con le tue informazioni.

 Note

Se si invia questa richiesta con un set di tag vuoto, Operazioni in batch elimina il set di tag esistente sull'oggetto. Tuttavia, se si utilizza questo approccio, viene addebitato un costo per una richiesta di livello 1 (PUT). Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per eliminare i tag esistenti per il processo di Operazioni in batch, si consiglia di utilizzare l'operazione `DeleteJobTagging`, che consente di ottenere lo stesso risultato senza incorrere in spese.

1. Identificare il lavoro TAGS che si desidera per il lavoro. In questo caso, si applicano due tag *department* e *FiscalYear*, con i valori *Marketing* e *2020* rispettivamente.

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
]
EOF
```

2. Esegui il seguente comando `put-job-tagging` con i parametri richiesti:

```
aws \
  s3control put-job-tagging \
  --account-id 123456789012 \
  --tags "${TAGS//'\n'/'}" \
  --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
  --region us-east-1
```

Utilizzo di AWS SDK per Java

Per inserire tag in un job S3 Batch Operations utilizzando l' AWS SDK per Java, puoi utilizzare il client `S3Control` per aggiungere o aggiornare tag con coppie chiave-valore per scopi di organizzazione e tracciamento.

Per esempi di come inserire tag di lavoro con l' AWS SDK per Java, consulta [Aggiungere tag a un lavoro](#) batch nell'API Reference di Amazon S3.

Recupero dei tag di processo di un processo S3 Batch Operations

Per recuperare i tag di un processo di Operazioni in batch Amazon S3, si può utilizzare l'operazione API `GetJobTagging`. Per maggiori informazioni, consulta i seguenti esempi.

Utilizzo di AWS CLI

Nell'esempio seguente vengono recuperati i tag da un processo di operazioni in batch tramite la AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws \
  s3control get-job-tagging \
  --account-id 123456789012 \
  --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
  --region us-east-1
```

Utilizzo di AWS SDK per Java

Per ottenere i tag di un job S3 Batch Operations utilizzando l' AWS SDK per Java, puoi utilizzare il client `S3Control` con l'ID del job per recuperare tutti i tag associati al job di operazioni batch e restituirli come elenco.

Per esempi su come ottenere i tag di lavoro con l' AWS SDK per Java, consulta [Ottenere tag da un lavoro batch](#) nell'API Reference di Amazon S3.

Controllo delle autorizzazioni per le operazioni in batch utilizzando i tag di processo

Per facilitare la gestione dei processi di Operazioni in batch Amazon S3, è possibile aggiungere tag di processo. Con i tag di processo, è possibile controllare l'accesso ai processi di operazioni in batch e imporre che i tag vengano applicati quando viene creato un processo.

È possibile applicare fino a 50 tag di processo a ciascun processo di operazioni in batch. Utilizzando i tag, è possibile impostare policy granulari per limitare l'insieme degli utenti che possono modificare il processo. I tag di lavoro possono favorire o limitare la capacità di un utente di annullare un lavoro, attivare un lavoro in stato di conferma o cambiare il livello di priorità di un lavoro. Inoltre, è possibile applicare i tag a tutti i nuovi lavori e specificare le coppie chiave-valore consentite per i tag. È possibile esprimere tutte queste condizioni utilizzando il [linguaggio delle policy AWS Identity and](#)

[Access Management \(IAM\)](#). Per ulteriori informazioni, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Nell'esempio seguente viene illustrato come utilizzare i tag di processo di operazioni in batch S3 per concedere agli utenti l'autorizzazione per la creazione e la modifica solo dei processi eseguiti all'interno di un reparto specifico (ad esempio, il reparto Finanza o Conformità). È inoltre possibile assegnare i lavori in base allo stadio di sviluppo a cui sono correlati, ad esempio QA o Produzione.

In questo esempio, si utilizzano i tag dei processi di Operazioni in batch S3 nelle policy IAM per concedere agli utenti l'autorizzazione a creare e modificare solo i processi eseguiti nel loro reparto. Assegnare i lavori in base alla fase di sviluppo a cui sono correlati, ad esempio QA o Produzione.

Gli esempi che seguono utilizzano i seguenti reparti, ognuno dei quali utilizza Operazioni in batch in modo diverso:

- Finanza
- Conformità
- Business Intelligence
- Engineering (Progettazione)

Argomenti

- [Controllo degli accessi mediante l'assegnazione di tag a utenti e risorse](#)
- [Tagging dei processi di operazioni in batch per fase e applicazione dei limiti sulla priorità del processo](#)

Controllo degli accessi mediante l'assegnazione di tag a utenti e risorse

In questo scenario, gli amministratori utilizzano il [controllo di accesso basato su attributi \(ABAC\)](#). ABAC è una strategia di autorizzazione IAM che definisce le autorizzazioni allegando tag sia agli utenti che alle risorse. AWS

Agli utenti e ai lavori viene assegnato uno dei seguenti tag reparto:

Chiave: Valore)

- department : Finance

- department : Compliance
- department : BusinessIntelligence
- department : Engineering

 Note

I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole.

Utilizzando la strategia di controllo degli accessi ABAC, concedi a un utente del reparto Finanza l'autorizzazione per la creazione e la gestione dei processi di operazioni in batch Amazon S3 all'interno del proprio reparto associando il tag department=Finance al relativo utente.

Inoltre, è possibile collegare una policy gestita all'utente IAM che consente a qualsiasi utente della propria azienda di creare o modificare processi di operazioni in batch Amazon S3 all'interno dei rispettivi reparti.

La policy riportata in questo esempio include tre dichiarazioni di policy:

- La prima istruzione della policy consente all'utente di creare un processo di operazioni in batch a condizione che la richiesta di creazione del processo includa un tag di processo corrispondente al rispettivo reparto. Si esprime utilizzando la sintassi "\${aws:PrincipalTag/department}", che viene sostituita dal tag reparto dell'utente al momento della valutazione delle policy. La condizione è soddisfatta quando il valore fornito per il tag reparto nella richiesta ("aws:RequestTag/department") corrisponde al reparto dell'utente.
- La seconda istruzione della policy consente agli utenti di modificare la priorità dei lavori o di aggiornare lo stato di un lavoro a condizione che il lavoro che l'utente sta aggiornando corrisponda al reparto dell'utente.
- La terza istruzione consente a un utente di aggiornare i tag di un job di Batch Operations in qualsiasi momento tramite una PutJobTagging richiesta, a condizione che (1) il tag di reparto venga preservato e (2) il lavoro che sta aggiornando sia all'interno del proprio reparto.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  

```

```

        {
            "Effect": "Allow",
            "Action": "s3:CreateJob",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                }
            },
            {
                "Effect": "Allow",
                "Action": [
                    "s3:UpdateJobPriority",
                    "s3:UpdateJobStatus"
                ],
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                    }
                },
                {
                    "Effect": "Allow",
                    "Action": "s3:PutJobTagging",
                    "Resource": "*",
                    "Condition": {
                        "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                        }
                    }
                }
            }
        ]
    }

```

Tagging dei processi di operazioni in batch per fase e applicazione dei limiti sulla priorità del processo

Tutti i processi di operazioni in batch Amazon S3 hanno una priorità numerica, che Amazon S3 utilizza per decidere in quale ordine eseguire i processi. In questo esempio, si limita la priorità massima che la maggior parte degli utenti può assegnare ai lavori, con intervalli di priorità più elevati riservati a un gruppo limitato di utenti con privilegi, come segue:

- Intervallo di priorità dello stadio QA (basso): 1-100
- Intervallo di priorità della fase di produzione (alto): 1-300

Per fare ciò, introdurre un nuovo set di tag che rappresenta la fase del lavoro:

Chiave: Valore)

- stage : QA
- stage : Production

Creazione e aggiornamento di lavori con priorità bassa all'interno di un reparto

Questa policy introduce due nuove restrizioni per la creazione e l'aggiornamento di processi di operazioni in batch S3, oltre alla restrizione basata sul reparto:

- Consente agli utenti di creare o aggiornare lavori nel proprio reparto con una nuova condizione che richiede che il lavoro includa il tag `stage=QA`.
- Consente agli utenti di creare o aggiornare la priorità di un lavoro fino a una nuova priorità massima di 100.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:CreateJob",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/department": "${aws:PrincipalTag/department}",
          "aws:RequestTag/stage": "QA"
        }
      }
    }
  ],
}
```

```

        "NumericLessThanEquals": {
            "s3:RequestJobPriority": 100
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:UpdateJobStatus"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:UpdateJobPriority",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:ResourceTag/stage": "QA"
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:PutJobTagging",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/department" : "${aws:PrincipalTag/department}",
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA",
                "aws:ResourceTag/stage": "QA"
            }
        }
    }
},

```

```
{
  "Effect": "Allow",
  "Action": "s3:GetJobTagging",
  "Resource": "*"
}
```

Creazione e aggiornamento di lavori ad alta priorità all'interno di un reparto

Un numero ristretto di utenti potrebbe richiedere la possibilità di creare lavori con priorità elevata in QA o Produzione. Per supportare questa esigenza, è possibile creare una policy gestita adattata alla policy con priorità bassa nella sezione precedente.

Questa policy esegue le seguenti operazioni:

- Consente agli utenti di creare o aggiornare lavori nel proprio reparto con il tag `stage=QA` o `stage=Production`.
- Consente agli utenti di creare o aggiornare la priorità di un lavoro fino a un massimo di 300.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:CreateJob",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:RequestTag/stage": [
            "QA",
            "Production"
          ]
        },
        "StringEquals": {
          "aws:RequestTag/department": "${aws:PrincipalTag/department}"
        },
        "NumericLessThanEquals": {
```

```

        "s3:RequestJobPriority": 300
    }
}
},
{
    "Effect": "Allow",
    "Action": [
        "s3:UpdateJobStatus"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
        }
    }
},
{
    "Effect": "Allow",
    "Action": "s3:UpdateJobPriority",
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:ResourceTag/stage": [
                "QA",
                "Production"
            ]
        },
        "StringEquals": {
            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
        },
        "NumericLessThanEquals": {
            "s3:RequestJobPriority": 300
        }
    }
},
{
    "Effect": "Allow",
    "Action": "s3:PutJobTagging",
    "Resource": "*",
    "Condition": {
        "StringEquals": {

```

```

        "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
        "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
    },
    "ForAnyValue:StringEquals": {
        "aws:RequestTag/stage": [
            "QA",
            "Production"
        ],
        "aws:ResourceTag/stage": [
            "QA",
            "Production"
        ]
    }
}

```

Gestione del blocco oggetti S3 utilizzando S3 Batch Operations

È possibile utilizzare Operazioni in batch S3 per eseguire operazioni in batch su larga scala su oggetti Amazon S3. Le operazioni in batch S3 possono eseguire una singola operazione su elenchi di oggetti Amazon S3 specificati. Un solo processo può eseguire l'operazione specificata su miliardi di oggetti contenenti exabyte di dati. Amazon S3 tiene traccia dei progressi, invia notifiche e archivia un report dettagliato sul completamento di tutte le azioni, offrendo un'esperienza completamente gestita, verificabile e serverless. Puoi utilizzare S3 Batch Operations tramite la console Amazon S3 AWS CLI, gli AWS SDK o l'API REST di Amazon S3.

Con il blocco oggetti S3 è possibile inserire anche un blocco di carattere legale sulla versione di un oggetto. Analogamente all'impostazione di un periodo di conservazione, un blocco a di carattere legale impedisce che una versione di un oggetto venga sovrascritta o eliminata. Tuttavia, un blocco legale non ha un periodo di conservazione associato e rimane in vigore fino a quando non viene rimosso. Per ulteriori informazioni, consulta [Blocco di carattere legale del blocco oggetti S3](#).

Per utilizzare Operazioni in batch S3 con Object Lock per aggiungere le blocchi legali a molti oggetti Amazon S3 in una sola volta, consulta i seguenti argomenti.

Argomenti

- [Abilitazione del blocco oggetti S3 utilizzando S3 Batch Operations](#)
- [Impostazione della conservazione del blocco oggetti mediante Batch Operations](#)
- [Utilizzo delle operazioni in batch S3 con la modalità di conformità della conservazione del blocco oggetti S3](#)
- [Utilizzare le operazioni in batch S3 con la modalità di governance della conservazione del blocco oggetti S3](#)
- [Utilizzo di Operazioni in batch S3 per disattivare i blocchi legali di S3 Object Lock](#)

Abilitazione del blocco oggetti S3 utilizzando S3 Batch Operations

È possibile utilizzare Operazioni in batch Amazon S3 con S3 Object Lock per gestire la conservazione o attivare un blocco legale per molti oggetti Amazon S3 contemporaneamente. Si specifica l'elenco degli oggetti di destinazione nel manifesto e lo si invia a Operazioni in batch per il completamento. Per ulteriori informazioni, consulta [the section called “Conservazione Blocco oggetto”](#) e [the section called “Blocco di carattere legale del blocco oggetto”](#).

Gli esempi seguenti mostrano come creare un ruolo AWS Identity and Access Management (IAM) con le autorizzazioni S3 Batch Operations e aggiornare le autorizzazioni del ruolo per creare job che abilitino Object Lock. È inoltre necessario disporre di un manifesto CSV che identifichi gli oggetti per il processo Operazioni in batch S3. Per ulteriori informazioni, consulta [the section called “Specifica di un manifesto”](#).

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Utilizzo di AWS CLI

1. Creare un ruolo IAM e assegnare autorizzazioni delle operazioni in batch S3 per l'esecuzione.

Questa fase è necessaria per tutti i processi di operazioni in batch S3.

```
export AWS_PROFILE='aws-user'

read -d '' batch_operations_trust_policy <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```



```

        "Service": [
            "batchoperations.s3.amazonaws.com"
        ],
        "Action": "sts:AssumeRole"
    }
]
}
EOF
aws iam create-role --role-name batch_operations-objectlock \
--assume-role-policy-document "${batch_operations_trust_policy}"

```

2. Configurare le operazioni in batch S3 con il blocco oggetti S3 per l'esecuzione.

In questa fase è possibile consentire al ruolo di eseguire le operazioni seguenti:

- Eseguire Object Lock sul bucket S3 che contiene gli oggetti di destinazione su cui eseguire Operazioni in batch.
- Leggere il bucket S3 in cui si trovano il file manifesto CSV e gli oggetti.
- Scrivi i risultati del processo di Operazioni in batch S3 nel bucket di reporting.

```

read -d '' batch_operations_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
            ]
        }
    ]
}
EOF

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::{amzn-s3-demo-completion-report-bucket}/*"
      ]
    }
  ]
}
EOF

aws iam put-role-policy --role-name batch_operations-objectlock \
--policy-name object-lock-permissions \
--policy-document "${batch_operations_permissions}"

```

Utilizzo di AWS SDK per Java

È possibile creare un ruolo IAM con le autorizzazioni per Operazioni in batch S3 e aggiornare le autorizzazioni del ruolo per creare processi che abilitano Object Lock tramite AWS SDK per Java. È inoltre necessario disporre di un manifest CSV che identifichi gli oggetti per il processo di operazioni in batch S3. Per ulteriori informazioni, consulta [the section called “Specifica di un manifest”](#).

Esegui queste fasi:

1. Creare un ruolo IAM e assegnare autorizzazioni delle operazioni in batch S3 per l'esecuzione. Questa fase è necessaria per tutti i processi di operazioni in batch S3.
2. Configurare Operazioni in batch S3 con S3 Object Lock per l'esecuzione.

Consenti al ruolo di eseguire le seguenti operazioni:

1. Eseguire il blocco oggetti sul bucket S3 che contiene gli oggetti di destinazione su cui eseguire le operazioni in batch.
2. Leggere il bucket S3 in cui si trovano il file manifesto CSV e gli oggetti.
3. Scrivi i risultati del processo di Operazioni in batch S3 nel bucket di reporting.

Per un esempio di codice che dimostri come creare un ruolo IAM per abilitare S3 Object Lock utilizzando S3 Batch Operations con l' AWS SDK per Java, consulta gli esempi di codice dell'SDK per Java [CreateObjectLockRole.java](#) 2.x. AWS

Impostazione della conservazione del blocco oggetti mediante Batch Operations

È possibile utilizzare Operazioni in batch Amazon S3 con S3 Object Lock per gestire la conservazione di più oggetti Amazon S3 contemporaneamente. Si specifica l'elenco degli oggetti di destinazione nel manifesto e lo si invia a Operazioni in batch per il completamento. Per ulteriori informazioni, consulta [the section called “Conservazione Blocco oggetto”](#) e [the section called “Blocco di carattere legale del blocco oggetto”](#).

Gli esempi seguenti mostrano come creare un ruolo AWS Identity and Access Management (IAM) con le autorizzazioni S3 Batch Operations e aggiornare le autorizzazioni del ruolo per includere le autorizzazioni in modo da poter eseguire la conservazione di S3 `s3:PutObjectRetention` Object Lock sugli oggetti nel bucket manifest. È inoltre necessario disporre di un manifesto CSV che identifichi gli oggetti per il processo Operazioni in batch S3. Per ulteriori informazioni, consulta [the section called “Specifica di un manifest”](#).

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Utilizzo di AWS CLI

L' AWS CLI esempio seguente mostra come utilizzare Batch Operations per applicare la conservazione di S3 Object Lock su più oggetti.

```
export AWS_PROFILE='aws-user'

read -d '' retention_permissions <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectRetention"
      ],
      "Resource": [
        "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
      ]
    }
  ]
}
```

```
}  
EOF  
  
aws iam put-role-policy --role-name batch_operations-objectlock --policy-  
name retention-permissions --policy-document "${retention_permissions}"
```

Utilizzo di AWS SDK per Java

Per esempi di come utilizzare Batch Operations per applicare la conservazione di S3 Object Lock su più oggetti con l' AWS SDK per Java, consulta [Use CreateJob with an AWS SDK o CLI](#) in Amazon S3 API Reference.

Utilizzo delle operazioni in batch S3 con la modalità di conformità della conservazione del blocco oggetti S3

L'esempio seguente si basa sugli esempi precedenti di creazione di una policy di attendibilità e sull'impostazione delle autorizzazioni di configurazione di S3 Batch Operations e del blocco oggetti S3 per gli oggetti. Questo esempio imposta la modalità di conservazione su COMPLIANCE e `retain` until date il 1° gennaio 2025. Questo esempio crea un processo che ha come target gli oggetti del bucket manifesto e riporta i risultati nel bucket del report identificato.

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Utilizzo di AWS CLI

AWS CLI Gli esempi seguenti mostrano come utilizzare Batch Operations per applicare la modalità di conformità alla conservazione di S3 Object Lock su più oggetti.

Example- Impostazione della modalità di conformità di conservazione S3 Object Lock per più oggetti

```
export AWS_PROFILE=aws-user  
export AWS_DEFAULT_REGION=us-west-2  
export ACCOUNT_ID=123456789012  
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'  
  
read -d '' OPERATION <<EOF  
{  
  "S3PutObjectRetention": {  
    "Retention": {  
      "RetainUntilDate": "2025-01-01T00:00:00",  
      "Mode": "COMPLIANCE"  
    }  
  }  
}
```

```

    }
  }
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::ReportBucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "amzn-s3-demo-completion-report-bucket/compliance-objects-batch-operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
  s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/'}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Set compliance retain-until to 1 Jul 2030";

```

Example— Estendere la data di conservazione della modalità COMPLIANCE fino al 15 gennaio 2025

L'esempio seguente estende la COMPLIANCE della modalità retain until date al 15 gennaio 2025.

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate": "2025-01-15T00:00:00",
      "Mode": "COMPLIANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/compliance-objects-batch_operations",
}
```

```
"ReportScope": "AllTasks"
}
EOF

aws \
  s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/'}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Extend compliance retention to 15 Jan 2025";
```

Utilizzo di AWS SDK per Java

I seguenti esempi di AWS SDK per Java mostrano come utilizzare Batch Operations per applicare la modalità di conservazione S3 Object Lock su più oggetti, inclusa l'impostazione della modalità di conservazione su COMPLIANCE con una conservazione fino alla data e l'estensione della modalità COMPLIANCE di conservazione fino alla data.

Per esempi di come utilizzare Batch Operations per applicare la modalità di conformità alla conservazione di S3 Object Lock su più oggetti con l' AWS SDK per Java, consulta [Use CreateJob with an AWS SDK o CLI](#) in Amazon S3 API Reference.

Utilizzare le operazioni in batch S3 con la modalità di governance della conservazione del blocco oggetti S3

L'esempio seguente si basa sull'esempio precedente di creazione di una policy di attendibilità e sull'impostazione delle autorizzazioni di configurazione di Operazioni in batch S3 e S3 Object Lock. Questo esempio mostra come applicare la governance di conservazione S3 Object Lock con `retain until` date il 30 gennaio 2025, su più oggetti. Crea un processo di operazioni in batch che utilizza il bucket manifest e notifica i risultati nel bucket dei report.

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Utilizzo di AWS CLI

AWS CLI Gli esempi seguenti mostrano come utilizzare Batch Operations per applicare la modalità di governance di conservazione di S3 Object Lock su più oggetti.

Example- Applicazione della governance di conservazione S3 Object Lock a più oggetti con la data di conservazione fino al 30 gennaio 2025

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate": "2025-01-30T00:00:00",
      "Mode": "GOVERNANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucketT",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/governance-objects",
  "ReportScope": "AllTasks"
```



```

}
EOF

aws \
  s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/'}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Put governance retention";

```

Example- Bypass della governance di conservazione su più oggetti

L'esempio seguente si basa sull'esempio precedente di creazione di una policy di attendibilità e sull'impostazione delle autorizzazioni di configurazione di Operazioni in batch S3 e S3 Object Lock. Viene illustrato come ignorare la governance della conservazione tra più oggetti e creare un processo di operazioni in batch che utilizza il bucket manifest e notifica i risultati nel bucket dei report.

```

export AWS_PROFILE='aws-user'

read -d '' bypass_governance_permissions <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:BypassGovernanceRetention"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
EOF

aws iam put-role-policy --role-name batch-operations-objectlock --policy-name bypass-
governance-permissions --policy-document "${bypass_governance_permissions}"

```

```

export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "BypassGovernanceRetention": true,
    "Retention": {
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/batch_operations-governance",
  "ReportScope": "AllTasks"
}
EOF

aws \

```

```
s3control create-job \  
--account-id "${ACCOUNT_ID}" \  
--manifest "${MANIFEST//$'\n'}" \  
--operation "${OPERATION//$'\n'/'}" \  
--report "${REPORT//$'\n'}" \  
--priority 10 \  
--role-arn "${ROLE_ARN}" \  
--client-request-token "$(uuidgen)" \  
--region "${AWS_DEFAULT_REGION}" \  
--description "Remove governance retention";
```

Utilizzo di AWS SDK per Java

I seguenti esempi di AWS SDK per Java mostrano come applicare la governance di conservazione di S3 Object Lock `retain until date` impostata al 30 gennaio 2025 su più oggetti, inclusa l'applicazione della governance di conservazione Object Lock su più oggetti con una data di conservazione fino alla data e bypassando la governance di conservazione su più oggetti.

Per esempi di come utilizzare Batch Operations con la modalità di governance della conservazione S3 Object Lock con l' AWS SDK per Java, consulta [Use CreateJob with an AWS SDK o CLI](#) nell'Amazon S3 API Reference.

Utilizzo di Operazioni in batch S3 per disattivare i blocchi legali di S3 Object Lock

L'esempio seguente si basa sugli esempi precedenti di creazione di una policy di attendibilità e sull'impostazione delle autorizzazioni di configurazione di operazioni in batch S3 e del blocco oggetti S3. Questo esempio mostra come disattivare il blocco legale Object Lock degli oggetti utilizzando Operazioni in batch.

Nell'esempio viene innanzitutto aggiornato il ruolo per concedere le autorizzazioni `s3:PutObjectLegalHold`, viene creato un processo di operazioni in batch che disattiva (rimuove) il blocco di carattere legale dagli oggetti identificati nel manifest, quindi viene inviata una segnalazione.

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Utilizzo di AWS CLI

AWS CLI Gli esempi seguenti mostrano come utilizzare Batch Operations per disattivare i blocchi legali di S3 Object Lock su più oggetti.

Example— Aggiorna il ruolo per concedere le autorizzazioni s3: PutObjectLegalHold

```
export AWS_PROFILE='aws-user'

read -d '' legal_hold_permissions <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectLegalHold"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}

EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-name legal-
hold-permissions --policy-document "${legal_hold_permissions}"
```

Example- Disattivazione del blocco legale

Nell'esempio seguente viene disattivato il blocco di carattere legale.

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectLegalHold": {
    "LegalHold": {
      "Status":"OFF"
    }
  }
}
EOF
```

```

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/legalhold-object-manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/legalhold-objects-batch_operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
  s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/'}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Turn off legal hold";

```

Utilizzo di AWS SDK per Java

Per esempi di come utilizzare S3 Batch Operations per disattivare il blocco legale di S3 Object Lock con l' AWS SDK per Java, consulta [Utilizzo CreateJob con un AWS SDK o una CLI](#) nell'API Reference di Amazon S3.

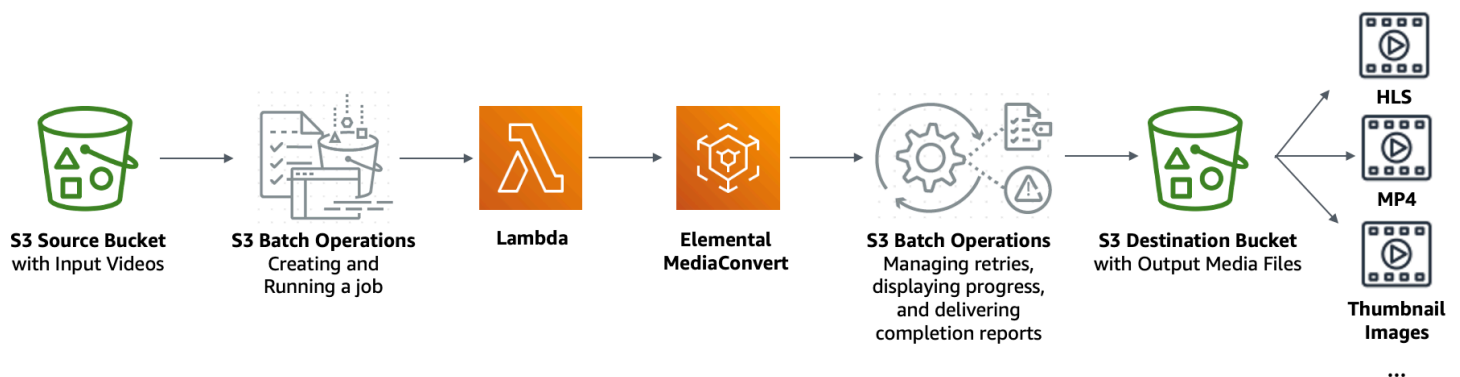
Tutorial: video con S3 Batch Operations Batch-transcoding

I consumatori di video utilizzano dispositivi di tutte le forme, dimensioni ed età per godere dei contenuti multimediali. Questa vasta gamma di dispositivi rappresenta una sfida per i creatori e i distributori di contenuti. I video non possono avere un formato unico, ma devono coprire un'ampia gamma di dimensioni, formati e velocità di trasmissione. Questa operazione di conversione è ancora più difficile quando si dispone di un numero elevato di video che devono essere convertiti.

AWS offre un metodo per creare un'architettura scalabile e distribuita che esegue le seguenti operazioni:

- Importa video di input
- Elabora i video per la riproduzione su un'ampia gamma di dispositivi
- Memorizza i file multimediali transcodificati
- Fornisce i file multimediali di output per soddisfare la domanda

Quando hai repository video di grandi dimensioni archiviati in Amazon S3, puoi transcodificare questi video dal loro formato di origine in più tipi di file nelle dimensioni, nella risoluzione o nel formato necessario per un determinato lettore video o dispositivo. In particolare, [S3 Batch Operations](#) fornisce una soluzione per richiamare AWS Lambda funzioni per i video di input esistenti in un bucket sorgente S3. Quindi, le funzioni Lambda richiamano [AWS Elemental MediaConvert](#) perché esegua processi di transcodifica di video su larga scala. I file multimediali di output convertiti sono archiviati in un bucket di destinazione S3.



Obiettivo

In questa esercitazione imparerai a impostare le operazioni in batch S3 per richiamare una funzione Lambda per la transcodificazione in batch di video memorizzati in un bucket S3 di origine. La funzione Lambda chiama MediaConvert per transcodificare i video. Gli output per ogni video nel bucket S3 di origine hanno le caratteristiche mostrate di seguito:

- Un flusso di bitrate adattivo [HTTP Live Streaming \(HLS\)](#) per la riproduzione su dispositivi di dimensioni multiple e con larghezza di banda variabile.
- Un file video MP4
- Immagini in miniatura raccolte a intervalli

Argomenti

- [Prerequisiti](#)
- [Fase 1: Creazione di un bucket S3 per i file multimediali di output](#)
- [Passaggio 2: creare un ruolo IAM per MediaConvert](#)
- [Fase 3: creazione di un ruolo IAM per la funzione Lambda](#)
- [Fase 4: Creazione di una funzione Lambda per la transcodifica dei video](#)
- [Fase 5: Configurazione dell'inventario Amazon S3 per il bucket S3 di origine](#)
- [Fase 6: creazione di un ruolo IAM per le operazioni in batch S3](#)
- [Fase 7: creazione ed esecuzione di un processo di operazioni in batch S3](#)
- [Fase 8: Controllo dei file multimediali di output dal bucket S3 di destinazione](#)
- [Fase 9: Pulizia](#)
- [Fasi successive](#)

Prerequisiti

Prima di iniziare questo tutorial, devi disporre di un bucket Amazon S3 di origine (ad esempio, *amzn-s3-demo-source-bucket*) dove siano già archiviati video da transcodificare.

Se lo desideri, puoi assegnare al bucket un altro nome. Per ulteriori informazioni sulle regole di denominazione dei bucket in Amazon S3, consulta [Regole di denominazione dei bucket per uso generico](#).

Per il bucket S3 di origine, mantieni le impostazioni relative a Impostazioni di blocco dell'accesso pubblico per questo bucket sui valori di default (l'opzione Blocca tutto l'accesso pubblico è abilitata). Per ulteriori informazioni, consulta [Creazione di un bucket per uso generico](#).

Per ulteriori informazioni sul caricamento di video nel bucket S3 di origine, consulta [Caricamento degli oggetti](#). Quando carichi un video in S3, puoi anche possibile utilizzare [Amazon S3 Transfer Acceleration](#) per configurare trasferimenti di file veloci e sicuri. Transfer Acceleration può velocizzare il caricamento dei video nel bucket S3 per il trasferimento a lunga distanza di video di grandi dimensioni. Per ulteriori informazioni, consulta [Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#).

Fase 1: Creazione di un bucket S3 per i file multimediali di output

In questa fase, viene creato un bucket S3 di destinazione per archiviare i file multimediali di output convertiti. Puoi inoltre creare una configurazione per l'abilitazione della condivisione di risorse multiorigine (CORS, Cross Origin Resource Sharing) per permettere l'accesso tra origini ai file multimediali transcodificati archiviati nel bucket S3 di destinazione.

Fasi secondarie

- [Creazione di un bucket per i file multimediali di output](#)
- [Aggiunta di una configurazione CORS a un bucket S3 di output](#)

Creazione di un bucket per i file multimediali di output

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Seleziona Crea bucket.
4. Per Nome bucket, specifica un nome per il bucket, ad esempio *amzn-s3-demo-destination-bucket1*.
5. Per la regione, scegli Regione AWS dove vuoi che risieda il bucket.
6. Per garantire l'accesso pubblico ai file multimediali di output, in Block Public Access settings for this bucket (Impostazioni di blocco dell'accesso pubblico per questo bucket), deseleziona Block all public access (Blocca tutto l'accesso pubblico).

 Warning

Prima di completare questa fase, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#) per confermare di avere compreso e accettato i rischi connessi alla concessione di un accesso pubblico. Quando si disattivano le impostazioni di blocco dell'accesso pubblico per rendere pubblico il bucket, chiunque su Internet può accedere al bucket. Consigliamo di bloccare tutti gli accessi pubblici ai bucket.

Se non desideri cancellare le impostazioni di Blocca accesso pubblico, puoi utilizzare Amazon CloudFront per distribuire i file multimediali transcodificati agli spettatori (utenti finali). Per ulteriori informazioni, consulta [Tutorial: Hosting di video in streaming su richiesta con Amazon S3 CloudFront, Amazon e Amazon Route 53](#).

7. Seleziona la casella di controllo accanto a I acknowledge that the current settings might result in this bucket and the objects within becoming public. (Riconosco che le impostazioni correnti possono portare il bucket e gli oggetti all'interno a diventare pubblici).
8. Mantieni le impostazioni rimanenti impostate sui valori predefiniti.
9. Seleziona Crea bucket.

Aggiunta di una configurazione CORS a un bucket S3 di output

Una configurazione JSON CORS definisce un metodo con cui le applicazioni Web client (lettori video in questo contesto) caricate in un dominio possono riprodurre file multimediali di output transcodificati in un dominio differente.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il nome del bucket creato in precedenza (ad esempio, *amzn-s3-demo-destination-bucket1*).
4. Scegli la scheda Autorizzazioni.
5. Nella sezione Condivisione Cross-origin delle risorse (CORS), scegli Modifica.
6. Nella casella di testo della configurazione CORS, copia e incolla la nuova configurazione CORS mostrata di seguito.

La configurazione CORS deve essere in formato JSON. In questo esempio, l'attributo `AllowedOrigins` utilizza il carattere jolly (*) per specificare tutte le origini. Se conosci la tua origine specifica, puoi limitare l'attributo `AllowedOrigins` all'URL del lettore specifico. Per ulteriori informazioni sulla configurazione di questo e altri attributi, consulta [Elementi di una configurazione CORS](#).

```
[
  {
    "AllowedOrigins": [
      "*"
    ],
    "AllowedMethods": [
      "GET"
    ],
    "AllowedHeaders": [
      "*"
    ],
    "ExposeHeaders": []
  }
]
```

7. Scegli **Save changes** (Salva modifiche).

Passaggio 2: creare un ruolo IAM per MediaConvert

AWS Elemental MediaConvert Per utilizzarlo per transcodificare i video di input archiviati nel bucket S3, devi disporre di un ruolo di servizio AWS Identity and Access Management (IAM) per concedere MediaConvert le autorizzazioni di lettura e scrittura di file video da e verso i bucket di origine e destinazione S3. Quando esegui processi di transcodifica, la console utilizza questo ruolo. MediaConvert

Per creare un ruolo IAM per MediaConvert

1. Crea un ruolo IAM scegliendo un nome di ruolo (ad esempio, **tutorial-mediaconvert-role**). Per creare questo ruolo, segui i passaggi descritti in [Crea il tuo MediaConvert ruolo in IAM \(console\)](#) nella Guida per l'AWS Elemental MediaConvert utente.
2. Dopo aver creato il ruolo IAM per MediaConvert, nell'elenco dei ruoli, scegli il nome del ruolo per MediaConvert il quale hai creato (ad esempio, **tutorial-mediaconvert-role**).

3. Nella pagina Riepilogo, copia l'ARN ruolo (che inizia con `arn:aws:iam::`) e salva l'ARN per utilizzarlo in un secondo momento.

Per ulteriori informazioni sull'utilizzo degli ARN, consulta il [nome della risorsa Amazon \(ARN\)](#) in Riferimenti generali di AWS .

Fase 3: creazione di un ruolo IAM per la funzione Lambda

Per transcodificare in batch i video con MediaConvert S3 Batch Operations, usi una funzione Lambda per connettere questi due servizi per convertire i video. Questa funzione Lambda deve avere un ruolo IAM che conceda alla funzione Lambda le autorizzazioni di accesso a S3 Batch Operations e MediaConvert.

Fasi secondarie

- [Creazione di un ruolo IAM per la funzione Lambda](#)
- [Incorporazione di una policy inline per il ruolo IAM della funzione Lambda](#)

Creazione di un ruolo IAM per la funzione Lambda

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>
2. Nel pannello di navigazione a sinistra, scegli Ruoli, quindi Crea ruolo.
3. Scegli il tipo di ruolo Servizio AWS dopodiché in Casi d'uso comuni scegli Lambda.
4. Scegli Successivo: autorizzazioni.
5. Sulla pagina Collega policy di autorizzazioni, immetti **AWSLambdaBasicExecutionRole** nella casella Filtra policy. Per allegare la policy gestita **AWSLambdaBasicExecutionRole** a questo ruolo per concedere autorizzazioni di scrittura ad Amazon CloudWatch Logs, seleziona la casella di controllo accanto a **AWSLambdaBasicExecutionRole**.
6. Scegli Avanti.
7. Per Nome ruolo, inserisci **tutorial-lambda-transcode-role**.
8. (Facoltativo) Aggiungi i tag alla policy gestita.
9. Scegliere Crea ruolo.

Incorporazione di una policy inline per il ruolo IAM della funzione Lambda

Per concedere le autorizzazioni alla MediaConvert risorsa necessaria per l'esecuzione della funzione Lambda, devi utilizzare una policy in linea.

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>
2. Nel pannello di navigazione a sinistra, seleziona Ruoli.
3. Nell'elenco Ruoli scegli il nome del ruolo IAM creato in precedenza per la funzione Lambda (ad esempio, **tutorial-lambda-transcode-role**).
4. Scegliere la scheda Permissions (Autorizzazioni).
5. Scegliere Add inline policy (Aggiungi policy inline).
6. Scegli la scheda JSON e copia e incolla la seguente policy JSON.

Nella policy JSON, sostituisci il valore ARN di esempio Resource con il ruolo ARN del ruolo IAM per MediaConvert quello che hai creato nel [passaggio 2](#) (ad esempio,). **tutorial-mediaconvert-role**

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "Logging"
    },
    {
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/tutorial-mediaconvert-role"
      ]
    }
  ]
}
```

```

    ],
    "Effect": "Allow",
    "Sid": "PassRole"
  },
  {
    "Action": [
      "mediaconvert:*"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow",
    "Sid": "MediaConvertService"
  },
  {
    "Action": [
      "s3:*"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow",
    "Sid": "S3Service"
  }
]
}

```

7. Scegli Esamina la policy.
8. In Nome, inserisci **tutorial-lambda-policy**.
9. Scegli Crea policy.

Una volta creata, la policy inline viene automaticamente incorporata nel ruolo IAM della funzione Lambda.

Fase 4: Creazione di una funzione Lambda per la transcodifica dei video

In questa sezione del tutorial, crei una funzione Lambda usando l'SDK per Python da integrare con S3 Batch Operations e MediaConvert. Per iniziare a transcodificare i video già archiviati nel bucket S3 di origine, esegui un processo di operazioni in batch S3 che richiama direttamente la funzione Lambda per ogni video nel bucket S3 di origine. Quindi, la funzione Lambda invia un processo di transcodifica per ogni video a MediaConvert.

Fasi secondarie

- [Scrittura del codice della funzione Lambda e creazione di un pacchetto di implementazione](#)
- [Creare una funzione Lambda con un ruolo di esecuzione \(console\)](#)
- [Implementa la tua funzione Lambda con gli archivi in file .zip e configura la funzione Lambda \(console\)](#)

Scrittura del codice della funzione Lambda e creazione di un pacchetto di implementazione

1. Nel computer locale, crea un cartella denominata `batch-transcode`.
2. Nella cartella `batch-transcode`, crea un file con le impostazioni del processo JSON. Ad esempio, è possibile utilizzare le impostazioni fornite in questa sezione e denominare il file `job.json`.

Un file `job.json` specifica le seguenti informazioni:

- Quali file transcodificare
- Come transcodificare i tuoi video di input
- Quali file multimediali di output si desidera creare
- Come denominare i file transcodificati
- Dove salvare i file transcodificati
- Le funzioni avanzate da applicare e così via.

In questo tutorial utilizziamo il seguente file `job.json` per creare i seguenti output per ogni video del bucket S3 di origine:

- Un flusso di bitrate adattivo HTTP Live Streaming (HLS) per la riproduzione su dispositivi di dimensioni differenti e con larghezza di banda variabile.
- Un file video MP4
- Immagini in miniatura raccolte a intervalli

Questo `job.json` file di esempio utilizza il bitrate Quality-Defined variabile (QVBR) per ottimizzare la qualità video. L'uscita HLS è Apple-compliant (audio non mixato dal video, durata del segmento di 6 secondi e qualità video ottimizzata tramite QVBR automatico).

Se non si desidera utilizzare le impostazioni di esempio fornite qui, è possibile generare una specifica `job.json` basata sul proprio caso d'uso. Per garantire la coerenza tra gli output, assicurati che i file di input abbiano configurazioni video e audio simili. Per tutti i file di input con configurazioni video e audio diverse, è consigliabile creare automazioni separate (impostazioni `job.json` univoche). Per ulteriori informazioni, consulta [Example AWS Elemental MediaConvert job settings in JSON](#) nella Guida per l'utente di AWS Elemental MediaConvert.

```
{
  "OutputGroups": [
    {
      "CustomName": "HLS",
      "Name": "Apple HLS",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
              ]
            }
          },
          "VideoDescription": {
```

```
"Width": 640,
"ScalingBehavior": "DEFAULT",
"Height": 360,
"TimecodeInsertion": "DISABLED",
"AntiAlias": "ENABLED",
"Sharpness": 50,
"CodecSettings": {
  "Codec": "H_264",
  "H264Settings": {
    "InterlaceMode": "PROGRESSIVE",
    "NumberReferenceFrames": 3,
    "Syntax": "DEFAULT",
    "Softness": 0,
    "GopClosedCadence": 1,
    "GopSize": 2,
    "Slices": 1,
    "GopBReference": "DISABLED",
    "MaxBitrate": 1200000,
    "SlowPal": "DISABLED",
    "SpatialAdaptiveQuantization": "ENABLED",
    "TemporalAdaptiveQuantization": "ENABLED",
    "FlickerAdaptiveQuantization": "DISABLED",
    "EntropyEncoding": "CABAC",
    "FramerateControl": "INITIALIZE_FROM_SOURCE",
    "RateControlMode": "QVBR",
    "CodecProfile": "MAIN",
    "Telecine": "NONE",
    "MinIInterval": 0,
    "AdaptiveQuantization": "HIGH",
    "CodecLevel": "AUTO",
    "FieldEncoding": "PAFF",
    "SceneChangeDetect": "TRANSITION_DETECTION",
    "QualityTuningLevel": "SINGLE_PASS_HQ",
    "FramerateConversionAlgorithm": "DUPLICATE_DROP",
    "UnregisteredSeiTimecode": "DISABLED",
    "GopSizeUnits": "SECONDS",
    "ParControl": "INITIALIZE_FROM_SOURCE",
    "NumberBFramesBetweenReferenceFrames": 2,
    "RepeatPps": "DISABLED"
  }
},
"AfdSignaling": "NONE",
"DropFrameTimecode": "ENABLED",
"RespondToAfd": "NONE",
```



```
    "ColorMetadata": "INSERT"
  },
  "OutputSettings": {
    "HlsSettings": {
      "AudioGroupId": "program_audio",
      "AudioRenditionSets": "program_audio",
      "SegmentModifier": "$dt$",
      "IFrameOnlyManifest": "EXCLUDE"
    }
  },
  "NameModifier": "_360"
},
{
  "ContainerSettings": {
    "Container": "M3U8",
    "M3u8Settings": {
      "AudioFramesPerPes": 4,
      "PcrControl": "PCR_EVERY_PES_PACKET",
      "PmtPid": 480,
      "PrivateMetadataPid": 503,
      "ProgramNumber": 1,
      "PatInterval": 0,
      "PmtInterval": 0,
      "TimedMetadata": "NONE",
      "TimedMetadataPid": 502,
      "VideoPid": 481,
      "AudioPids": [
        482,
        483,
        484,
        485,
        486,
        487,
        488,
        489,
        490,
        491,
        492
      ]
    }
  },
  "VideoDescription": {
    "Width": 960,
    "ScalingBehavior": "DEFAULT",
```

```
"Height": 540,  
"TimecodeInsertion": "DISABLED",  
"AntiAlias": "ENABLED",  
"Sharpness": 50,  
"CodecSettings": {  
  "Codec": "H_264",  
  "H264Settings": {  
    "InterlaceMode": "PROGRESSIVE",  
    "NumberReferenceFrames": 3,  
    "Syntax": "DEFAULT",  
    "Softness": 0,  
    "GopClosedCadence": 1,  
    "GopSize": 2,  
    "Slices": 1,  
    "GopBReference": "DISABLED",  
    "MaxBitrate": 3500000,  
    "SlowPal": "DISABLED",  
    "SpatialAdaptiveQuantization": "ENABLED",  
    "TemporalAdaptiveQuantization": "ENABLED",  
    "FlickerAdaptiveQuantization": "DISABLED",  
    "EntropyEncoding": "CABAC",  
    "FramerateControl": "INITIALIZE_FROM_SOURCE",  
    "RateControlMode": "QVBR",  
    "CodecProfile": "MAIN",  
    "Telecine": "NONE",  
    "MinIInterval": 0,  
    "AdaptiveQuantization": "HIGH",  
    "CodecLevel": "AUTO",  
    "FieldEncoding": "PAFF",  
    "SceneChangeDetect": "TRANSITION_DETECTION",  
    "QualityTuningLevel": "SINGLE_PASS_HQ",  
    "FramerateConversionAlgorithm": "DUPLICATE_DROP",  
    "UnregisteredSeiTimecode": "DISABLED",  
    "GopSizeUnits": "SECONDS",  
    "ParControl": "INITIALIZE_FROM_SOURCE",  
    "NumberBFramesBetweenReferenceFrames": 2,  
    "RepeatPps": "DISABLED"  
  }  
},  
"AfdSignaling": "NONE",  
"DropFrameTimecode": "ENABLED",  
"RespondToAfd": "NONE",  
"ColorMetadata": "INSERT"  
},
```

```
"OutputSettings": {
  "HlsSettings": {
    "AudioGroupId": "program_audio",
    "AudioRenditionSets": "program_audio",
    "SegmentModifier": "$dt$",
    "IFrameOnlyManifest": "EXCLUDE"
  }
},
"NameModifier": "_540"
},
{
  "ContainerSettings": {
    "Container": "M3U8",
    "M3u8Settings": {
      "AudioFramesPerPes": 4,
      "PcrControl": "PCR_EVERY_PES_PACKET",
      "PmtPid": 480,
      "PrivateMetadataPid": 503,
      "ProgramNumber": 1,
      "PatInterval": 0,
      "PmtInterval": 0,
      "TimedMetadata": "NONE",
      "VideoPid": 481,
      "AudioPids": [
        482,
        483,
        484,
        485,
        486,
        487,
        488,
        489,
        490,
        491,
        492
      ]
    }
  }
},
"VideoDescription": {
  "Width": 1280,
  "ScalingBehavior": "DEFAULT",
  "Height": 720,
  "TimecodeInsertion": "DISABLED",
  "AntiAlias": "ENABLED",
```

```
"Sharpness": 50,
"CodecSettings": {
  "Codec": "H_264",
  "H264Settings": {
    "InterlaceMode": "PROGRESSIVE",
    "NumberReferenceFrames": 3,
    "Syntax": "DEFAULT",
    "Softness": 0,
    "GopClosedCadence": 1,
    "GopSize": 2,
    "Slices": 1,
    "GopBReference": "DISABLED",
    "MaxBitrate": 5000000,
    "SlowPal": "DISABLED",
    "SpatialAdaptiveQuantization": "ENABLED",
    "TemporalAdaptiveQuantization": "ENABLED",
    "FlickerAdaptiveQuantization": "DISABLED",
    "EntropyEncoding": "CABAC",
    "FramerateControl": "INITIALIZE_FROM_SOURCE",
    "RateControlMode": "QVBR",
    "CodecProfile": "MAIN",
    "Telecine": "NONE",
    "MinIInterval": 0,
    "AdaptiveQuantization": "HIGH",
    "CodecLevel": "AUTO",
    "FieldEncoding": "PAFF",
    "SceneChangeDetect": "TRANSITION_DETECTION",
    "QualityTuningLevel": "SINGLE_PASS_HQ",
    "FramerateConversionAlgorithm": "DUPLICATE_DROP",
    "UnregisteredSeiTimecode": "DISABLED",
    "GopSizeUnits": "SECONDS",
    "ParControl": "INITIALIZE_FROM_SOURCE",
    "NumberBFramesBetweenReferenceFrames": 2,
    "RepeatPps": "DISABLED"
  }
},
"AfdSignaling": "NONE",
"DropFrameTimecode": "ENABLED",
"RespondToAfd": "NONE",
"ColorMetadata": "INSERT"
},
"OutputSettings": {
  "HlsSettings": {
    "AudioGroupId": "program_audio",
```

```

        "AudioRenditionSets": "program_audio",
        "SegmentModifier": "$dt$",
        "IFrameOnlyManifest": "EXCLUDE"
    },
    "NameModifier": "_720"
},
{
    "ContainerSettings": {
        "Container": "M3U8",
        "M3u8Settings": {}
    },
    "AudioDescriptions": [
        {
            "AudioSourceName": "Audio Selector 1",
            "CodecSettings": {
                "Codec": "AAC",
                "AacSettings": {
                    "Bitrate": 96000,
                    "CodingMode": "CODING_MODE_2_0",
                    "SampleRate": 48000
                }
            }
        }
    ],
    "OutputSettings": {
        "HlsSettings": {
            "AudioGroupId": "program_audio",
            "AudioTrackType": "ALTERNATE_AUDIO_AUTO_SELECT_DEFAULT"
        }
    },
    "NameModifier": "_audio"
}
],
"OutputGroupSettings": {
    "Type": "HLS_GROUP_SETTINGS",
    "HlsGroupSettings": {
        "ManifestDurationFormat": "INTEGER",
        "SegmentLength": 6,
        "TimedMetadataId3Period": 10,
        "CaptionLanguageSetting": "OMIT",
        "Destination": "s3://EXAMPLE-BUCKET/HLS/",
        "DestinationSettings": {
            "S3Settings": {

```

```

        "AccessControl": {
            "CannedAcl": "PUBLIC_READ"
        }
    },
    "TimedMetadataId3Frame": "PRIV",
    "CodecSpecification": "RFC_4281",
    "OutputSelection": "MANIFESTS_AND_SEGMENTS",
    "ProgramDateTimePeriod": 600,
    "MinSegmentLength": 0,
    "DirectoryStructure": "SINGLE_DIRECTORY",
    "ProgramDateTime": "EXCLUDE",
    "SegmentControl": "SEGMENTED_FILES",
    "ManifestCompression": "NONE",
    "ClientCache": "ENABLED",
    "StreamInfResolution": "INCLUDE"
}
},
{
    "CustomName": "MP4",
    "Name": "File Group",
    "Outputs": [
        {
            "ContainerSettings": {
                "Container": "MP4",
                "Mp4Settings": {
                    "CslgAtom": "INCLUDE",
                    "FreeSpaceBox": "EXCLUDE",
                    "MoovPlacement": "PROGRESSIVE_DOWNLOAD"
                }
            },
            "VideoDescription": {
                "Width": 1280,
                "ScalingBehavior": "DEFAULT",
                "Height": 720,
                "TimecodeInsertion": "DISABLED",
                "AntiAlias": "ENABLED",
                "Sharpness": 100,
                "CodecSettings": {
                    "Codec": "H_264",
                    "H264Settings": {
                        "InterlaceMode": "PROGRESSIVE",
                        "ParNumerator": 1,

```

```

        "NumberReferenceFrames": 3,
        "Syntax": "DEFAULT",
        "Softness": 0,
        "GopClosedCadence": 1,
        "HrdBufferInitialFillPercentage": 90,
        "GopSize": 2,
        "Slices": 2,
        "GopBReference": "ENABLED",
        "HrdBufferSize": 10000000,
        "MaxBitrate": 5000000,
        "ParDenominator": 1,
        "EntropyEncoding": "CABAC",
        "RateControlMode": "QVBR",
        "CodecProfile": "HIGH",
        "MinIInterval": 0,
        "AdaptiveQuantization": "AUTO",
        "CodecLevel": "AUTO",
        "FieldEncoding": "PAFF",
        "SceneChangeDetect": "ENABLED",
        "QualityTuningLevel": "SINGLE_PASS_HQ",
        "UnregisteredSeiTimecode": "DISABLED",
        "GopSizeUnits": "SECONDS",
        "ParControl": "SPECIFIED",
        "NumberBFramesBetweenReferenceFrames": 3,
        "RepeatPps": "DISABLED",
        "DynamicSubGop": "ADAPTIVE"
    }
},
"AfdSignaling": "NONE",
"DropFrameTimecode": "ENABLED",
"RespondToAfd": "NONE",
"ColorMetadata": "INSERT"
},
"AudioDescriptions": [
    {
        "AudioTypeControl": "FOLLOW_INPUT",
        "AudioSourceName": "Audio Selector 1",
        "CodecSettings": {
            "Codec": "AAC",
            "AacSettings": {
                "AudioDescriptionBroadcasterMix": "NORMAL",
                "Bitrate": 160000,
                "RateControlMode": "CBR",
                "CodecProfile": "LC",

```

```

        "CodingMode": "CODING_MODE_2_0",
        "RawFormat": "NONE",
        "SampleRate": 48000,
        "Specification": "MPEG4"
    }
},
    "LanguageCodeControl": "FOLLOW_INPUT",
    "AudioType": 0
}
]
}
],
"OutputGroupSettings": {
    "Type": "FILE_GROUP_SETTINGS",
    "FileGroupSettings": {
        "Destination": "s3://EXAMPLE-BUCKET/MP4/",
        "DestinationSettings": {
            "S3Settings": {
                "AccessControl": {
                    "CannedAcl": "PUBLIC_READ"
                }
            }
        }
    }
}
},
{
    "CustomName": "Thumbnails",
    "Name": "File Group",
    "Outputs": [
        {
            "ContainerSettings": {
                "Container": "RAW"
            },
            "VideoDescription": {
                "Width": 1280,
                "ScalingBehavior": "DEFAULT",
                "Height": 720,
                "TimecodeInsertion": "DISABLED",
                "AntiAlias": "ENABLED",
                "Sharpness": 50,
                "CodecSettings": {
                    "Codec": "FRAME_CAPTURE",
                    "FrameCaptureSettings": {

```



```

        "FramerateNumerator": 1,
        "FramerateDenominator": 5,
        "MaxCaptures": 500,
        "Quality": 80
    }
},
"AfdSignaling": "NONE",
"DropFrameTimecode": "ENABLED",
"RespondToAfd": "NONE",
"ColorMetadata": "INSERT"
}
],
"OutputGroupSettings": {
    "Type": "FILE_GROUP_SETTINGS",
    "FileGroupSettings": {
        "Destination": "s3://EXAMPLE-BUCKET/Thumbnails/",
        "DestinationSettings": {
            "S3Settings": {
                "AccessControl": {
                    "CannedAcl": "PUBLIC_READ"
                }
            }
        }
    }
}
},
"AdAvailOffset": 0,
"Inputs": [
    {
        "AudioSelectors": {
            "Audio Selector 1": {
                "Offset": 0,
                "DefaultSelection": "DEFAULT",
                "ProgramSelection": 1
            }
        },
        "VideoSelector": {
            "ColorSpace": "FOLLOW"
        },
        "FilterEnable": "AUTO",
        "PsiControl": "USE_PSI",
        "FilterStrength": 0,
    }
]

```

```

        "DeblockFilter": "DISABLED",
        "DenoiseFilter": "DISABLED",
        "TimecodeSource": "EMBEDDED",
        "FileInput": "s3://EXAMPLE-INPUT-BUCKET/input.mp4"
    }
]
}

```

3. Nella cartella batch-transcode, crea un file con una funzione Lambda. Puoi utilizzare il seguente esempio Python e denominare il file `convert.py`.

Le operazioni in batch S3 inviano dati di processi specifici a una funzione Lambda e richiedono i dati dei risultati. Per gli esempi di richiesta e risposta per la funzione Lambda, le informazioni sui codici di risposta e dei risultati e le funzioni Lambda di esempio per le operazioni in batch S3, consulta [Invoke AWS Lambda funzione](#).

```

import json
import os
from urllib.parse import urlparse
import uuid
import boto3

"""
When you run an S3 Batch Operations job, your job
invokes this Lambda function. Specifically, the Lambda function is
invoked on each video object listed in the manifest that you specify
for the S3 Batch Operations job in Step 5.

Input parameter "event": The S3 Batch Operations event as a request
                        for the Lambda function.

Input parameter "context": Context about the event.

Output: A result structure that Amazon S3 uses to interpret the result
        of the operation. It is a job response returned back to S3 Batch
        Operations.
"""
def handler(event, context):

    invocation_schema_version = event['invocationSchemaVersion']
    invocation_id = event['invocationId']
    task_id = event['tasks'][0]['taskId']

```

```

source_s3_key = event['tasks'][0]['s3Key']
source_s3_bucket = event['tasks'][0]['s3BucketArn'].split(':::')[0]
source_s3 = 's3://' + source_s3_bucket + '/' + source_s3_key

result_list = []
result_code = 'Succeeded'
result_string = 'The input video object was converted successfully.'

# The type of output group determines which media players can play
# the files transcoded by MediaConvert.
# For more information, see Creating outputs with AWS Elemental MediaConvert.
output_group_type_dict = {
    'HLS_GROUP_SETTINGS': 'HlsGroupSettings',
    'FILE_GROUP_SETTINGS': 'FileGroupSettings',
    'CMAF_GROUP_SETTINGS': 'CmafGroupSettings',
    'DASH_ISO_GROUP_SETTINGS': 'DashIsoGroupSettings',
    'MS_SMOOTH_GROUP_SETTINGS': 'MsSmoothGroupSettings'
}

try:
    job_name = 'Default'
    with open('job.json') as file:
        job_settings = json.load(file)

    job_settings['Inputs'][0]['FileInput'] = source_s3

    # The path of each output video is constructed based on the values of
    # the attributes in each object of OutputGroups in the job.json file.
    destination_s3 = 's3://{0}/{1}/{2}' \
        .format(os.environ['amzn-s3-demo-destination-bucket'],
                os.path.splitext(os.path.basename(source_s3_key))[0],
                os.path.splitext(os.path.basename(job_name))[0])

    for output_group in job_settings['OutputGroups']:
        output_group_type = output_group['OutputGroupSettings']['Type']
        if output_group_type in output_group_type_dict.keys():
            output_group_type = output_group_type_dict[output_group_type]
            output_group['OutputGroupSettings'][output_group_type]
['Destination'] = \
    "{0}{1}".format(destination_s3,
                    urlparse(output_group['OutputGroupSettings']
[output_group_type]['Destination']).path)
        else:
            raise ValueError("Exception: Unknown Output Group Type {}".format(output_group_type))

```

```
        .format(output_group_type))

    job_metadata_dict = {
        'assetID': str(uuid.uuid4()),
        'application': os.environ['Application'],
        'input': source_s3,
        'settings': job_name
    }

    region = os.environ['AWS_DEFAULT_REGION']
    endpoints = boto3.client('mediaconvert', region_name=region) \
        .describe_endpoints()
    client = boto3.client('mediaconvert', region_name=region,
                          endpoint_url=endpoints['Endpoints'][0]['Url'],
                          verify=False)

    try:
        client.create_job(Role=os.environ['MediaConvertRole'],
                          UserMetadata=job_metadata_dict,
                          Settings=job_settings)

        # You can customize error handling based on different error codes that
        # MediaConvert can return.
        # For more information, see MediaConvert error codes.
        # When the result_code is TemporaryFailure, S3 Batch Operations retries
        # the task before the job is completed. If this is the final retry,
        # the error message is included in the final report.
    except Exception as error:
        result_code = 'TemporaryFailure'
        raise

except Exception as error:
    if result_code != 'TemporaryFailure':
        result_code = 'PermanentFailure'
    result_string = str(error)

finally:
    result_list.append({
        'taskId': task_id,
        'resultCode': result_code,
        'resultString': result_string,
    })

return {
    'invocationSchemaVersion': invocation_schema_version,
```

```
'treatMissingKeyAs': 'PermanentFailure',  
'invocationId': invocation_id,  
'results': result_list  
}
```

4. Per creare un pacchetto di implementazione con `convert.py` e `job.json` come file `.zip` denominato `lambda.zip`, nel computer locale, apri la cartella `batch-transcode` creata in precedenza ed emetti il comando seguente.

Per utenti macOS, eseguire il seguente comando:

```
zip -r lambda.zip convert.py job.json
```

Per utenti Windows, esegui questi comandi:

```
powershell Compress-Archive convert.py lambda.zip
```

```
powershell Compress-Archive -update job.json lambda.zip
```

Creare una funzione Lambda con un ruolo di esecuzione (console)

1. Apri la console all'indirizzo. AWS Lambda <https://console.aws.amazon.com/lambda/>
2. Nel pannello di navigazione a sinistra, scegli Functions (Funzioni).
3. Selezionare Create function (Crea funzione).
4. Scegli Author from scratch (Crea da zero).
5. In Basic information (Informazioni di base) eseguire queste operazioni:
 - a. Nel campo Function name (Nome funzione), immettere **tutorial-lambda-convert**.
 - b. Per Runtime, scegli Python 3.13.
6. Scegli Change default execution role (Cambia ruolo di esecuzione predefinito) e in Execution role (Ruolo di esecuzione) scegli Use an existing role (Utilizza un ruolo esistente).
7. In Ruolo esistente, scegli il nome del ruolo IAM creato per la funzione Lambda nella [Fase 3](#) (ad esempio, **tutorial-lambda-transcode-role**).
8. Mantieni le impostazioni rimanenti impostate sui valori di default.
9. Scegli Crea funzione.

Implementa la tua funzione Lambda con gli archivi in file .zip e configura la funzione Lambda (console)

1. Nel riquadro Origine codice della pagina della funzione Lambda creata in precedenza (ad esempio, **tutorial-lambda-convert**), scegli Carica da e poi File .zip.
2. Scegli Upload (Carica) per selezionare il file .zip locale.
3. Scegli il file `lambda.zip` creato in precedenza, quindi scegli Apri.
4. Selezionare Salva.
5. Nel pannello Runtime settings (Impostazioni runtime), scegli Edit (Modifica).
6. Per indicare al runtime Lambda quale metodo gestore richiamare nel codice della funzione Lambda, inserisci **convert.handler** nel campo Gestore.

Quando si configura una funzione in Python, il valore dell'impostazione del gestore è costituito dal nome del file e dal nome del modulo del gestore, separati da un punto (.). Ad esempio, `convert.handler` richiama il metodo `handler` definito nel file `convert.py`.

7. Selezionare Salva.
8. Nella pagina della funzione Lambda, scegli la scheda Configuration (Configurazione). Nel pannello di navigazione a sinistra nella scheda Configurazione, scegli Variabili di ambiente, quindi scegli Modifica.
9. Scegli Add environment variable (Aggiungi variabile d'ambiente). Quindi, inserisci Chiave e Valore per ciascuna delle variabili di ambiente elencate di seguito.

- Chiave: **DestinationBucket** Valore: **amzn-s3-demo-destination-bucket1**

Questo valore è il bucket S3 per i file multimediali di output creati nella [Fase 1](#).

- Chiave: **MediaConvertRole** Valore: **arn:aws:iam::111122223333:role/tutorial-mediaconvert-role**

Questo valore è l'ARN del ruolo IAM per MediaConvert il quale hai creato nel [passaggio 2](#). Assicurati di sostituire questo ARN con l'ARN effettivo del tuo ruolo IAM.

- Chiave: **Application** Valore: **Batch-Transcoding**

Questo valore è il nome dell'applicazione.

10. Selezionare Salva.

11. (Facoltativo) Nella scheda Configuration (Configurazione), nella sezione General configuration (Configurazione generale) del pannello di navigazione a sinistra, seleziona Edit (Modifica). Nel campo Timeout inserisci **2 min 0 sec**. Poi, scegli Salva.

Il Timeout è la quantità di tempo consentita da Lambda per l'esecuzione di una funzione per una chiamata prima di arrestarla. Il valore predefinito è 3 secondi. I prezzi si basano sulla quantità di memoria configurata e sulla quantità di tempo di esecuzione del codice. Per ulteriori informazioni, consulta [Prezzi di AWS Lambda](#).

Fase 5: Configurazione dell'inventario Amazon S3 per il bucket S3 di origine

Dopo aver impostato la funzione di transcodifica Lambda, devi creare un processo di operazioni in batch S3 per transcodificare una serie di video. Innanzitutto, devi disporre di un elenco degli oggetti video di input sui quali desideri che le operazioni in Batch S3 eseguano l'azione di transcodifica specificata. Per ottenere un elenco di oggetti video di input, puoi generare un report di inventario S3 per il bucket S3 di origine (ad esempio, *amzn-s3-demo-source-bucket*).

Fasi secondarie

- [Creazione e configurazione di un bucket per i report di inventario S3 dei video di input](#)
- [Configurazione dell'inventario Amazon S3 per il bucket S3 di origine dei video](#)
- [Controllo del report di inventario per il bucket S3 di origine dei video](#)

Creazione e configurazione di un bucket per i report di inventario S3 dei video di input

Per archiviare un report di inventario S3 che elenca gli oggetti del bucket S3 di origine, devi creare un bucket di destinazione dell'inventario S3 e configurare una policy perché il bucket possa scrivere i file di inventario nel bucket S3 di origine.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Seleziona Crea bucket.
4. Per Nome bucket, specifica un nome per il bucket, ad esempio *amzn-s3-demo-destination-bucket2*.
5. Per Regione AWS, scegli Regione AWS dove vuoi che risieda il bucket.

Il bucket di destinazione dell'inventario deve trovarsi nello stesso Regione AWS bucket di origine in cui stai configurando S3 Inventory. Il bucket di destinazione dell'inventario può trovarsi in un diverso Account AWS.

6. In Impostazioni di blocco dell'accesso pubblico per questo bucket, mantieni le impostazioni di default (l'opzione Blocca tutto l'accesso pubblico è abilitata).
7. Mantieni le impostazioni rimanenti impostate sui valori di default.
8. Seleziona Crea bucket.
9. Nell'elenco Buckets (Bucket) scegli il nome del bucket appena creato (ad esempio, *amzn-s3-demo-destination-bucket2*).
10. Per concedere ad Amazon S3 l'autorizzazione a scrivere dati per i report di inventario nel bucket di destinazione dell'inventario S3, seleziona la scheda Autorizzazioni.
11. Scorri verso il basso fino alla sezione Policy di bucket e scegli Modifica. Viene visualizzata la pagina Policy del bucket.
12. Per concedere le autorizzazioni per l'inventario S3, nel campo Policy copia la seguente policy del bucket.

Sostituisci i tre valori di esempio rispettivamente con i seguenti valori:

- Il nome del bucket creato per archiviare i rapporti di inventario (ad esempio, *amzn-s3-demo-destination-bucket2*).
- Il nome del bucket di origine che archivia i video di input (ad esempio, *amzn-s3-demo-source-bucket*).
- L' Account AWS ID che hai usato per creare il bucket di sorgenti video S3 (ad esempio, *111122223333*).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InventoryAndAnalyticsExamplePolicy",
      "Effect": "Allow",
      "Principal": {"Service": "s3.amazonaws.com"},
      "Action": "s3:PutObject",
```



```
"Resource":["arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"],
"Condition": {
  "ArnLike": {
    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
  },
  "StringEquals": {
    "aws:SourceAccount": "111122223333",
    "s3:x-amz-acl": "bucket-owner-full-control"
  }
}
}
```

13. Scegli Save changes (Salva modifiche).

Configurazione dell'inventario Amazon S3 per il bucket S3 di origine dei video

Per generare un elenco di file flat di oggetti video e metadati, devi configurare l'inventario S3 per il bucket S3 di origine dei video. Questi report pianificati possono includere tutti gli oggetti del bucket oppure oggetti raggruppati in base a un prefisso condiviso. In questo tutorial, il report di inventario S3 include tutti gli oggetti video nel bucket S3 di origine.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Per configurare un report di inventario S3 dei video di input nel bucket S3 di origine, nell'elenco Bucket scegli il nome del bucket S3 di origine (ad esempio, **amzn-s3-demo-source-bucket**).
4. Scegliere la scheda Management (Gestione),
5. Scorri fino alla sezione Configurazione dell'inventario e scegli Crea configurazione dell'inventario.
6. Nel campo Inventory configuration name (Nome configurazione inventario) inserisci un nome (ad esempio, **tutorial-inventory-config**).
7. In Ambito dell'inventario, scegli Solo versione corrente per Versioni dell'oggetto e mantieni le altre impostazioni di Ambito dell'inventario sui valori predefiniti per questo tutorial.
8. Nella sezione Dettagli report, per Bucket di destinazione, scegli Questo account.
9. In Destinazione, scegli Sfoglia S3 e scegli il bucket di destinazione creato in precedenza per salvare i report di inventario (ad esempio, **amzn-s3-demo-destination-bucket2**). Quindi, scegli Seleziona percorso.

Il bucket di destinazione dell'inventario deve trovarsi nello stesso bucket Regione AWS di origine in cui stai configurando S3 Inventory. Il bucket di destinazione dell'inventario può trovarsi in un diverso Account AWS.

Nel campo Destination bucket (Bucket di destinazione) la Destination bucket permission (Autorizzazione per il bucket di destinazione) viene aggiunta alla policy del bucket di destinazione dell'inventario per consentire ad Amazon S3 di inserirvi i dati. Per ulteriori informazioni, consulta [Creazione di una policy di bucket di destinazione](#).

10. In Frequenza, seleziona Giornaliero.
11. Per Formato di output, seleziona CSV.
12. In Stato, scegli Abilitato.
13. Nella sezione Server-side crittografia, scegli Disabilita per questo tutorial.

Per ulteriori informazioni, consulta [Configurazione dell'inventario utilizzando la console S3](#) e [Concessione ad Amazon S3 dell'autorizzazione per l'utilizzo della chiave gestita dal cliente per la crittografia](#).

14. Nella sezione Campi aggiuntivi - facoltativo, seleziona Dimensioni, Ultima modifica e Classe di archiviazione.
15. Scegli Create (Crea).

Per ulteriori informazioni, consulta [Configurazione dell'inventario utilizzando la console S3](#).

Controllo del report di inventario per il bucket S3 di origine dei video

Quando viene pubblicato un elenco di inventario, i file manifesto vengono inviati al bucket di destinazione dell'inventario S3.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) scegli il nome del bucket di origine dei video (ad esempio, *amzn-s3-demo-source-bucket*).
4. Seleziona Gestione.

5. Per verificare se il report di inventario S3 è pronto per la creazione di un processo di operazioni in batch S3 nella [Fase 7](#), in Configurazioni di inventario, verifica se il pulsante Create processo dal manifesto è abilitato.

 Note

La consegna del primo report di inventario può richiedere fino a 48 ore. Se il pulsante Create job from manifest (Crea processo dal manifesto) è disattivato, il primo report di inventario non è stato consegnato. Devi attendere che venga consegnato il primo report di inventario e che il pulsante Crea processo dal manifesto sia abilitato per creare un processo di operazioni in batch S3 nella [Fase 7](#).

6. Per controllare un report di inventario S3 (`manifest.json`), nella colonna Destinazione, scegli il nome del bucket di destinazione dell'inventario creato in precedenza per l'archiviazione dei report di inventario (ad esempio, *amzn-s3-demo-destination-bucket2*).
7. Nella scheda Oggetti, scegli la cartella esistente con il nome del bucket di origine S3 (ad esempio, *amzn-s3-demo-source-bucket*). Quindi scegli il nome che hai inserito in Nome configurazione inventario quando hai creato la configurazione dell'inventario (ad esempio, **tutorial-inventory-config**).

Puoi visualizzare un elenco di cartelle denominate con la data di generazione dei report.

8. Per controllare il report di inventario S3 giornaliero di una certa data, scegli una cartella denominata con una data di generazione, quindi scegli `manifest.json`.
9. Per controllare i dettagli del report di inventario in una data specifica, nella pagina `manifest.json`, scegli Download (Scarica) o Open (Apri).

Fase 6: creazione di un ruolo IAM per le operazioni in batch S3

Per utilizzare le operazioni in batch S3 per eseguire la transcodifica in batch, per prima cosa devi creare un ruolo IAM per consentire ad Amazon S3 di disporre delle autorizzazioni per eseguire le operazioni in batch S3.

Fasi secondarie

- [Creazione di una policy IAM per le operazioni in batch S3](#)
- [Creare un ruolo IAM per le operazioni in batch S3 e assegna le policy di autorizzazione](#)

Creazione di una policy IAM per le operazioni in batch S3

Devi creare una policy IAM che fornisca alle operazioni in batch S3 l'autorizzazione per leggere il manifesto di input, richiamare la funzione Lambda e scrivere il report di completamento del processo di operazioni in batch S3.

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione sinistro, scegli Policy.
3. Scegli Crea policy.
4. Scegliere la scheda JSON.
5. Nel campo di testo JSON incolla la seguente policy JSON.

Nella policy JSON, sostituisci i quattro valori di esempio con i seguenti valori:

- Il nome del bucket di origine che archivia i video di input (ad esempio, *amzn-s3-demo-source-bucket*).
- Il nome del bucket di destinazione dell'inventario creato nella [Fase 5](#) per archiviare i file `manifest.json` (ad esempio, *amzn-s3-demo-destination-bucket2*).
- Il nome del bucket creato nella [Fase 1](#) per archiviare i file multimediali di output (ad esempio, *amzn-s3-demo-destination-bucket1*). In questo tutorial, abbiamo messo i report di completamento del processo nel bucket di destinazione per i file multimediali di output.
- L'ARN del ruolo della funzione Lambda creato nella [Fase 4](#). Per trovare e copiare l'ARN del ruolo della funzione Lambda, completa le seguenti operazioni:
 - In una nuova scheda del browser, apri la pagina Funzioni nella console Lambda all'indirizzo <https://console.aws.amazon.com/lambda/home#/functions>.
 - Nell'elenco Funzioni, scegli la funzione Lambda creata nella [Fase 4](#) (ad esempio, **tutorial-lambda-convert**).
 - Scegli Copy ARN (Copia ARN).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

        "Sid": "S3Get",
        "Effect": "Allow",
        "Action": [
            "s3:GetObject",
            "s3:GetObjectVersion"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"
        ]
    },
    {
        "Sid": "S3PutJobCompletionReport",
        "Effect": "Allow",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket1/*"
    },
    {
        "Sid": "S3BatchOperationsInvokeLambda",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": [
            "arn:aws:lambda:us-west-2:111122223333:function:tutorial-  

lambda-convert"
        ]
    }
]
}

```

6. Scegliere Next: Tags (Successivo: Tag).
7. Scegliere Next:Review (Successivo: Rivedi).
8. Nel campo Name (Nome), inserire **tutorial-s3batch-policy**.
9. Scegli Crea policy.

Creare un ruolo IAM per le operazioni in batch S3 e assegna le policy di autorizzazione

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione a sinistra, scegli Ruoli, quindi Crea ruolo.

3. Scegli il tipo di ruolo Servizio AWS, quindi seleziona il servizio S3.
4. In Select your use case (Seleziona il tuo caso d'uso), scegli S3 Batch Operations (Operazioni in batch S3).
5. Scegli Avanti.
6. In Collega autorizzazioni, immetti il nome della policy IAM creata in precedenza (ad esempio, **tutorial-s3batch-policy**) nella casella di ricerca per filtrare l'elenco di policy. Seleziona la casella di controllo accanto al nome della policy (ad esempio, **tutorial-s3batch-policy**).
7. Scegli Avanti.
8. Per Nome ruolo, inserisci **tutorial-s3batch-role**.
9. Scegliere Crea ruolo.

Dopo aver creato il ruolo IAM per le operazioni in batch S3, la seguente policy di attendibilità viene automaticamente associata al ruolo per permettere all'entità del servizio delle operazioni in batch S3 di assumere il ruolo IAM. Questa policy di attendibilità consente al principale del servizio di operazioni in batch S3 di assumere il ruolo IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "batchoperations.s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Fase 7: creazione ed esecuzione di un processo di operazioni in batch S3

Per creare un processo di operazioni in batch S3 per elaborare i video di input nel bucket S3 di origine, devi specificare i parametri per questo particolare processo.

 Note

Per iniziare a creare un processo di operazioni in batch S3, devi assicurarti che il pulsante Crea processo dal manifesto sia abilitato. Per ulteriori informazioni, consulta [Controllo del report di inventario per il bucket S3 di origine dei video](#). Se il pulsante Crea processo dal manifesto è disabilitato, il primo report di inventario non è stato consegnato e devi attendere che il pulsante sia abilitato. Dopo aver configurato l'inventario Amazon S3 per il bucket S3 di origine nella [Fase 5](#), la consegna del primo report dell'inventario può richiedere fino a 48 ore.

Fasi secondarie

- [Creare un processo di operazioni in batch S3](#)
- [Esecuzione del processo di operazioni in batch di S3 per richiamare la funzione Lambda](#)
- [\(Facoltativo\) Controllo del report di completamento](#)
- [\(Facoltativo\) Monitoraggio di ogni chiamata Lambda nella console Lambda](#)
- [\(Facoltativo\) Monitora ogni processo di MediaConvert transcodifica video nella console MediaConvert](#)

Creare un processo di operazioni in batch S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Operazioni in batch.
3. Scegli Crea processo.
4. Per Regione AWS, scegli la regione in cui creare il processo.

In questo tutorial, al fine di utilizzare il processo di operazioni in batch S3 per richiamare una funzione Lambda, devi creare il processo nella stessa regione del bucket S3 di origine dei video in cui si trovano gli oggetti a cui fa riferimento il manifesto.

5. Nella sezione Manifesto, procedi nel seguente modo:
 - a. Per Manifest format (Formato manifesto), scegliere S3 inventory report (manifest.json) (Report inventario S3 (manifest.json)).
 - b. In Oggetto manifesto scegli Sfoglia S3 per trovare il bucket creato nella [Fase 5](#) per l'archiviazione dei report di inventario (ad esempio, *amzn-s3-demo-destination-*

- bucket2*). Nella pagina Oggetto manifesto, naviga tra i nomi degli oggetti fino a trovare un file `manifest.json` per una data specifica. Questo file elenca le informazioni su tutti i video che vuoi transcodificare in batch. Una volta trovato il file `manifest.json` da utilizzare, scegli il pulsante di opzione accanto ad esso. Quindi, scegli Seleziona percorso.
- c. (Facoltativo) In ID versione oggetto manifesto - facoltativo, inserisci l'ID versione dell'oggetto manifesto se desideri utilizzare una versione diversa da quella più recente.
6. Scegli Avanti.
 7. Per utilizzare la funzione Lambda per transcodificare tutti gli oggetti elencati nel file `manifest.json` selezionato, in Tipo di operazione, scegli Invoca funzione AWS Lambda .
 8. Nella sezione Chiamare una funzione Lambda completa le operazioni seguenti:
 - a. Scegli Choose from functions in your account (Scegli tra le funzioni del tuo account).
 - b. In Funzione Lambda, scegli la funzione Lambda creata nella [Fase 4](#) (ad esempio, **tutorial-lambda-convert**).
 - c. In Versione della funzione Lambda mantieni il valore di default \$LATEST.
 9. Scegli Avanti. Viene visualizzata la pagina Configura opzioni aggiuntive.
 10. In Opzioni aggiuntive mantieni le impostazioni predefinite.

Per ulteriori informazioni su queste opzioni, consulta [Elementi della richiesta di un processo di operazioni in batch](#).

11. Nella sezione Report di completamento, per Percorso di destinazione del report di completamento, scegli Sfoglia S3. Individua il bucket creato per i file multimediali di output nella [Fase 1](#) (ad esempio, *amzn-s3-demo-destination-bucket1*). Scegli il pulsante di opzione accanto al nome del bucket. Quindi, scegli Seleziona percorso.

Mantieni le impostazioni rimanenti di Report di completamento impostate sui valori di default. Per ulteriori informazioni sulla configurazione dei report di completamento, consulta [Elementi della richiesta di un processo di operazioni in batch](#). Un report di completamento mantiene un registro dei dettagli del processo e delle operazioni eseguite.

12. Nella sezione Autorizzazioni, seleziona Scegli tra ruoli IAM esistenti. In IAM role (Ruolo IAM) scegli il ruolo IAM per il processo di operazioni in batch S3 creato nella [Fase 6](#) (ad esempio, **tutorial-s3batch-role**).
13. Scegli Avanti.
14. Nella pagina Revisione, rivedi le impostazioni. Quindi seleziona Crea processo.

Dopo che S3 ha terminato la lettura del manifesto del processo di operazioni in batch S3, il processo imposta lo stato del processo su In attesa di conferma dell'esecuzione. Per visualizzare gli aggiornamenti dello stato del processo, aggiorna la pagina. Non sarà possibile eseguire il processo finché lo stato non sarà In attesa di esecuzione della conferma.

Esecuzione del processo di operazioni in batch di S3 per richiamare la funzione Lambda

Esegui il processo di operazioni in batch per richiamare la funzione Lambda per la transcodifica dei video. Se il processo non riesce, puoi controllare il report di completamento per identificare la causa.

Per eseguire il processo di operazioni in batch S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Operazioni in batch.
3. Nell'elenco Processi, scegli l'ID processo del processo nella prima riga, ovvero il processo di operazioni in batch S3 creato in precedenza.
4. Scegli Esegui processo.
5. Riesamina i parametri del processo e conferma che il valore di Total objects listed in manifest (Totale oggetti elencati nel manifesto) corrisponda al numero di oggetti nel manifesto. Seleziona quindi Esegui processo.

Viene visualizzata la pagina del processo di operazioni in batch S3.

6. Dopo l'inizio dell'esecuzione del processo, nella pagina del processo, in Status (Stato) controlla lo stato di avanzamento del processo di operazioni in batch S3, ad esempio Status (Stato), % Complete (% completamento), Total succeeded (rate) (Totale riusciti (tasso)), Total failed (rate) (Totale non riusciti (tasso)), Date terminated (Data di terminazione) e Reason for termination (Motivo della terminazione).

Al termine del processo di operazioni in batch S3, visualizza i dati nella pagina del processo per confermare che è stato completato come previsto.

Se oltre il 50% delle operazioni sugli oggetti di un processo di operazione in batch S3 ha esito negativo dopo aver tentato più di 1.000 operazioni, il processo ha automaticamente esito negativo. Per controllare il report di completamento per identificare la causa degli errori, consulta la procedura facoltativa riportata di seguito.

(Facoltativo) Controllo del report di completamento

Puoi utilizzare il report di completamento per determinare quali oggetti non sono riusciti e la causa degli errori.

Come controllare il report di completamento con i dettagli sugli oggetti non eseguiti correttamente

1. Nella pagina del processo di operazioni in batch S3, in Report di completamento, scegli il collegamento per Destinazione del report di completamento.

Viene aperta la pagina del bucket di destinazione dell'output S3.

2. Nella scheda Oggetti, scegli la cartella che ha il nome che termina con l'ID del processo di operazioni in batch S3 creato in precedenza.
3. Scegli results/ (risultati/).
4. Seleziona la casella di controllo accanto al file .csv.
5. Per visualizzare il report del processo, scegli Apri o Scarica.

(Facoltativo) Monitoraggio di ogni chiamata Lambda nella console Lambda

Dopo l'avvio del processo di operazioni in batch S3, il processo richiama la funzione Lambda per ogni oggetto video di input. S3 scrive i log di ogni chiamata Lambda su Logs. CloudWatch Puoi utilizzare il pannello di controllo di monitoraggio della console Lambda per monitorare la funzione Lambda.

1. Apri la console all'indirizzo. AWS Lambda <https://console.aws.amazon.com/lambda/>
2. Nel pannello di navigazione a sinistra, scegli Functions (Funzioni).
3. Nell'elenco Funzioni, scegli la funzione Lambda creata nella [Fase 4](#) (ad esempio, **tutorial-lambda-convert**).
4. Selezionare la scheda Monitor (Monitora).
5. In Metrics (Parametri), visualizza i parametri di runtime per la funzione Lambda.
6. In Logs, visualizza i dati di log per ogni chiamata Lambda tramite CloudWatch Logs Insights.

Note

Quando utilizzi le operazioni in batch S3 con una funzione Lambda, la funzione Lambda viene richiamata su ciascun oggetto. Se il tuo processo di operazioni in batch S3 è grande, può richiamare più funzioni Lambda contemporaneamente, causando un picco nella simultaneità Lambda.

Ciascuna Account AWS ha una quota di concorrenza Lambda per regione. Per ulteriori informazioni, consulta [Dimensionamento della funzione AWS Lambda](#) nella Guida per gli sviluppatori di AWS Lambda . Una best practice per l'utilizzo delle funzioni Lambda con le operazioni in batch S3 è impostare un limite di simultaneità sulla funzione Lambda stessa. Ciò impedisce al tuo processo di consumare la maggior parte della simultaneità Lambda e potenzialmente di limitare altre funzioni nel tuo account. Per ulteriori informazioni, consulta [Gestione della simultaneità riservata Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

(Facoltativo) Monitora ogni processo di MediaConvert transcodifica video nella console MediaConvert

Un MediaConvert lavoro consiste nel transcodificare un file multimediale. Quando il job S3 Batch Operations richiama la funzione Lambda per ogni video, ogni richiamo della funzione Lambda crea un processo di transcodifica per ogni video in ingresso. MediaConvert

1. Accedi e apri la console all'indirizzo. Console di gestione AWS MediaConvert <https://console.aws.amazon.com/mediaconvert/>
2. Se viene visualizzata la pagina MediaConvert introduttiva, scegli **Inizia**.
3. Nell'elenco Processi, visualizza ogni riga per monitorare l'attività di transcodifica per ogni video di input.
4. Identifica la riga del processo che desideri controllare e scegli il collegamento ID processo per aprire la pagina dei dettagli.
5. Nella pagina Job summary (Riepilogo del processo), in Output, scegli il collegamento per l'output HLS, MP4 o miniature, a seconda di cosa supporta il browser in uso, per passare al bucket S3 di destinazione per i file multimediali di output.
6. Nella cartella corrispondente (HLS, MP4 o Miniature) del bucket S3 di destinazione dell'output, scegli il nome dell'oggetto file multimediale di output.

Viene aperta la pagina dei dettagli dell'oggetto.

7. Nella pagina dell'oggetto, in **Panoramica oggetto**, scegli il link in URL oggetto per esaminare il file multimediale di output transcodificato.

Fase 8: Controllo dei file multimediali di output dal bucket S3 di destinazione

Come controllare i file multimediali di output dal bucket S3 di destinazione

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il nome del bucket S3 di destinazione per i file multimediali di output creati nella [Fase 1](#) (ad esempio, *amzn-s3-demo-destination-bucket1*).
4. Nella scheda Objects (Oggetti), ogni video di input ha una cartella con il nome del video di input. Ogni cartella contiene i file multimediali di output transcodificati di un video di input.

Per controllare i file multimediali di output di un video di input, esegui le seguenti operazioni:

- a. Scegli la cartella con il nome del video di input che desideri controllare.
- b. Scegli la cartella Default/ (Predefinito/).
- c. Scegli la cartella di un formato transcodificato (HLS, MP4 o miniature in questo tutorial).
- d. Scegli il nome del file multimediale di output.
- e. Per esaminare il file transcodificato, nella pagina dell'oggetto scegli il link in URL oggetto.

I file multimediali di output in formato HLS vengono suddivisi in segmenti brevi. Per riprodurre questi video, incorpora l'URL oggetto del file .m3u8 in un lettore compatibile.

Fase 9: Pulizia

Se hai transcodificato i video utilizzando S3 Batch Operations, Lambda e MediaConvert solo come esercizio di apprendimento, elimina le AWS risorse che hai allocato in modo da non accumulare più addebiti.

Fasi secondarie

- [Eliminazione della configurazione di inventario S3 per il bucket S3 di origine](#)
- [Eliminazione della funzione Lambda](#)
- [Elimina il gruppo di CloudWatch log](#)
- [Eliminazione dei ruoli IAM e delle policy inline per i ruoli IAM](#)
- [Eliminazione della policy IAM gestita dal cliente](#)
- [Svuotare i bucket S3](#)

- [Eliminazione dei bucket S3](#)

Eliminazione della configurazione di inventario S3 per il bucket S3 di origine

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) scegli il nome del bucket di origine (ad esempio, *amzn-s3-demo-source-bucket*).
4. Scegliere la scheda Management (Gestione),
5. Nella sezione Configurazioni inventario scegli la configurazione di inventario creata nella [Fase 5](#) (ad esempio, **tutorial-inventory-config**).
6. Scegli Elimina e poi Conferma.

Eliminazione della funzione Lambda

1. Apri la AWS Lambda console all'indirizzo. <https://console.aws.amazon.com/lambda/>
2. Nel pannello di navigazione a sinistra, scegli Functions (Funzioni).
3. Seleziona la casella di controllo accanto alla funzione creata nella [Fase 4](#) (ad esempio, **tutorial-lambda-convert**).
4. Scegli Azioni, quindi Elimina.
5. Nella finestra di dialogo Delete function (Elimina funzione), scegli Delete (Elimina).

Elimina il gruppo di CloudWatch log

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel pannello di navigazione a sinistra scegli Log, quindi Gruppi di log.
3. Seleziona la casella di controllo accanto al gruppo di log dal nome che termina con la funzione Lambda creata nella [Fase 4](#) (ad esempio, **tutorial-lambda-convert**).
4. Scegli Actions (Operazioni), quindi scegli Delete log group(s) (Elimina gruppi di registri).
5. Nella finestra di dialogo Delete log group(s) (Elimina gruppo/i di log) scegli Delete (Elimina).

Eliminazione dei ruoli IAM e delle policy inline per i ruoli IAM

Per eliminare i ruoli IAM creati nella [Fase 2](#), nella [Fase 3](#), e nella [Fase 6](#) esegui invece le seguenti operazioni:

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Ruoli, quindi seleziona la casella di controllo accanto al nome del ruolo che desideri eliminare.
3. Scegliere Elimina.
4. Nella finestra di dialogo di conferma inserisci la risposta richiesta nel campo di inserimento di testo in base al comando e scegli Delete (Elimina).

Eliminazione della policy IAM gestita dal cliente

Per eliminare la policy IAM gestita dal cliente creata nella [Fase 6](#), completa le seguenti operazioni:

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione sinistro, scegli Policy.
3. Scegli il pulsante di opzione accanto alla policy creata nella [Fase 6](#) (ad esempio, **tutorial-s3batch-policy**). Puoi utilizzare la casella di ricerca per filtrare l'elenco di policy.
4. Scegli Azioni, quindi Elimina.
5. Conferma di voler eliminare questa policy inserendone il nome nel campo di testo, quindi scegli Elimina.

Svuotare i bucket S3

Per svuotare i bucket S3 creati nei [Prerequisiti](#), nella [Fase 1](#) e nella [Fase 5](#), completa le seguenti operazioni:

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il pulsante di opzione accanto al nome del bucket che desideri svuotare, quindi scegli Svuota.

4. Nella pagina Svuota bucket conferma che desideri svuotare il bucket inserendo **permanently delete** nel campo di testo e quindi scegli Svuota.

Eliminazione dei bucket S3

Per eliminare i bucket S3 creati nei [Prerequisiti](#), nella [Fase 1](#) e nella [Fase 5](#), completa invece le seguenti operazioni:

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket, scegli il pulsante di opzione accanto al nome del bucket che desideri eliminare.
4. Scegliere Elimina.
5. Nella pagina Delete bucket (Elimina bucket) conferma che desideri eliminare il bucket inserendone il nome nel campo di testo e quindi scegli Delete bucket (Elimina bucket).

Fasi successive

Dopo aver completato questo tutorial, puoi esplorare altri casi d'uso rilevanti:

- Puoi usare Amazon CloudFront per trasmettere in streaming i file multimediali transcodificati agli spettatori di tutto il mondo. Per ulteriori informazioni, consulta [Tutorial: Hosting di video in streaming su richiesta con Amazon S3 CloudFront, Amazon e Amazon Route 53](#).
- Puoi transcodificare i video nel momento in cui li carichi nel bucket di origine S3. A tale scopo, puoi configurare un trigger di eventi Amazon S3 che richiami automaticamente la funzione Lambda per transcodificare nuovi oggetti in S3 con MediaConvert. Per maggiori informazioni consulta [Tutorial: Uso di un trigger Amazon S3 per richiamare una funzione Lambda](#) nella Guida per gli sviluppatori di AWS Lambda.

Risoluzione dei problemi relativi a Operazioni in batch S3

Operazioni in batch Amazon S3 consente di eseguire operazioni in batch su larga scala su oggetti Amazon S3. Questa guida ti aiuta a risolvere i problemi più comuni che potresti riscontrare.

Per risolvere i problemi con S3 Batch Replication, consulta [Risoluzione dei problemi nella replica](#).

Sono disponibili due tipi principali di errori relativi a Operazioni in batch:

1. Errore dell'API: l'API richiesta (ad esempio `CreateJob`) non è stata eseguita.
2. Errore del processo: la richiesta API iniziale è stata completata ma il processo non è riuscito, ad esempio, a causa di problemi con il manifesto o le autorizzazioni agli oggetti specificati nel manifesto.

NoSuchJobException

Tipo: errore dell'API

`NoSuchJobException` si verifica quando Operazioni in batch S3 non riesce a individuare il processo specificato. Questo errore può verificarsi in diversi scenari oltre la semplice scadenza del processo. Le cause più comuni sono descritte di seguito.

1. Scadenza del processo: i processi vengono eliminati automaticamente 90 giorni dopo aver raggiunto lo stato terminale (`Complete`, `Cancelled` o `Failed`).
2. ID del processo errato: l'ID del processo utilizzato in `DescribeJob` o `UpdateJobStatus` non corrisponde all'ID restituito da `CreateJob`.
3. Regione errata: tentativo di accedere a un processo in una Regione diversa da quella in cui è stato creato.
4. Account errato: utilizzo di un job ID di un altro account. AWS
5. Errori di formato dell'ID del processo: errori di battitura, caratteri aggiuntivi o formattazione errata nell'ID del processo.
6. Problemi relativi alla tempistica: verifica dello stato del processo subito dopo la creazione, prima che il processo sia completamente registrato.

I messaggi di errore correlati sono descritti di seguito.

1. No such job
2. The specified job does not exist

Best practice per prevenire errori delle API **NoSuchJobException**

1. Archivia immediatamente gli ID del processo: salva l'ID del processo dalla risposta `CreateJob` prima di effettuare le chiamate API successive.

2. Implementa la logica dei tentativi: aggiungi un backoff esponenziale quando controlli lo stato del processo subito dopo la creazione.
3. Configura il monitoraggio: crea CloudWatch allarmi per tenere traccia del completamento del lavoro prima della scadenza di 90 giorni. Per i dettagli, consulta [Using CloudWatch alarms](#) nella Amazon User Guide. CloudWatch
4. Utilizza Regioni coerenti: assicurati che tutte le operazioni del processo utilizzino la stessa Regione per la creazione del processo.
5. Convalida l'input: controlla il formato dell'ID del processo prima di effettuare chiamate API.

Scadenza dei processi

I processi nello stato terminale vengono eliminati automaticamente dopo 90 giorni. Per evitare di perdere informazioni del processo, considera quanto segue.

1. Scarica i report di completamento prima della scadenza: per istruzioni su come recuperare e archiviare i risultati del processo, consulta [Rapporti di completamento](#).
2. Archivia i metadati del processo nei tuoi sistemi: archivia le informazioni critiche del processo nei database o nei sistemi di monitoraggio.
3. Configura notifiche automatiche prima della scadenza di 90 giorni: utilizza Amazon EventBridge per creare regole che attivino le notifiche al termine dei lavori. Per ulteriori informazioni, consulta [Notifiche di eventi Amazon S3](#).

Risoluzione dei problemi di **NoSuchJobException**

1. Utilizza il comando seguente per verificare che il processo sia presente nell'account e nella Regione.

```
aws s3control list-jobs --account-id 111122223333 --region us-east-1
```

2. Usa il seguente comando per effettuare una ricerca in tutti gli stati dei lavori. I possibili stati del processo sono Active, Cancelled, Cancelling, Complete, Completing, Failed, Failing, New, Paused, Pausing, Preparing, Ready e Suspended.

```
aws s3control list-jobs --account-id 111122223333 --job-statuses your-job-status
```

3. Utilizza il comando seguente per verificare se il processo è presente in altre Regioni in cui di solito si creano processi.

```
aws s3control list-jobs --account-id 111122223333 --region job-region-1  
aws s3control list-jobs --account-id 111122223333 --region job-region-2
```

4. Convalida il formato dell'ID del processo. Gli ID del processo in genere contengono 36 caratteri, ad esempio 12345678-1234-1234-1234-123456789012. Verifica la presenza di spazi aggiuntivi, caratteri mancanti o problemi di distinzione tra maiuscole e minuscole e verifica di utilizzare l'ID del processo completo restituito dal comando `CreateJob`.
5. Utilizzate il comando seguente per controllare CloudTrail i log relativi agli eventi di creazione del lavoro.

```
aws logs filter-log-events --log-group-name CloudTrail/S3BatchOperations \ --  
filter-pattern "{ $.eventName = CreateJob }" \ --start-time timestamp
```

AccessDeniedException

Tipo: errore dell'API

`AccessDeniedException` si verifica quando una richiesta di Operazioni in batch S3 viene bloccata a causa di autorizzazioni insufficienti, operazioni non supportate o restrizioni delle policy. Questo è uno degli errori più comuni in Operazioni in batch. Le cause comuni sono le seguenti:

1. Autorizzazioni IAM mancanti: l'identità IAM non dispone delle autorizzazioni necessarie per le API di Operazioni in batch.
2. Autorizzazioni S3 insufficienti: autorizzazioni mancanti per accedere ai bucket di origine o destinazione e agli oggetti.
3. Problemi relativi al ruolo di esecuzione del processo: il ruolo di esecuzione del processo non dispone delle autorizzazioni per eseguire l'operazione specificata.

4. Operazioni non supportate: tentativo di utilizzare operazioni non supportate nella Regione o nel tipo di bucket correnti.
5. Cross-account problemi di accesso: autorizzazioni mancanti per l'accesso a bucket o oggetti tra account.
6. Resource-based restrizioni relative alle policy: policy del bucket o ACL degli oggetti che bloccano l'operazione.
7. Restrizioni SCP (Service Control Policy): Organization-level politiche che impediscono l'operazione.

Messaggi di errore correlati:

1. Access Denied
2. User: arn:aws:iam::account:user/username is not authorized to perform: s3:operation
3. Cross-account pass role is not allowed
4. The bucket policy does not allow the specified operation

Le migliori pratiche per prevenire gli errori AccessDeniedException delle API

1. Utilizza il principio del privilegio minimo: concedi solo le autorizzazioni minime richieste per le operazioni specifiche.
2. Verifica le autorizzazioni prima di eseguire processi di grandi dimensioni: esegui piccoli processi di test per convalidare le autorizzazioni prima di elaborare migliaia di oggetti.
3. Utilizza il simulatore di policy IAM: testa le policy prima dell'implementazione utilizzando il simulatore di policy IAM. Per ulteriori informazioni, consulta [Test delle policy IAM con il simulatore di policy IAM](#) nella Guida per l'utente IAM.
4. Implementa una corretta configurazione multi-account: controlla la configurazione dell'accesso multi-account per le configurazioni dei processi multi-account. Per maggiori informazioni, consulta il tutorial [IAM: Delegare l'accesso tra AWS gli account utilizzando i ruoli IAM](#) nella IAM User Guide.
5. Monitora le modifiche alle autorizzazioni: imposta CloudTrail avvisi per le modifiche alle policy IAM che potrebbero influire sulle operazioni in batch.
6. Documenta i requisiti dei ruoli: mantieni una documentazione chiara delle autorizzazioni richieste per ogni tipo di processo.

7. Utilizza modelli di autorizzazione comuni: utilizza gli esempi di autorizzazione e i modelli di policy:
 - a. [Concessione di autorizzazioni per le operazioni in batch](#)
 - b. [Risorse multi-account in IAM](#) nella Guida per l'utente IAM.
 - c. [Controlla l'accesso agli endpoint VPC utilizzando le policy sugli endpoint PrivateLink](#) nella Guida. AWS PrivateLink

AccessDeniedException risoluzione dei problemi

Segui sistematicamente queste fasi per identificare e risolvere i problemi di autorizzazione.

1. Consulta [Operazioni supportate dalle operazioni in batch S3](#) per le operazioni supportate per Regione. Verifica che le operazioni del bucket di directory siano disponibili solo negli endpoint regionali e zonali. Verifica che l'operazione sia supportata per la classe di archiviazione del bucket.
2. Utilizza il seguente comando per determinare se puoi elencare i processi.

```
aws s3control list-jobs --account-id 111122223333
```

3. Utilizza il comando seguente per verificare le autorizzazioni IAM per l'identità richiedente. L'account che esegue il job necessita delle seguenti autorizzazioni: `s3:CreateJob`, `s3:DescribeJob`, `s3:ListJobs`, `s3:UpdateJobPriority`, `s3:UpdateJobStatus`, e `iam:PassRole`

```
aws sts get-caller-identity 111122223333
```

4. Utilizza il comando seguente per verificare che il ruolo sia presente e utilizzabile.

```
aws iam get-role --role-name role-name
```

5. Utilizza il comando seguente per esaminare la policy di attendibilità del ruolo. Il ruolo che esegue il processo deve disporre di:

1. Una relazione di attendibilità che consente a `batchoperations.s3.amazonaws.com` di assumere il ruolo.
2. Le operazioni eseguite da Operazioni in batch (ad esempio `s3:PutObjectTagging` per le operazioni di tagging).
3. Accesso ai bucket di origine e di destinazione.
4. Autorizzazione a leggere il file manifesto.
5. Autorizzazione a scrivere report di completamento.

```
aws iam get-role --role-name role-name --query 'Role.AssumeRolePolicyDocument'
```

6. Usa il comando seguente per testare l'accesso al manifest e ai bucket di origine.

```
aws s3 ls s3://amzn-s3-demo-bucket
```

7. Testa l'operazione eseguita da Operazioni in batch. Ad esempio, se Operazioni in batch esegue il tagging, applica un tag a un oggetto di esempio nel bucket di origine.
8. Esamina le politiche dei bucket per individuare le politiche che potrebbero negare l'operazione.
 1. Controlla le ACL degli oggetti se utilizzi controlli degli accessi legacy.
 2. Verifica che nessuna policy di controllo dei servizi blocchi l'operazione.
 3. Verifica che le policy degli endpoint VPC consentano Operazioni in batch se si utilizzano endpoint VPC.
9. Usa il seguente comando da utilizzare per identificare CloudTrail gli errori di autorizzazione.

```
aws logs filter-log-events --log-group-name CloudTrail/S3BatchOperations \  
  --filter-pattern "{ $.errorCode = AccessDenied }" \  
  --start-time timestamp
```

SlowDownError

Tipo: errore dell'API

L'eccezione `SlowDownError` si verifica quando l'account ha superato il limite di velocità delle richieste per le API di Operazioni in batch S3. Questo è un meccanismo di limitazione (della larghezza di banda della rete) per proteggere il servizio dal sovraccarico dovuto a troppe richieste. Le cause comuni sono le seguenti:

1. Elevata frequenza di richieste API: troppe chiamate API in un breve periodo di tempo.
2. Operazioni di lavoro simultanee: processi simultanei di più applicazioni o utenti creating/managing .
3. Script automatizzati senza limiti di velocità: script che non implementano strategie di backoff adeguate.
4. Polling troppo frequenti dello stato del processo: verifica dello stato del processo eseguita più spesso del necessario.
5. Modelli di traffico aumentato: picchi improvvisi nell'utilizzo delle API durante i periodi di elaborazione di punta.
6. Limiti di capacità regionale: superamento della capacità di richiesta allocata per la Regione.

Messaggi di errore correlati:

1. `SlowDown`
2. `Please reduce your request rate`
3. `Request rate exceeded`

Procedure consigliate per prevenire gli errori `SlowDownError` delle API

1. Implementa la limitazione della velocità sul lato client: aggiungi ritardi tra le chiamate API nelle applicazioni.
2. Utilizza il backoff esponenziale con jitter: applica la randomizzazione dei ritardi dei tentativi per evitare problemi di thundering herd.
3. Imposta una logica dei tentativi adeguata: implementa tentativi automatici con ritardi crescenti per gli errori transitori.
4. Utilizza architetture basate sugli eventi: sostituisci il polling con EventBridge notifiche per le modifiche allo stato del lavoro.

5. Distribuisci il carico nel tempo: organizza la creazione di processi e i controlli dello stato in diversi periodi di tempo.
6. Monitora e invia avvisi sui limiti di frequenza: imposta CloudWatch allarmi per rilevare quando ti stai avvicinando ai limiti.

La maggior parte degli AWS SDK include una logica di ripetizione integrata per gli errori di limitazione della frequenza. Configurali come segue:

1. AWS CLI: utilizza i parametri `cli-read-timeout` e `cli-connect-timeout`.
2. AWS SDK for Python (Boto3): configura le modalità di riprova e il numero massimo di tentativi nella configurazione del client.
3. AWS SDK per Java: utilizzo e impostazioni. `RetryPolicy ClientConfiguration`
4. AWS SDK per JavaScript: configura `maxRetries` e `retryDelayOptions`

Per ulteriori informazioni sui modelli di riprova e sulle best practice, vedi [Riprova con modello di backoff](#) nella guida Prescriptive Guidance. AWS

SlowDownError risoluzione dei problemi

1. Nel codice, implementa immediatamente il backoff esponenziale.

Example di backoff esponenziale in bash

```
for attempt in {1..5}; do
    if aws s3control describe-job --account-id 111122223333 --job-id job-id; then
        break
    else
        wait_time=$((2**attempt)) echo "Rate limited, waiting ${wait_time}
seconds..." sleep $wait_time
    fi
done
```

2. CloudTrail Da utilizzare per identificare l'origine dell'elevato volume di richieste.

```
aws logs filter-log-events \
    --log-group-name CloudTrail/S3BatchOperations \
```

```
--filter-pattern "{ $.eventName = CreateJob || $.eventName = DescribeJob }" \  
--start-time timestamp \  
--query 'events[*].[eventTime,sourceIPAddress,userIdentity.type,eventName]'
```

3. Verifica la frequenza di polling.

1. Evita di controllare lo stato del processo più di una volta ogni 30 secondi per i processi attivi.
2. Se possibile, utilizza le notifiche di completamento del processo anziché il polling.
3. Implementa jitter negli intervalli di polling per evitare richieste sincronizzate.

4. Ottimizza i modelli di utilizzo delle API.

1. Se possibile, esegui più operazioni in batch.
2. Utilizza `ListJobs` per ottenere lo stato di più processi in una sola chiamata.
3. Memorizza nella cache le informazioni sui processi per ridurre le chiamate API ridondanti.
4. Suddividi la creazione dei processi nel tempo anziché crearne molti contemporaneamente.

5. Utilizza CloudWatch le metriche per le chiamate API per monitorare i modelli di richiesta.

```
aws logs put-metric-filter \  
  --log-group-name CloudTrail/S3BatchOperations \  
  --filter-name S3BatchOpsAPICallCount \  
  --filter-pattern "{ $.eventSource = s3.amazonaws.com && $.eventName =  
CreateJob }" \  
  --metric-transformations \  
    metricName=S3BatchOpsAPICalls,metricNamespace=Custom/  
S3BatchOps,metricValue=1
```

InvalidManifestContent

Tipo: errore del processo

L'eccezione `InvalidManifestContent` si verifica quando ci sono problemi con il formato, il contenuto o la struttura del file manifesto che impediscono a Operazioni in batch S3 di elaborare il processo. Le cause comuni sono le seguenti:

1. Violazioni del formato: colonne obbligatorie mancanti, delimitatori errati o struttura CSV non valida.

2. Problemi di codifica dei contenuti: codifica dei caratteri errata, marcatori BOM o non caratteri UTF-8
3. Problemi con le chiavi dell'oggetto: caratteri non validi, codifica URL non corretta o chiavi che superano i limiti di lunghezza.
4. Limiti relativi alle dimensioni: il manifesto contiene più oggetti di quelli supportati dall'operazione.
5. Errori di formato dell'ID della versione: ID della versione non validi o non corretti per gli oggetti con controllo delle versioni.
6. Problemi relativi al formato di ETag: formato di ETag errato o virgolette mancanti per le operazioni che richiedono ETag.
7. Dati incoerenti: formati misti all'interno dello stesso manifesto o numero di colonne non coerente.

Messaggi di errore correlati:

1. Required fields are missing in the schema: + missingFields
2. Invalid Manifest Content
3. The S3 Batch Operations job failed because it contains more keys than the maximum allowed in a single job
4. Invalid object key format
5. Manifest file is not properly formatted
6. Invalid version ID format
7. ETag format is invalid

Procedure consigliate per prevenire il fallimento del lavoro InvalidManifestContent

1. Convalida prima del caricamento: testa il formato del manifesto con piccoli processi prima di elaborare set di dati di grandi dimensioni.
2. Usa una codifica coerente: usa sempre la UTF-8 codifica senza BOM per i file manifest.
3. Implementa gli standard di generazione dei manifesti: crea modelli e procedure di convalida per la creazione di manifesti.
4. Gestisci correttamente i caratteri speciali: gli URL codificano le chiavi degli oggetti che contengono caratteri speciali.
5. Monitora il numero di oggetti: monitora le dimensioni del manifesto e suddividi i lavori di grandi dimensioni in modo proattivo.

6. Convalida la presenza degli oggetti: verifica la presenza degli oggetti prima di includerli nei manifesti.
7. Usa AWS strumenti per la generazione di manifesti: sfruttali per generare elenchi AWS CLI `s3api list-objects-v2` di oggetti formattati correttamente.

Problemi e soluzioni comuni relativi ai manifesti:

1. Colonne obbligatorie mancanti: assicurati che il manifesto includa tutte le colonne obbligatorie per il tipo di operazione. Le colonne mancanti più comuni sono Bucket e Chiave.
2. Formato CSV non corretto: utilizza le virgole come delimitatori, assicura un numero di colonne uniforme su tutte le righe ed evita gli embedding delle interruzioni di riga nei campi.
3. Caratteri speciali nelle chiavi degli oggetti: gli URL codificano le chiavi degli oggetti che contengono spazi, caratteri Unicode o caratteri speciali XML (<, >, &, ", ').
4. File manifesti di grandi dimensioni: suddividi i manifesti con un numero di operazioni superiore al limite in diversi manifesti più piccoli e crea processi separati.
5. ID della versione non validi: assicurati che gli ID della versione siano stringhe alfanumeriche formattate correttamente. Rimuovi la colonna ID della versione se non è necessaria.
6. Problemi di codifica: salva i file manifest senza BOM. UTF-8 Evita di copiare i manifesti attraverso sistemi che potrebbero alterare la codifica.

Per le specifiche dettagliate e gli esempi relativi al formato del manifesto, consulta quanto segue:

1. [Specifica di un manifest](#)
2. [Operazioni supportate dalle operazioni in batch S3](#)
3. [Denominazione di oggetti Amazon S3](#)

InvalidManifestContent risoluzione dei problemi

1. Scarica e controlla il file manifesto. Verifica manualmente che il manifesto soddisfi i requisiti di formato:
 1. Formato CSV con virgola come delimitatore.
 2. UTF-8 codifica senza BOM.
 3. Numero coerente di colonne per tutte le righe.
 4. Senza righe vuote o spazi finali.

5. Le chiavi dell'oggetto sono codificate correttamente nell'URL se contengono caratteri speciali.

Utilizza il seguente comando per scaricare il file manifesto.

```
aws s3 cp s3://amzn-s3-demo-bucket1/manifest-key ./manifest.csv
```

2. Controlla le colonne obbligatorie per l'operazione:
 1. Tutte le operazioni: Bucket, Key
 2. Operazioni di copia: `VersionId` (facoltativo)
 3. Operazioni di ripristino: `VersionId` (facoltativo)
 4. Operazioni di sostituzione di tag: non sono necessarie colonne aggiuntive.
 5. Operazioni di sostituzione di ACL: non sono necessarie colonne aggiuntive.
 6. Avvia ripristino: `VersionId` (facoltativo)
3. Controlla i limiti del numero di oggetti:
 1. Copia: massimo 1 miliardo di oggetti.
 2. Eliminazione: massimo 1 miliardo di oggetti.
 3. Ripristino: massimo 1 miliardo di oggetti.
 4. Tagging: massimo 1 miliardo di oggetti.
 5. ACL: massimo 1 miliardo di oggetti.
4. Crea un manifesto di test con alcuni oggetti del tuo manifesto originale.
5. Utilizzate il comando seguente per verificare se esiste un campione di oggetti del manifesto.

```
aws s3 ls s3://amzn-s3-demo-bucket1/object-key
```

6. Controlla i dettagli dell'errore del processo e verifica il motivo ed eventuali dettagli specifici dell'errore nella descrizione del processo.

```
aws s3control describe-job --account-id 111122223333 --job-id job-id
```

Interrogazione dei dati in loco con Amazon S3 Select

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Con Amazon S3 Select è possibile utilizzare un linguaggio di query strutturata (SQL) per filtrare i contenuti di oggetti Amazon S3 e recuperare solo il sottoinsieme di dati necessario. Utilizzando Amazon S3 Select per filtrare questi dati, è possibile ridurre la quantità di dati trasferiti da Amazon S3, riducendo il costo e la latenza di recupero dei dati.

Amazon S3 Select consente di interrogare un solo oggetto alla volta. Funziona su un oggetto memorizzato in formato CSV, JSON o Apache Parquet. Funziona anche con un oggetto compresso con GZIP o BZIP2 (solo per oggetti CSV e JSON) e con un oggetto crittografato lato server. È possibile specificare il formato dei risultati come CSV o JSON e determinare in che modo i record del risultato sono delimitati.

Passi espressioni SQL ad Amazon S3 nella richiesta. Amazon S3 Select supporta un sottoinsieme di SQL. Per ulteriori informazioni sugli elementi SQL supportati da Amazon S3 Select, consulta [Documentazione di riferimento su SQL per Amazon S3 Select](#).

Puoi eseguire query SQL utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'operazione API `SelectObjectContent` REST o gli SDK AWS.

Note

La console di Amazon S3 limita la quantità di dati restituiti a 40 MB. Per recuperare più dati, utilizza o l'AWS CLI API.

Requisiti e limiti

Di seguito vengono riportati i requisiti per l'utilizzo di Amazon S3 Select:

- Devi disporre delle autorizzazioni `s3:GetObject` per l'oggetto su esegui la query.
- Se l'oggetto che stai interrogando è crittografato con crittografia lato server con chiavi fornite dal cliente (SSE-C), devi utilizzare `https` e devi fornire la chiave di crittografia nella richiesta.

Per l'utilizzo di Amazon S3 Select si applicano i seguenti limiti:

- S3 Select può interrogare un solo oggetto per richiesta.
- S3 Select supporta l'interrogazione di file di dimensioni fino a 5 TB.
- La lunghezza massima di un'espressione SQL è di 256 KB.
- La lunghezza massima di un record nell'input o nel risultato è di 1 MB.
- Amazon S3 Select può emettere solo dati nidificati utilizzando il formato di output JSON.
- Non è possibile interrogare un oggetto memorizzato nelle classi di storage Recupero flessibile S3 Glacier, S3 Glacier Deep Archive o Reduced Redundancy Storage (RRS). Inoltre, non è possibile interrogare un oggetto archiviato nel livello S3 Intelligent-Tiering Archive Access o nel livello S3 Intelligent-Tiering Deep Archive Access. Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

Ulteriori limitazioni si applicano quando si utilizza Amazon S3 Select con un oggetto Parquet:

- Amazon S3 Select supporta solo la compressione a colonne con GZIP o Snappy. Amazon S3 Select non supporta la compressione dell'intero oggetto per un oggetto Parquet.
- Amazon S3 Select non supporta l'output Parquet. È necessario specificare il formato di output, ad esempio CSV o JSON.
- La dimensione massima del gruppo di righe non compresso è 256 MB.
- È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
- Se si seleziona un campo ripetuto, viene restituito solo l'ultimo valore.

Costruzione di una richiesta

Quando costruisci una richiesta, devi fornire i dettagli dell'oggetto su cui si sta eseguendo la query utilizzando un oggetto `InputSerialization`. Fornisci i dettagli del modo in cui i risultati vengono restituiti utilizzando un oggetto `OutputSerialization`. Includi anche l'espressione SQL utilizzata da Amazon S3 per filtrare la richiesta.

Per ulteriori informazioni sulla creazione di una richiesta Amazon S3 Select, consulta [SelectObjectContent](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service. Uno degli esempi di codice SDK è anche disponibile nelle seguenti sezioni.

Richieste che utilizzano intervalli di scansione

Amazon S3 Select consente di eseguire la scansione di un sottoinsieme di un oggetto specificando un intervallo di byte su cui eseguire la query. Ciò consente di parallelizzare la scansione dell'intero oggetto dividendo il lavoro tra due richieste Amazon S3 Select separate per una serie di intervalli di scansione senza sovrapposizione.

Gli intervalli di scansione non devono essere allineati con i limiti di record. Una richiesta Amazon S3 Select di intervallo di scansione viene eseguita nell'intervallo di byte specificato. Un record che inizia nell'intervallo di scansione specificato ma che si estende oltre verrà elaborato dalla query. Ad esempio, di seguito viene mostrato un oggetto Amazon S3 contenente una serie di record in formato CSV delimitato da righe:

```
A,B  
C,D  
D,E  
E,F  
G,H  
I,J
```

Viene utilizzato il parametro `ScanRange` di Amazon S3 Select e `Start a (Byte) 1` ed `End a (Byte) 4`. Pertanto, l'intervallo di scansione inizia a ", " e la scansione verrà eseguita fino alla fine del record che inizia a C. La richiesta dell'intervallo di scansione restituirà il risultato C, D perché questa è la fine del record.

Le richieste di intervallo di scansione di Amazon S3 Select supportano gli oggetti Parquet, CSV (senza delimitatori quotati) o JSON (solo in modalità `LINES`). Gli oggetti CSV e JSON non devono essere compressi. Per gli oggetti CSV e JSON basati su righe, quando viene specificato un intervallo di scansione come parte della richiesta Amazon S3 Select, vengono elaborati tutti i record che iniziano nell'intervallo di scansione. Per gli oggetti Parquet, vengono elaborati tutti i gruppi di righe che iniziano all'interno dell'intervallo di scansione richiesto.

Le richieste relative all'intervallo di scansione di Amazon S3 Select possono essere utilizzate con l' AWS CLI API Amazon S3 e gli SDK. AWS Per questa caratteristica, è possibile utilizzare il parametro `ScanRange` nella richiesta Amazon S3 Select. Per ulteriori informazioni, consulta

[SelectObjectContent](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Errori

Amazon S3 Select restituisce un codice di errore e un messaggio di errore associato quando si verifica un problema durante il tentativo di esecuzione di una query. Per un elenco di codici di errore e descrizioni, consulta la sezione relativa all'[elenco dei codici di errore relativo al contenuto dell'oggetto SELECT](#) nella pagina delle risposte agli errori nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Per maggiori informazioni su Amazon S3 Select, consulta gli argomenti seguenti:

Argomenti

- [Esempi di utilizzo di Amazon S3 Select su un oggetto](#)
- [Documentazione di riferimento su SQL per Amazon S3 Select](#)

Esempi di utilizzo di Amazon S3 Select su un oggetto

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Puoi utilizzare S3 Select per selezionare il contenuto da un oggetto utilizzando la console Amazon S3, l'API REST e gli SDK. AWS

Per ulteriori informazioni sulle funzioni SQL supportate per S3 Select, consulta [Funzioni SQL](#).

Utilizzo della console S3

Per selezionare il contenuto da un oggetto nella console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Scegli il bucket che contiene l'oggetto da cui desideri selezionare il contenuto, quindi scegli il nome dell'oggetto.

4. Scegli Azioni oggetto e Interroga con S3 Select.
5. Configura impostazioni di input, in base al formato dei dati di input.
6. Configura impostazioni di output, in base al formato dell'output che desideri ricevere.
7. Per estrarre i record dall'oggetto scelto, in query SQL, inserisci i comandi SELECT SQL. Per ulteriori informazioni su come scrivere comandi SQL, consulta [Documentazione di riferimento su SQL per Amazon S3 Select](#).
8. Dopo aver inserito le query SQL, scegli Esegui query SQL. Quindi, in Risultati della query, puoi visualizzare i risultati delle tue query SQL.

Utilizzo della REST API

Puoi utilizzare gli AWS SDK per selezionare il contenuto di un oggetto. Tuttavia, se l'applicazione lo richiede, è possibile inviare richieste REST direttamente. Per ulteriori informazioni sul formato della richiesta e della risposta, consulta [SelectObjectContent](#).

Utilizzo di AWS SDK

È possibile utilizzare Amazon S3 Select per selezionare alcuni dei contenuti di un oggetto utilizzando il metodo `selectObjectContent`. Se questo metodo ha esito positivo, restituisce i risultati dell'espressione SQL.

Java

Per utilizzare Amazon S3 Select con l' AWS SDK per Java, puoi restituire il valore della prima colonna per ogni record archiviato in un oggetto che contiene dati archiviati in formato CSV. È anche possibile richiedere che vengano restituiti i messaggi Progress e Stats. Fornire un nome bucket e un oggetto validi contenenti dati in formato CSV.

Per utilizzare Amazon S3 Select con l' AWS SDK per Java, puoi restituire il valore della prima colonna per ogni record archiviato in un oggetto che contiene dati archiviati in formato CSV. È anche possibile richiedere che vengano restituiti i messaggi Progress e Stats. Fornire un nome bucket e un oggetto validi contenenti dati in formato CSV.

Per esempi di come utilizzare Amazon S3 Select con l' AWS SDK per Java, consulta [Selezione di contenuti da un oggetto](#) nell'Amazon S3 API Reference.

JavaScript

Per un JavaScript esempio che utilizza l'operazione AWS SDK per JavaScript con `selectObjectContentAPI` S3 per selezionare record da file JSON e CSV archiviati in Amazon

S3, consulta il post del blog [Introducing support for Amazon S3 Select nel. AWS SDK per JavaScript](#)

Python

Per un esempio Python sull'utilizzo delle query SQL per cercare i dati caricati su Amazon S3 come file CSV (Comma-Separated Value) utilizzando S3 Select, vedere il post del blog [Interrogazione di dati senza server o database tramite Amazon S3 Select](#).

Documentazione di riferimento su SQL per Amazon S3 Select

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Questa documentazione di riferimento contiene una descrizione degli elementi SQL supportati da Amazon S3 Select.

Argomenti

- [SELECT command](#)
- [Tipi di dati](#)
- [Operatori](#)
- [Parole chiave riservate](#)
- [Funzioni SQL](#)

SELECT command

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta soltanto il comando SQL SELECT. Le seguenti clausole standard ANSI sono supportate per SELECT:

- SELECT Elenco
- FROM Clausola
- WHERE Clausola
- LIMIT Clausola

 Note

Al momento, le query di Amazon S3 Select non supportano query secondarie o join.

SELECT elenco

L'elenco SELECT assegna un nome a colonne, funzioni ed espressioni che la query deve restituire. L'elenco rappresenta l'output della query.

```
SELECT *  
SELECT projection1 AS column_alias_1, projection2 AS column_alias_2
```

La prima forma di SELECT con * (asterisco) restituisce ogni riga che ha passato la clausola , così com'è. Il secondo formato di SELECT crea una riga con espressioni scalari di output definite dall'utente **projection1** e **projection2** per ogni colonna.

FROM clausola

Amazon S3 Select supporta i seguenti formati della clausola FROM:

```
FROM table_name  
FROM table_name alias  
FROM table_name AS alias
```

In ogni forma della clausola FROM, `table_name` è il `S3Object` che viene interrogato. Gli utenti abituati a database relazionali tradizionali possono considerare questo come uno schema di database che contiene più viste di una tabella.

Nel linguaggio SQL standard, la clausola FROM crea righe che vengono filtrate nella clausola WHERE e proiettate nell'elenco SELECT.

Per tutti gli oggetti JSON archiviati in Amazon S3 Select, puoi anche utilizzare i seguenti moduli della clausola FROM:

```
FROM S3object[*].path  
FROM S3object[*].path alias  
FROM S3object[*].path AS alias
```

Utilizzando questo modulo della clausola FROM, puoi selezionare da array o oggetti inclusi in un oggetto JSON. Puoi specificare path mediante uno dei seguenti moduli:

- Per nome (in un oggetto): *.name* o [*'name'*]
- Per indice (in un array): [*index*]
- Per carattere jolly (in un oggetto): *.**
- Per carattere jolly (in un array): [***]

Note

- Questo modulo della clausola FROM è utilizzabile solo con oggetti JSON.
- I caratteri jolly emettono sempre almeno un record. Se nessun record corrisponde, Amazon S3 Select emette il valore MISSING. Durante la serializzazione dell'output (dopo che la query è stata completata), Amazon S3 Select sostituisce i valori MISSING con record vuoti.
- Le funzioni di aggregazione (AVG, COUNT, MAX, MIN e SUM) ignorano i valori MISSING.
- Se non fornisci un alias quando utilizzi un carattere jolly, puoi fare riferimento alla riga utilizzando l'ultimo elemento nel percorso. Ad esempio, puoi selezionare tutti i prezzi da un elenco di libri utilizzando la query `SELECT price FROM S3object[*].books[*].price`. Se il percorso termina con un carattere jolly anziché con un nome, puoi utilizzare il valore `_1` per fare riferimento alla riga. Ad esempio, anziché `SELECT price FROM S3object[*].books[*].price`, puoi usare la query `SELECT _1.price FROM S3object[*].books[*]`.
- Amazon S3 Select considera sempre un documento JSON come un array di valori a livello di radice. Pertanto, anche se l'oggetto JSON che stai interrogando ha solo un elemento radice, la clausola FROM deve iniziare con `S3object[*]`. Tuttavia, per motivi di compatibilità, Amazon S3 Select consente di omettere il carattere jolly se non si include un percorso. Pertanto, la clausola completa `FROM S3object` è equivalente a `FROM S3object[*] as S3object`. Se includi un percorso, devi utilizzare anche il carattere jolly. Pertanto `FROM S3object` e `FROM S3object[*].path` sono entrambe clausole valide, ma `FROM S3object.path` non è valida.

Example

Esempi:

Esempio 1

Questo esempio mostra i risultati utilizzando i seguenti set di dati e query:

```
{ "Rules": [ {"id": "1"}, {"expr": "y > x"}, {"id": "2", "expr": "z = DEBUG"} ]}  
{ "created": "June 27", "modified": "July 6" }
```

```
SELECT id FROM S3object[*].Rules[*].id
```

```
{"id":"1"}  
{}  
{"id":"2"}  
{}
```

Amazon S3 Select produce ciascun risultato per i seguenti motivi:

- {"id":"id-1"}— S3object[0].Rules[0].id ha prodotto una corrispondenza.
- {} - S3object[0].Rules[1].id non ha prodotto una corrispondenza con un record, quindi Amazon S3 Select ha emesso un valore MISSING, che è stato quindi modificato in un record vuoto durante la serializzazione dell'output e restituito.
- {"id":"id-2"}— S3object[0].Rules[2].id ha prodotto una corrispondenza.
- {}-S3object[1] non ha prodotto una corrispondenza in Rules, quindi Amazon S3 Select ha emesso un valore MISSING, che è stato quindi modificato in un record vuoto durante la serializzazione dell'output e restituito.

Se non desideri che Amazon S3 Select restituisca record vuoti quando non trova una corrispondenza, puoi testare il valore MISSING. La seguente query restituisce gli stessi risultati della query precedente, ma con i valori vuoti omessi:

```
SELECT id FROM S3object[*].Rules[*].id WHERE id IS NOT MISSING
```

```
{"id":"1"}  
{"id":"2"}
```

Esempio 2

Questo esempio mostra i risultati utilizzando i seguenti set di dati e query:

```
{ "created": "936864000", "dir_name": "important_docs", "files": [ { "name": "." },  
  { "name": ".." }, { "name": ".aws" }, { "name": "downloads" } ], "owner": "Amazon  
S3" }  
{ "created": "936864000", "dir_name": "other_docs", "files": [ { "name": "." },  
  { "name": ".." }, { "name": "my stuff" }, { "name": "backup" } ], "owner": "User" }
```

```
SELECT d.dir_name, d.files FROM S3Object[*] d
```

```
{"dir_name":"important_docs","files":[{"name":"."},{"name":".."}, {"name":".aws"},  
{"name":"downloads"}]}  
{"dir_name":"other_docs","files":[{"name":"."},{"name":".."}, {"name":"my stuff"},  
{"name":"backup"}]}
```

```
SELECT _1.dir_name, _1.owner FROM S3Object[*]
```

```
{"dir_name":"important_docs","owner":"Amazon S3"}  
{"dir_name":"other_docs","owner":"User"}
```

WHERE clausola

La sintassi della clausola WHERE è la seguente:

```
WHERE condition
```

La clausola WHERE filtra le righe in base alla *condition*. Una condizione è un'espressione che genera un risultato booleano. Solo le righe per le quali la condizione è TRUE sono restituite nel risultato.

LIMIT clausola

La sintassi della clausola LIMIT è la seguente:

```
LIMIT number
```

La clausola LIMIT limita il numero di record che desideri vengano restituiti dalla query in base al *number* specificato.

Accesso agli attributi

Le clausole SELECT e WHERE possono fare riferimento a record di dati utilizzando uno dei metodi descritti nelle seguenti sezioni, a seconda che il file su cui viene eseguita la query sia in formato CSV o JSON.

CSV

- Numeri di colonna: puoi fare riferimento alla N-esima colonna di una riga con il nome di colonna *_N*, dove *N* è la posizione della colonna. La numerazione delle posizioni inizia da 1. Ad esempio, la prima colonna è denominata *_1* e la seconda è denominata *_2*.

Puoi fare riferimento a una colonna con *_N* o *alias._N*. Ad esempio, *_2* e *myAlias._2* sono entrambi modi validi di fare riferimento a una colonna nell'elenco SELECT e nella clausola WHERE.

- Intestazioni di colonna: per gli oggetti in formato CSV che hanno una riga di intestazione, le intestazioni sono disponibili per l'elenco SELECT e la clausola WHERE. In particolare, come nel linguaggio SQL classico, all'interno di espressioni con le clausole SELECT e WHERE è possibile fare riferimento alle colonne in base a *alias.column_name* o *column_name*.

JSON

- Documento: puoi accedere ai campi di documento JSON con *alias.name*. È inoltre possibile accedere ai campi nidificati, ad esempio *alias.name1.name2.name3*.
- Elenco: puoi accedere agli elementi in un elenco JSON utilizzando indici a base zero con l'operatore *[]*. Ad esempio, puoi accedere al secondo elemento di un elenco con *alias[1]*. È possibile abbinare l'accesso agli elementi dell'elenco con i campi, *alias.name1.name2[1].name3*, ad esempio.
- Esempi: considera questo oggetto JSON come un set di dati di esempio:

```
{
  "name": "Susan Smith",
  "org": "engineering",
  "projects": [
    {
      "project_name": "project1",
      "completed": false
    },
    {
      "project_name": "project2",
      "completed": true
    }
  ]
}
```

```
}
```

Esempio 1

La seguente query restituisce questi risultati:

```
Select s.name from S3Object s
```

```
{"name":"Susan Smith"}
```

Esempio 2

La seguente query restituisce questi risultati:

```
Select s.projects[0].project_name from S3Object s
```

```
{"project_name":"project1"}
```

Distinzione tra maiuscole e minuscole nei nomi di intestazioni/attributi

Con Amazon S3 Select puoi utilizzare le virgolette doppie per indicare che nelle intestazioni di colonna (per gli oggetti CSV) e negli attributi (per gli oggetti JSON) si applica la distinzione tra maiuscole e minuscole. In assenza delle virgolette doppie, le intestazioni e gli attributi degli oggetti non prevedono distinzione tra maiuscole e minuscole. In caso di ambiguità viene generato un errore.

I seguenti esempi sono 1) oggetti Amazon S3 in formato CSV con le intestazioni di colonna specificate e con impostato su "Use" per la richiesta di query oppure 2) oggetti Amazon S3 in formato JSON con gli attributi specificati.

Esempio #1: l'oggetto su cui viene eseguita la query ha intestazione o attributo NAME.

- La seguente espressione restituisce correttamente i valori dall'oggetto. Poiché non sono presenti virgolette, la query non fa distinzione tra maiuscole e minuscole.

```
SELECT s.name from S3Object s
```

- La seguente espressione genera un errore 400 MissingHeaderName. Poiché sono presenti le virgolette, la query fa distinzione tra maiuscole e minuscole.

```
SELECT s."name" from S3object s
```

Esempio 2: l'oggetto Amazon S3 su cui viene eseguita la query ha un'intestazione o attributo con NAME e un'altra intestazione o attributo con name.

- La seguente espressione genera un errore 400 `AmbiguousFieldName`. Poiché senza virgolette, senza distinzione tra maiuscole e minuscole, ma ci sono due corrispondenze, quindi viene generato un errore.

```
SELECT s.name from S3object s
```

- La seguente espressione restituisce correttamente i valori dall'oggetto. Poiché sono presenti le virgolette, la query fa distinzione tra maiuscole e minuscole, quindi non vi è alcuna ambiguità.

```
SELECT s."NAME" from S3object s
```

Utilizzo di parole chiave riservate come termini definiti dall'utente

Amazon S3 Select dispone di un set di parole chiave riservate, necessarie per eseguire le espressioni SQL utilizzate per le query sul contenuto degli oggetti. Tali parole chiave riservate includono nomi di funzioni, tipi di dati, operatori e così via. In alcuni casi, i termini definiti dall'utente, ad esempio le intestazioni di colonna (per i file CSV) o gli attributi (per gli oggetti JSON) possono essere in conflitto con una parola chiave riservata. Quando ciò si verifica, devi utilizzare le virgolette doppie per indicare che stai intenzionalmente utilizzando un termine definito dall'utente in conflitto con una parola chiave riservata. In caso contrario, verrà generato un errore di analisi 400.

Per l'elenco completo delle parole chiave riservate, consulta [Parole chiave riservate](#).

Il seguente esempio è 1) un oggetto Amazon S3 in formato CSV con le intestazioni di colonna specificate e con `FileHeaderInfo` impostato su "Use" per la richiesta di query oppure 2) un oggetto Amazon S3 in formato JSON con gli attributi specificati.

Esempio: l'oggetto su cui viene eseguita la query ha un'intestazione o attributo denominato CAST, che è una parola chiave riservata.

- La seguente espressione restituisce correttamente i valori dall'oggetto. Poiché nella query vengono utilizzate le virgolette, S3 Select utilizza l'intestazione o l'attributo definiti dall'utente.


```
SELECT s."CAST" from S3object s
```

- La seguente espressione genera un errore 400 di analisi. Poiché nella query non vengono utilizzate virgolette, CAST entra in conflitto con una parola chiave riservata.

```
SELECT s.CAST from S3object s
```

Espressioni scalari

Nella clausola WHERE e nell'elenco SELECT, puoi avere espressioni scalari di SQL, ovvero espressioni che restituiscono valori scalari. Queste espressioni hanno la seguente forma:

- ***literal***

Un valore letterale SQL.

- ***column_reference***

Un riferimento a una colonna nel modulo *column_name* o *alias.column_name*.

- ***unary_op expression***

In questo caso, ***unary_op*** è un operatore SQL unario.

- ***expression binary_op expression***

In questo caso, ***binary_op*** è un operatore binario SQL.

- ***func_name***

In questo caso, ***func_name*** è il nome della funzione scalare da richiamare.

- ***expression* [NOT] BETWEEN *expression* AND *expression***

- ***expression* LIKE *expression* [ESCAPE *expression*]**

Tipi di dati

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta diversi tipi di dati primitivi.

Conversioni dei tipi di dati

La regola generale è di seguire la funzione CAST se definita. Se CAST non è definita, tutti i dati di input vengono trattati come stringa. In tal caso, è necessario inserire i dati di input ai tipi di dati pertinenti quando necessario.

Per ulteriori informazioni sulla funzione CAST, consulta [CAST](#).

Tipi di dati supportati

Amazon S3 Select supporta il seguente set di tipi di dati primitivi.

Nome	Descrizione	Esempi
bool	Un valore booleano, TRUE o FALSE.	FALSE
int, integer	Intero con segno da 8 byte compreso nell'intervallo da -9.223.372.036.854.775.808 a 9.223.372.036.854.775.807.	100000
string	Una stringa di UTF8-encoded lunghezza variabile. Il limite di default è 1 carattere. Il limite massimo di caratteri è 2.147.483.647.	'xyz'
float	Numero in virgola mobile a 8 byte.	CAST(0.456 AS FLOAT)
decimal, numeric	Numero in base 10, con una precisione massima di 38 (ovvero il numero massimo di cifre significative) e con scala compresa nell'intervallo da -2^{31} a $2^{31}-1$ (ovvero l'esponente in base 10).	123.456

 **Note**
Amazon S3 Select ignora il dimensionamento e la precisione quando vengono forniti entrambi contemporaneamente.

Nome	Descrizione	Esempi
timestamp	<p>I time stamp rappresentano un momento specifico nel tempo, includono sempre un offset locale e consentono di stabilire una precisione arbitraria.</p> <p>Nel formato di testo, i timestamp seguono i formati di data e ora della notazione W3C, ma devono terminare con il letterale T se la precisione non è di almeno un giorno completo. Sono consentite frazioni di secondo, con almeno una cifra di precisione e un massimo illimitato. Local-time gli offset possono essere rappresentati come offset di ore:minut i dall'UTC o come valore letterale Z per indicare l'ora locale dell'UTC. Local-time gli offset sono obbligatori nei timestamp con l'ora e non sono consentiti sui valori di data.</p>	CAST('2007-04-05T14:30Z' AS TIMESTAMP)

Supportata Parquet tipi

Amazon S3 Select supporta i seguenti tipi di Parquet:

- DATE
- DECIMAL
- ENUM
- INT(8)
- INT(16)
- INT(32)
- INT(64)
- LIST

Note

Per l'output del tipo LIST Parquet, Amazon S3 Select supporta solo il formato JSON. Tuttavia, se la query limita i dati a valori semplici, il tipo di LIST Parquet può essere interrogato anche in formato CSV.

- STRING
- TIMESTAMP precisione supportata (MILLIS/MICROS/NANOS)

 Note

I timestamp salvati come INT(96) non sono supportati.

A causa della gamma del tipo INT(64), i timestamp che utilizzano l'unità NANOS possono rappresentare solo valori compresi tra 1677-09-21 00:12:43 e 2262-04-11 23:47:16. I valori al di fuori di questo intervallo non possono essere rappresentati con l'unità NANOS.

Mappatura di Parquet tipi ai tipi di dati supportati in Amazon S3 Select

Tipi di Parquet	Tipi di dati supportati
DATE	timestamp
DECIMAL	decimal, numeric
ENUM	string
INT(8)	int, integer
INT(16)	int, integer
INT(32)	int, integer
INT(64)	decimal, numeric
LIST	Ogni tipo di Parquet nell'elenco è mappato al tipo di dati corrispondente
STRING	string

Tipi di Parquet	Tipi di dati supportati
TIMESTAMP	timestamp

Operatori

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta i seguenti operatori.

Operatori logici

- AND
- NOT
- OR

Operatori di confronto

- <
- >
- <=
- >=
- =
- <>
- !=
- BETWEEN
- IN – Ad esempio: IN ('a', 'b', 'c')

Pattern-matching operatori

- LIKE

- `_` (Corrisponde a qualsiasi carattere)
- `%` (Corrisponde a qualsiasi sequenza di caratteri)

Operatori unitari

- `IS NULL`
- `IS NOT NULL`

Operatori matematici

Sono supportati gli operatori di addizione, sottrazione, moltiplicazione, divisione e modulo come segue:

- `+`
- `-`
- `*`
- `/`
- `%`

Precedenza degli operatori

Nella tabella seguente è indicata la precedenza degli operatori in ordine decrescente.

Operatore o elemento	Associatività	Campo obbligatorio
<code>-</code>	destra	meno unario
<code>*</code> , <code>/</code> , <code>%</code>	sinistra	moltiplicazione, divisione, modulo
<code>+</code> , <code>-</code>	sinistra	addizione, sottrazione
<code>IN</code>		appartenenza a un set

Operatore o elemento	Associatività	Campo obbligatorio
BETWEEN		limitazione a un intervallo
LIKE		criteri di ricerca di stringhe
<>		minore di, maggiore di
=	destra	uguaglianza, assegnazione
NOT	destra	negazione logica
AND	sinistra	congiunzione logica
OR	sinistra	disgiunzione logica

Parole chiave riservate

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Di seguito è riportato l'elenco delle parole chiave riservate per Amazon S3 Select. Sono inclusi nomi di funzioni, tipi di dati, operatori e così via, necessari per eseguire le espressioni SQL utilizzate per le query sul contenuto degli oggetti.

```
absolute  
action  
add
```

```
all
allocate
alter
and
any
are
as
asc
assertion
at
authorization
avg
bag
begin
between
bit
bit_length
blob
bool
boolean
both
by
cascade
cascaded
case
cast
catalog
char
char_length
character
character_length
check
clob
close
coalesce
collate
collation
column
commit
connect
connection
constraint
constraints
continue
```


convert
corresponding
count
create
cross
current
current_date
current_time
current_timestamp
current_user
cursor
date
day
deallocate
dec
decimal
declare
default
deferrable
deferred
delete
desc
describe
descriptor
diagnostics
disconnect
distinct
domain
double
drop
else
end
end-exec
escape
except
exception
exec
execute
exists
external
extract
false
fetch
first

float
for
foreign
found
from
full
get
global
go
goto
grant
group
having
hour
identity
immediate
in
indicator
initially
inner
input
insensitive
insert
int
integer
intersect
interval
into
is
isolation
join
key
language
last
leading
left
level
like
limit
list
local
lower
match
max

min
minute
missing
module
month
names
national
natural
nchar
next
no
not
null
nullif
numeric
octet_length
of
on
only
open
option
or
order
outer
output
overlaps
pad
partial
pivot
position
precision
prepare
preserve
primary
prior
privileges
procedure
public
read
real
references
relative
restrict
revoke

right
rollback
rows
schema
scroll
second
section
select
session
session_user
set
sexp
size
smallint
some
space
sql
sqlcode
sqlerror
sqlstate
string
struct
substring
sum
symbol
system_user
table
temporary
then
time
timestamp
timezone_hour
timezone_minute
to
trailing
transaction
translate
translation
trim
true
tuple
union
unique
unknown

```
unpivot  
update  
upper  
usage  
user  
using  
value  
values  
varchar  
varying  
view  
when  
whenever  
where  
with  
work  
write  
year  
zone
```

Funzioni SQL

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta le seguenti funzioni SQL.

Argomenti

- [Funzioni di aggregazione](#)
- [Funzioni condizionali](#)
- [Funzioni di conversione](#)
- [Funzioni di data](#)
- [Funzioni stringa](#)

Funzioni di aggregazione

 Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta le seguenti funzioni di aggregazione:

Funzione	Tipo di argomento	Tipo restituito
AVG(<i>espressio</i> <i>n</i>)	INT, FLOAT, DECIMAL	DECIMAL per un argomento INT, FLOAT un argomento in virgola mobile; in caso contrario, lo stesso tipo di dati dell'argomento.
COUNT	-	INT
MAX(<i>espressio</i> <i>n</i>)	INT, DECIMAL	Lo stesso tipo dell'argomento.
MIN(<i>espressio</i> <i>n</i>)	INT, DECIMAL	Lo stesso tipo dell'argomento.
SUM(<i>espressio</i> <i>n</i>)	INT, FLOAT, DOUBLE, DECIMAL	INT per un argomento INT, FLOAT un argomento in virgola mobile; in caso contrario, lo stesso tipo di

Funzione	Tipo di argomento	Tipo restituito
		dati dell'argomento.

SUM example

Per aggregare le dimensioni totali degli oggetti di una cartella in un [report S3 Inventory](#), usa un'espressione SUM.

Il seguente report S3 Inventory è un file CSV compresso con GZIP. Sono disponibili tre colonne.

- La prima colonna è il nome del bucket S3 (*DOC-EXAMPLE-BUCKET*) a cui è destinato il rapporto S3 Inventory.
- La seconda colonna è il nome della chiave dell'oggetto che identifica in modo univoco l'oggetto nel bucket.

Il valore *example-folder/* nella prima riga si riferisce alla cartella *example-folder*. Quando crei una cartella nel bucket in Amazon S3, S3 crea un oggetto con dimensioni pari a 0 byte con una chiave impostata sul nome della cartella fornito.

Il valore *example-folder/object1* nella seconda riga si riferisce all'oggetto *object1* nella cartella *example-folder*.

Il valore *example-folder/object2* nella terza riga si riferisce all'oggetto *object2* nella cartella *example-folder*.

Per ulteriori informazioni sulle cartelle S3, consulta [Organizzazione degli oggetti nella console di Amazon S3 utilizzando le cartelle](#).

- La terza colonna è la dimensione dell'oggetto in byte.

```
"DOC-EXAMPLE-BUCKET", "example-folder/", "0"  
"DOC-EXAMPLE-BUCKET", "example-folder/object1", "2011267"  
"DOC-EXAMPLE-BUCKET", "example-folder/object2", "1570024"
```

Per utilizzare un'espressione SUM per calcolare la dimensione totale della cartella *example-folder*, esegui la query SQL con Amazon S3 Select.

```
SELECT SUM(CAST(_3 as INT)) FROM s3object s WHERE _2 LIKE 'example-folder/%' AND _2 != 'example-folder/';
```

Risultato della query:

3581291

Funzioni condizionali

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta le seguenti funzioni condizionali.

Argomenti

- [CASE](#)
- [COALESCE](#)
- [NULLIF](#)

CASE

L'espressione CASE è un'espressione condizionale, simile alle istruzioni `if/then/else` presenti in altre lingue. CASE è utilizzata per specificare un risultato quando ci sono condizioni multiple. Esistono due tipi di espressioni CASE: semplici e ricercate.

Nelle espressioni CASE semplici, un'espressione viene confrontata con un valore. Quando viene trovata una corrispondenza, viene applicata l'azione specificata nella clausola `THEN`. Se non viene trovata una corrispondenza, viene applicata l'azione nella clausola `ELSE`.

Nelle espressioni CASE cercate, ogni CASE viene valutata in base a un'espressione booleana e l'istruzione CASE restituisce la prima CASE corrispondente. Se non vengono trovate corrispondenze CASE tra le clausole `WHEN`, viene restituita l'operazione nella clausola `ELSE`.

Sintassi

Note

Attualmente Amazon S3 Select non supporta ORDER BY o query che contengono nuove righe. Assicurati di utilizzare query senza interruzioni di riga.

Quella che segue è una semplice dichiarazione CASE che viene utilizzata per soddisfare le condizioni:

```
CASE expression WHEN value THEN result [WHEN...] [ELSE result] END
```

Di seguito è disponibile una dichiarazione CASE ricercata che viene utilizzata per valutare ogni condizione:

```
CASE WHEN boolean condition THEN result [WHEN ...] [ELSE result] END
```

Esempi

Note

Se utilizzi la console Amazon S3 per eseguire i seguenti esempi e il file CSV contiene una riga di intestazione, seleziona Exclude the first line of CSV data (Escludi la prima riga di dati CSV).

Esempio 1: utilizza una semplice espressione CASE per sostituire New York City con Big Apple in una query. Sostituire tutti gli altri nomi di città con other.

```
SELECT venuecity, CASE venuecity WHEN 'New York City' THEN 'Big Apple' ELSE 'other' END  
FROM S3object;
```

Risultato della query:

venuecity	case
Los Angeles	other
New York City	Big Apple

```
San Francisco    | other
Baltimore        | other
...
```

Esempio 2: utilizza un'espressione CASE con ricerca per assegnare numeri di gruppo in base al valore pricepaid per le vendite di biglietti singoli:

```
SELECT pricepaid, CASE WHEN CAST(pricepaid as FLOAT) < 10000 THEN 'group 1' WHEN
CAST(pricepaid as FLOAT) > 10000 THEN 'group 2' ELSE 'group 3' END FROM S3Object;
```

Risultato della query:

```
pricepaid | case
-----+-----
12624.00 | group 2
10000.00 | group 3
10000.00 | group 3
9996.00  | group 1
9988.00  | group 1
...
```

COALESCE

COALESCE valuta gli argomenti in ordine e restituisce il primo valore non sconosciuto, ovvero il primo non nullo o non mancante. Questa funzione non propaga valori null e mancanti.

Sintassi

```
COALESCE ( expression, expression, ... )
```

Parameters

expression

L'espressione di destinazione su cui viene eseguita la funzione.

Esempi

```
COALESCE(1)           -- 1
COALESCE(null)        -- null
COALESCE(null, null)  -- null
```

```
COALESCE(missing)          -- null
COALESCE(missing, missing) -- null
COALESCE(1, null)          -- 1
COALESCE(null, null, 1)    -- 1
COALESCE(null, 'string')   -- 'string'
COALESCE(missing, 1)       -- 1
```

NULLIF

Date due espressioni, NULLIF restituisce NULL se le due espressioni restituiscono lo stesso valore. In caso contrario, restituisce il risultato della valutazione della prima espressione.

Sintassi

```
NULLIF ( expression1, expression2 )
```

Parameters

expression1, *expression2*

Le espressioni di destinazione su cui viene eseguita la funzione.

Esempi

```
NULLIF(1, 1)          -- null
NULLIF(1, 2)          -- 1
NULLIF(1.0, 1)        -- null
NULLIF(1, '1')        -- 1
NULLIF([1], [1])      -- null
NULLIF(1, NULL)       -- 1
NULLIF(NULL, 1)       -- null
NULLIF(null, null)    -- null
NULLIF(missing, null) -- null
NULLIF(missing, missing) -- null
```

Funzioni di conversione

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta le seguenti funzioni di conversione.

Argomenti

- [CAST](#)

CAST

La funzione CAST converte un'entità, ad esempio un'espressione che restituisce un singolo valore, da un tipo a un altro.

Sintassi

```
CAST ( expression AS data_type )
```

Parameters

expression

Una combinazione di uno o più valori, operatori e funzioni SQL che restituisce un valore.

data_type

Il tipo di dati di destinazione, ad esempio INT, per il quale eseguire il cast dell'espressione. Per un elenco dei tipi di dati supportati, consulta [Tipi di dati](#).

Esempi

```
CAST('2007-04-05T14:30Z' AS TIMESTAMP)  
CAST(0.456 AS FLOAT)
```

Funzioni di data

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta le seguenti funzioni di data.

Argomenti

- [DATE_ADD](#)
- [DATE_DIFF](#)
- [EXTRACT](#)
- [TO_STRING](#)
- [TO_TIMESTAMP](#)
- [UTCNOW](#)

DATE_ADD

Dati una parte di data, una quantità e un timestamp, restituisce un timestamp aggiornato modificando la parte di data in base alla quantità.

Sintassi

```
DATE_ADD( date_part, quantity, timestamp )
```

Parameters

date_part

Specifica la parte di data da modificare. Può essere una delle seguenti:

- anno
- mese
- giorno
- ora
- minuti
- secondo

quantity

Il valore da applicare al timestamp aggiornato. I valori positivi per *quantity* vengono aggiunti a *date_part* del timestamp, mentre i valori negativi vengono sottratti.

timestamp

Il timestamp di destinazione su cui viene eseguita la funzione.

Esempi

```
DATE_ADD(year, 5, `2010-01-01T`)      -- 2015-01-01 (equivalent to
2015-01-01T)
DATE_ADD(month, 1, `2010T`)           -- 2010-02T (result will add precision
as necessary)
DATE_ADD(month, 13, `2010T`)          -- 2011-02T
DATE_ADD(day, -1, `2017-01-10T`)      -- 2017-01-09 (equivalent to
2017-01-09T)
DATE_ADD(hour, 1, `2017T`)            -- 2017-01-01T01:00-00:00
DATE_ADD(hour, 1, `2017-01-02T03:04Z`) -- 2017-01-02T04:04Z
DATE_ADD(minute, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:05:05.006Z
DATE_ADD(second, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:04:06.006Z
```

DATE_DIFF

Dati una parte di data e due timestamp validi, DATE_DIFF restituisce la differenza in parti di data. Il valore restituito è un numero intero negativo quando il valore *date_part* di *timestamp1* è maggiore del valore *date_part* di *timestamp2*. Il valore restituito è un numero intero positivo quando il valore *date_part* di *timestamp1* è minore del valore *date_part* di *timestamp2*.

Sintassi

```
DATE_DIFF( date_part, timestamp1, timestamp2 )
```

Parameters

date_part

Specifica la parte dei timestamp da confrontare. Per la definizione di *date_part*, consulta [DATE_ADD](#).

timestamp1

Il primo timestamp da confrontare.

timestamp2

Il secondo timestamp da confrontare.

Esempi

```
DATE_DIFF(year, `2010-01-01T`, `2011-01-01T`)      -- 1
```

```
DATE_DIFF(year, `2010T`, `2010-05T`) -- 4 (2010T is equivalent to
2010-01-01T00:00:00.000Z)
DATE_DIFF(month, `2010T`, `2011T`) -- 12
DATE_DIFF(month, `2011T`, `2010T`) -- -12
DATE_DIFF(day, `2010-01-01T23:00`, `2010-01-02T01:00`) -- 0 (need to be at least 24h
apart to be 1 day apart)
```

EXTRACT

Dati una parte di data e un timestamp, EXTRACT restituisce il valore della parte di data del timestamp.

Sintassi

```
EXTRACT( date_part FROM timestamp )
```

Parameters

date_part

Specifica la parte dei timestamp da estrarre. Può essere una delle seguenti:

- YEAR
- MONTH
- DAY
- HOUR
- MINUTE
- SECOND
- TIMEZONE_HOUR
- TIMEZONE_MINUTE

timestamp

Il timestamp di destinazione su cui viene eseguita la funzione.

Esempi

```
EXTRACT(YEAR FROM `2010-01-01T`) -- 2010
EXTRACT(MONTH FROM `2010T`) -- 1 (equivalent to
2010-01-01T00:00:00.000Z)
EXTRACT(MONTH FROM `2010-10T`) -- 10
EXTRACT(HOUR FROM `2017-01-02T03:04:05+07:08`) -- 3
```

```
EXTRACT(MINUTE FROM `2017-01-02T03:04:05+07:08`)      -- 4
EXTRACT(TIMEZONE_HOUR FROM `2017-01-02T03:04:05+07:08`)  -- 7
EXTRACT(TIMEZONE_MINUTE FROM `2017-01-02T03:04:05+07:08`) -- 8
```

TO_STRING

Dati un timestamp e un pattern di formato, TO_STRING restituisce una rappresentazione in formato stringa del timestamp fornito nel formato specificato.

Sintassi

```
TO_STRING ( timestamp time_format_pattern )
```

Parameters

timestamp

Il timestamp di destinazione su cui viene eseguita la funzione.

time_format_pattern

Una stringa che ha le seguenti interpretazioni di caratteri speciali.

Formato	Esempio	Descrizione
yy	69	Anno a 2 cifre
y	1969	Anno a 4 cifre
yyyy	1969	Zero-padded anno a 4 cifre
M	1	Mese dell'anno
MM	01	Zero-padd ed mese dell'anno
MMM	Jan	Nome abbreviat

Formato	Esempio	Descrizione
		o del mese dell'anno
MMMM	January	Nome completo del mese dell'anno
MMMMM	J	Prima lettera del mese dell'anno (NOTA: questo formato non è utilizzabile con la funzione TO_TIMESTAMP .)
d	2	Giorno del mese (1-31)
dd	02	Zero-padded giorno del mese (01-31)
a	AM	AM o PM
h	3	Ora del giorno (1-12)
hh	03	Zero-padded ora del giorno (01-12)
H	3	Ora del giorno (0-23)

Formato	Esempio	Descrizione
HH	03	Zero-padded ora del giorno (00-23)
m	4	Minuto dell'ora (0-59)
mm	04	Zero-padded minuto dell'ora (00-59)
s	5	Secondo del minuto (0-59)
ss	05	Zero-padded secondo del minuto (00-59)
S	0	Frazione di secondo (precisione: 0,1, intervallo: 0,0-0,9)
SS	6	Frazione di secondo (precisione: 0,01, intervallo: 0,0-0,99)
SSS	60	Frazione di secondo (precisione: 0,001, intervallo: 0,0-0,999)
...	...	...

Formato	Esempio	Descrizione
SSSSSSSSS	60000000	Frazione di secondo (precisione massima: 1 nanosecondo, intervallo: 0,0-0,99999999)
n	60000000	Nano di secondo
X	+07 o Z	Offset in ore o Z se l'offset è 0
XX o XXXX	+0700 o Z	Offset in ore e minuti o Z se l'offset è 0
XXX o XXXXX	+07:00 o Z	Offset in ore e minuti o Z se l'offset è 0
x	7	Offset in ore
xx o xxxx	700	Offset in ore e minuti
xxx o xxxxx	+07:00	Offset in ore e minuti

Esempi

TO_STRING(`1969-07-20T20:18Z`, 'MMMM d, y')

TO_STRING(`1969-07-20T20:18Z`, 'MMM d, yyyy')

-- "July 20, 1969"

-- "Jul 20, 1969"

```

TO_STRING(`1969-07-20T20:18Z`, 'M-d-yy')           -- "7-20-69"
TO_STRING(`1969-07-20T20:18Z`, 'MM-d-y')          -- "07-20-1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMMM d, y h:m a')  -- "July 20, 1969 8:18 PM"
TO_STRING(`1969-07-20T20:18Z`, 'y-MM-dd''T''H:m:ssX') --
"1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00Z`, 'y-MM-dd''T''H:m:ssX') --
"1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXX') --
"1969-07-20T20:18:00+0800"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXXX') --
"1969-07-20T20:18:00+08:00"

```

TO_TIMESTAMP

Data una stringa, TO_TIMESTAMP la converte in un timestamp. TO_TIMESTAMP è l'operazione inversa di TO_STRING.

Sintassi

```
TO_TIMESTAMP ( string )
```

Parameters

string

La stringa di destinazione su cui viene eseguita la funzione.

Esempi

```

TO_TIMESTAMP('2007T')           -- `2007T`
TO_TIMESTAMP('2007-02-23T12:14:33.079-08:00') -- `2007-02-23T12:14:33.079-08:00`

```

UTCNOW

Restituisce l'ora corrente in UTC come timestamp.

Sintassi

```
UTCNOW()
```

Parameters

UTCNOW non prende parametri.

Esempi

```
UTCNOW() -- 2017-10-13T16:02:11.123Z
```

Funzioni stringa

Important

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#)

Amazon S3 Select supporta le seguenti funzioni di stringa.

Argomenti

- [CHAR_LENGTH, CHARACTER_LENGTH](#)
- [LOWER](#)
- [SUBSTRING](#)
- [TRIM](#)
- [UPPER](#)

CHAR_LENGTH, CHARACTER_LENGTH

CHAR_LENGTH (o CHARACTER_LENGTH) conta il numero di caratteri della stringa specificata.

Note

CHAR_LENGTH e CHARACTER_LENGTH sono sinonimi.

Sintassi

```
CHAR_LENGTH ( string )
```

Parameters

string

La stringa di destinazione su cui viene eseguita la funzione.

Esempi

```
CHAR_LENGTH(' ')      -- 0
CHAR_LENGTH('abcdefg') -- 7
```

LOWER

Data una stringa, LOWER converte tutti i caratteri maiuscoli in minuscoli. I caratteri non maiuscoli rimangono invariati.

Sintassi

```
LOWER ( string )
```

Parameters

string

La stringa di destinazione su cui viene eseguita la funzione.

Esempi

```
LOWER('AbCdEfG!@#') -- 'abcdefg!@#'
```

SUBSTRING

Dati una stringa, un indice iniziale e, facoltativamente, una lunghezza, SUBSTRING restituisce la sottostringa dall'indice iniziale fino alla fine della stringa oppure fino alla lunghezza specificata.

Note

Il primo carattere della stringa di input ha indice 1.

- Se `start` è < 1 , senza una lunghezza specificata allora viene impostato su 1.
- Se `start` è < 1 , con una lunghezza specificata, allora la posizione dell'indice viene impostata su `start + length - 1`.
- Se `start + length - 1 < 0` allora viene restituita una stringa vuota.
- Se `start + length - 1 >= 0` allora viene restituita la sottostringa che inizia dall'indice 1 con lunghezza `start + length - 1`.

Sintassi

```
SUBSTRING( string FROM start [ FOR length ] )
```

Parameters

string

La stringa di destinazione su cui viene eseguita la funzione.

start

La posizione iniziale della stringa.

length

La lunghezza della sottostringa da restituire. Se non è presente, procede fino alla fine della stringa.

Esempi

```
SUBSTRING("123456789", 0)      -- "123456789"
SUBSTRING("123456789", 1)      -- "123456789"
SUBSTRING("123456789", 2)      -- "23456789"
SUBSTRING("123456789", -4)     -- "123456789"
SUBSTRING("123456789", 0, 999) -- "123456789"
SUBSTRING("123456789", 1, 5)   -- "12345"
```

TRIM

Taglia i caratteri iniziali o finali di una stringa. Il carattere di default da rimuovere è uno spazio (' ').

Sintassi

```
TRIM ( [[LEADING | TRAILING | BOTH remove_chars] FROM] string )
```

Parameters

string

La stringa di destinazione su cui viene eseguita la funzione.

LEADING | TRAILING | BOTH

Il parametro indica se tagliare i caratteri iniziali o finali o entrambi.

remove_chars

Il set di caratteri da rimuovere. *remove_chars* può essere una stringa con lunghezza >

1. Questa funzione restituisce la stringa da cui sono stati rimossi i caratteri specificati in *remove_chars* trovati all'inizio o alla fine della stringa.

Esempi

```
TRIM('      foobar      ') -- 'foobar'
TRIM('      \tfoobar\t      ') -- '\tfoobar\t'
TRIM(LEADING FROM '      foobar      ') -- 'foobar      '
TRIM(TRAILING FROM '      foobar      ') -- '      foobar'
TRIM(BOTH FROM '      foobar      ') -- 'foobar'
TRIM(BOTH '12' FROM '1112211foobar22211122') -- 'foobar'
```

UPPER

Data una stringa, UPPER converte tutti i caratteri minuscoli in maiuscoli. I caratteri non minuscoli rimangono invariati.

Sintassi

```
UPPER ( string )
```

Parameters

string

La stringa di destinazione su cui viene eseguita la funzione.

Esempi

```
UPPER('AbCdEfG!@#') -- 'ABCDEFG!@#'
```

Operazioni con i bucket di directory

I bucket di directory organizzano i dati in modo gerarchico in directory, a differenza della struttura di archiviazione piatta dei bucket per uso generico. Non ci sono limiti di prefisso per i bucket di directory e le singole directory possono scalare orizzontalmente.

Puoi creare fino a 100 bucket di directory in ciascuno dei tuoi Account AWS, senza limiti al numero di oggetti che puoi archiviare in un bucket. La quota del bucket viene applicata a ciascuna regione nell'Account AWS. Se la tua applicazione richiede un aumento di questo limite, contatta Supporto.

Important

I bucket di directory presenti in zone di disponibilità che non hanno attività di richiesta per un periodo di almeno 90 giorni passano allo stato inattivo. In uno stato inattivo, un bucket di directory è temporaneamente inaccessibile per letture e scritture. I bucket inattivi mantengono tutta l'archiviazione, i metadati degli oggetti e i metadati dei bucket. I costi di archiviazione esistenti si applicano ai bucket inattivi. Se si effettua una richiesta di accesso a un bucket inattivo, il bucket passa allo stato attivo, in genere entro pochi minuti. Durante questo periodo di transizione, le letture e le scritture restituiscono un codice di errore HTTP 503 (Service Unavailable). Questo comportamento non si applica ai bucket nelle zone locali.

Sono disponibili diversi tipi di bucket Amazon S3. Prima di creare un bucket, accertati di scegliere il tipo di bucket più adatto ai requisiti dell'applicazione e delle prestazioni. Per ulteriori informazioni sui vari tipi di bucket e sui casi d'uso appropriati per ogni tipo, consulta [Bucket](#).

I seguenti argomenti forniscono informazioni sui bucket di directory. Per ulteriori informazioni sui bucket per uso generico, consulta [Panoramica dei bucket per uso generico](#).

Per ulteriori informazioni sui bucket di directory, consulta i seguenti argomenti.

- [Nomi dei bucket di directory](#)
- [Directory](#)
- [Nomi delle chiavi](#)
- [Gestione degli accessi](#)

Nomi dei bucket di directory

Il nome di un bucket di directory è composto da un nome di base fornito dall'utente e da un suffisso che contiene l'ID della zona (zona di disponibilità o zona locale) in cui si trova il bucket. I nomi dei bucket di directory devono utilizzare il seguente formato e rispettare le regole di denominazione dei bucket di directory:

```
bucket-base-name--zone-id--x-s3
```

Ad esempio, il seguente nome del bucket di directory contiene l'ID zona di disponibilità `usw2-az1`:

```
bucket-base-name--usw2-az1--x-s3
```

Per ulteriori informazioni, consulta [Regole di denominazione dei bucket di directory](#).

Directory

I bucket di directory organizzano i dati in modo gerarchico in directory, a differenza della struttura di ordinamento piatta dei bucket per uso generico.

Con uno spazio dei nomi gerarchico, il delimitatore nella chiave dell'oggetto è importante. Il solo delimitatore supportato è una barra (/). Le directory sono determinate dai limiti dei delimitatori. Ad esempio, la chiave dell'oggetto `dir1/dir2/file1.txt` comporta che le directory `dir1/` e `dir2/` vengano create automaticamente e che l'oggetto `file1.txt` venga aggiunto alla directory `/dir2` nel percorso `dir1/dir2/file1.txt`.

Il modello di indicizzazione del bucket di directory restituisce risultati non ordinati per l'operazione API `ListObjectsV2`. Se è necessario limitare i risultati a una sottosezione del bucket, è possibile specificare un percorso di sottodirectory nel parametro `prefix`, ad esempio `prefix=dir1/`.

Nomi delle chiavi

Per i bucket di directory, le sottodirectory comuni a più chiavi oggetto vengono create con la prima chiave dell'oggetto. Le chiavi oggetto aggiuntive per la stessa sottodirectory utilizzano la sottodirectory creata in precedenza. Questo modello offre flessibilità nella scelta delle chiavi degli oggetti più adatte all'applicazione, con uguale supporto per directory sparse e dense.

Gestione degli accessi

Nei bucket di directory, tutte le impostazioni Blocco dell'accesso pubblico S3 sono abilitate per impostazione predefinita a livello di bucket. Proprietà dell'oggetto S3 è impostata su Proprietario del bucket applicato e le liste di controllo degli accessi (ACL) sono disabilitate. Queste impostazioni non possono essere modificate.

Per impostazione predefinita, gli utenti non hanno i permessi per i bucket di directory. Per concedere le autorizzazioni di accesso per i bucket di directory, puoi utilizzare IAM per creare utenti, gruppi o ruoli e collegare le autorizzazioni a tali identità. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).

È possibile controllare l'accesso ai bucket di directory anche tramite punti di accesso. Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. I punti di accesso sono nomi host univoci creati per applicare autorizzazioni e controlli di rete distinti per tutte le richieste effettuate tramite un punto di accesso. Per ulteriori informazioni, consulta [Gestione dell'accesso ai set di dati condivisi in bucket di directory con punti di accesso](#).

Quote dei bucket di directory

Le quote, chiamate anche limiti, rappresentano il numero massimo di risorse o di operazioni di servizio consentite per il tuo Account AWS. Di seguito sono riportate le quote per i bucket di directory. Per ulteriori informazioni sulle quote di Amazon S3, consulta [Quote di Amazon S3](#).

Nome	Predefinita	Adattabile	Description
Bucks di directory	Ogni account: 100	Sì	Il numero di bucket di directory Amazon S3 che puoi creare in un account.
TPS di lettura per bucket di directory	Ogni bucket di directory: fino a 200.000 TPS di lettura	Per richiedere un aumento della quota, contatta il Supporto .	Il numero di GET/HEAD richieste al secondo per bucket di directory.

Nome	Predefinita	Adattabile	Description
TPS di scrittura per bucket di directory	Ogni bucket di directory: fino a 100.000 TPS di scrittura	Per richiedere un aumento della quota, contatta il Supporto .	Il numero di PUT/DELETE richieste al secondo per bucket di directory.

Creazione e utilizzo di bucket di directory

Per ulteriori informazioni sull'utilizzo di bucket di directory, consulta gli argomenti seguenti.

- [Casi d'uso dei bucket di directory](#)
- [Differenze per i bucket di directory](#)
- [Collegamento in rete per i bucket di directory](#)
- [Regole di denominazione dei bucket di directory](#)
- [Visualizzazione delle proprietà dei bucket di directory](#)
- [Gestione delle policy dei bucket di directory](#)
- [Svuotamento di un bucket di directory](#)
- [Eliminazione di un bucket di directory](#)
- [Elencare i bucket di directory](#)
- [Determinazione del fatto che sia possibile accedere a un bucket di directory](#)
- [Utilizzo di oggetti in un bucket di directory](#)
- [Sicurezza per i bucket di directory](#)
- [Gestione dell'accesso ai set di dati condivisi in bucket di directory con punti di accesso](#)
- [Ottimizzazione delle prestazioni del bucket della directory](#)
- [Sviluppo con i bucket di directory](#)
- [Utilizzo di tag con i bucket di directory S3](#)
- [Test di resilienza in S3 Express One Zone](#)

Casi d'uso dei bucket di directory

I bucket di directory supportano la creazione di bucket nei seguenti tipi di posizione del bucket: zona di disponibilità o zona locale.

Per i casi d'uso a bassa latenza, è possibile creare un bucket di directory in una singola zona di disponibilità per archiviare i dati. I bucket di directory nelle zone di disponibilità supportano la classe di storage S3 Express One Zone. La classe di storage S3 Express One Zone è consigliata se l'applicazione è sensibile alle prestazioni e beneficia di latenze a una cifra al millisecondo PUT e GET. Per saperne di più sulla creazione di bucket di directory nelle zone di disponibilità, consulta [Carichi di lavoro ad alte prestazioni](#).

Per i casi d'uso relativi alla residenza dei dati, puoi creare un bucket di directory in un'unica zona locale AWS dedicata (DLZ) per archiviare i dati. I bucket di directory nelle zone locali supportano la classe di archiviazione S3 One Zone-Infrequent Access (S3 One;). Zone-IA Z-IA Per saperne di più sulla creazione di bucket di directory in Zone locali, consulta [Carichi di lavoro di residenza dei dati](#).

Argomenti

- [Carichi di lavoro ad alte prestazioni](#)
- [Carichi di lavoro di residenza dei dati](#)

Carichi di lavoro ad alte prestazioni

S3 Express One Zone

È possibile utilizzare Amazon S3 Express One Zone per carichi di lavoro ad alte prestazioni. S3 Express One Zone è la prima classe di storage S3 in cui è possibile selezionare un'unica zona di disponibilità con la possibilità di co-localizzare lo storage di oggetti con le risorse di calcolo, per ottenere la massima velocità di accesso possibile. Gli oggetti in S3 Express One Zone sono memorizzati in bucket di directory situati nelle zone di disponibilità. Per ulteriori informazioni sui bucket di directory, consulta [Bucket di directory](#).

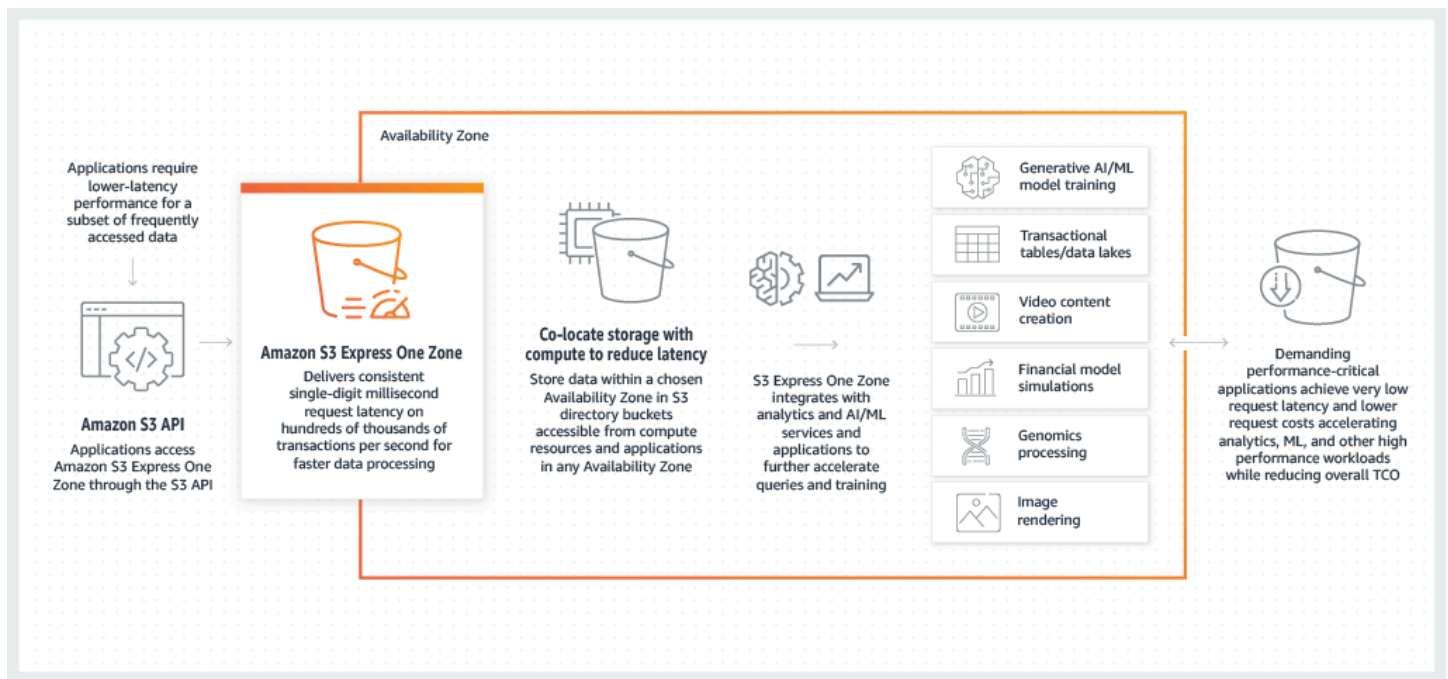
Amazon S3 Express One Zone è una classe di archiviazione Amazon S3 a zona singola ad alte prestazioni, creata appositamente per fornire un accesso ai dati coerente di pochi millisecondi per le applicazioni sensibili alla latenza. S3 Express One Zone è la classe di storage cloud-object a più bassa latenza oggi disponibile, con velocità di accesso ai dati fino a 10 volte superiori e con costi di richiesta inferiori del 50% rispetto a S3 Standard. Le applicazioni possono beneficiare

immediatamente di un completamento delle richieste fino a un ordine di grandezza più rapido. S3 Express One Zone offre un'elasticità delle prestazioni simile a quella delle altre classi di storage S3. S3 Express One Zone è utilizzato per i carichi di lavoro o le applicazioni critiche dal punto di vista delle prestazioni che richiedono una latenza costante a una cifra al millisecondo.

Come per le altre classi di storage Amazon S3, non è necessario pianificare o fornire in anticipo i requisiti di capacità o di throughput. È possibile scalare lo storage verso l'alto o verso il basso, in base alle esigenze, e accedere ai dati tramite l'API di Amazon S3.

La classe di storage Amazon S3 Express One Zone è progettata per una disponibilità del 99,95% all'interno di una singola zona di disponibilità ed è supportata dall'[Accordo sul livello di servizio di Amazon S3 Service](#). Con S3 Express One Zone, i dati vengono archiviati in modo ridondante su più dispositivi all'interno di un'unica zona di disponibilità. S3 Express One Zone è progettata per gestire guasti simultanei dei dispositivi rilevando e riparando rapidamente l'eventuale ridondanza persa. Se il dispositivo esistente rileva un guasto, S3 Express One Zone sposta automaticamente le richieste in nuovi dispositivi all'interno di una zona di disponibilità. Questa ridondanza garantisce l'accesso ininterrotto ai dati all'interno di una zona di disponibilità.

S3 Express One Zone è ideale per qualsiasi applicazione in cui è importante ridurre al minimo la latenza richiesta per accedere a un oggetto. Tali applicazioni possono essere flussi di processo interattivi, come l'editing video, in cui i professionisti della creatività hanno bisogno di un accesso reattivo ai contenuti dalle loro interfacce utente. S3 Express One Zone beneficia, inoltre, di carichi di lavoro di analisi e machine learning che hanno requisiti di reattività simili ai relativi dati, in particolare carichi di lavoro con molti accessi più piccoli o un numero elevato di accessi casuali. S3 Express One Zone può essere utilizzato con altri Servizi AWS per supportare carichi di lavoro di analisi, intelligenza artificiale e machine learning (AI/ML), come Amazon EMR, Amazon AI e Amazon Athena. SageMaker



Per i bucket di directory che utilizzano la classe di storage S3 Express One Zone, i dati vengono archiviati su più dispositivi all'interno di una singola zona di disponibilità, ma non vengono archiviati in modo ridondante tra le varie zone di disponibilità. Quando crei un bucket di directory per utilizzare la classe di storage S3 Express One Zone, ti consigliamo di specificare una Regione AWS e una zona di disponibilità locali alle tue istanze di calcolo Amazon EC2, Amazon Elastic Kubernetes Service o Amazon Elastic Container Service (Amazon ECS) per ottimizzare le prestazioni.

Quando si utilizza S3 Express One Zone, è possibile interagire con il bucket della directory in un cloud privato virtuale (VPC) utilizzando un endpoint VPC gateway. Con un endpoint gateway, è possibile accedere ai bucket della directory S3 Express One Zone dal VPC senza un gateway Internet o un dispositivo NAT per il VPC e senza costi aggiuntivi.

Con i bucket di directory è possibile utilizzare molte delle stesse operazioni e funzioni dell'API Amazon S3 che si utilizzano con i bucket per uso generico e altre classi di storage. Questi includono Mountpoint per Amazon S3, crittografia lato server con chiavi gestite Amazon S3 (SSE-S3), crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS), S3 Batch Operations e S3 Block Public Access. Puoi accedere a S3 Express One Zone utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli SDK e l'API REST di Amazon S3. AWS

Per ulteriori informazioni su S3 Express One Zone, consulta i seguenti argomenti.

- [Panoramica di](#)
- [Funzionalità di S3 Express One Zone](#)

- [Servizi correlati](#)
- [Fasi successive](#)

Panoramica di

Per ottimizzare le prestazioni e ridurre la latenza, S3 Express One Zone introduce i seguenti nuovi concetti.

Zone di disponibilità

La classe di storage Amazon S3 Express One Zone è progettata per una disponibilità del 99,95% all'interno di una singola zona di disponibilità ed è supportata dall'[Accordo sul livello di servizio di Amazon S3 Service](#). Con S3 Express One Zone, i dati vengono archiviati in modo ridondante su più dispositivi all'interno di un'unica zona di disponibilità. S3 Express One Zone è progettata per gestire guasti simultanei dei dispositivi rilevando e riparando rapidamente l'eventuale ridondanza persa. Se il dispositivo esistente rileva un guasto, S3 Express One Zone sposta automaticamente le richieste in nuovi dispositivi all'interno di una zona di disponibilità. Questa ridondanza garantisce l'accesso ininterrotto ai dati all'interno di una zona di disponibilità.

Una zona di disponibilità è uno o più data center discreti con alimentazione, rete e connettività ridondanti in Regione AWS. Quando crei un bucket di directory, scegli la zona di disponibilità e Regione AWS dove verrà posizionato il bucket.

Zona di disponibilità singola

Quando si crea un bucket di directory, si sceglie la zona di disponibilità e la Regione AWS.

I bucket di directory utilizzano la classe di archiviazione S3 Express One Zone, creata per essere utilizzata da applicazioni sensibili alle prestazioni. S3 Express One Zone è la prima classe di archiviazione S3 in cui è possibile selezionare una singola zona di disponibilità con la possibilità di co-ubicare l'archiviazione di oggetti con le risorse di calcolo, che offre la massima velocità di accesso possibile.

Con S3 Express One Zone, i dati vengono archiviati in modo ridondante su più dispositivi all'interno di una singola zona di disponibilità. S3 Express One Zone è progettato per una disponibilità del 99,95% all'interno di una singola zona di disponibilità ed è supportato dall'[Accordo sul livello di servizio di Amazon S3](#). Per ulteriori informazioni, consulta [Zone di disponibilità](#)

Endpoint ed endpoint VPC del gateway

Bucket-management Le operazioni API per i bucket di directory sono disponibili tramite un endpoint regionale e sono denominate operazioni API per endpoint regionali. Esempi di operazioni API degli endpoint regionali sono `CreateBucket` e `DeleteBucket`. Dopo aver creato un bucket di directory, puoi utilizzare le operazioni API degli endpoint zionali per caricare e gestire gli oggetti nel bucket di directory. Le operazioni API degli endpoint zionali sono disponibili tramite un endpoint zonale. Esempi di operazioni API degli endpoint zionali sono `PutObject` e `CopyObject`.

È possibile accedere a S3 Express One Zone dalla propria VPC utilizzando endpoint VPC gateway. Dopo aver creato un endpoint gateway, è possibile aggiungerlo come destinazione nella tabella di routing per il traffico destinato dalla VPC alla S3 Express One Zone. Analogamente ad Amazon S3, l'utilizzo di endpoint del gateway non comporta costi supplementari. Per ulteriori informazioni su come configurare gli endpoint VPC del gateway, consulta [Collegamento in rete per i bucket di directory](#)

Session-based autorizzazione

Con S3 Express One Zone, l'autenticazione e l'autorizzazione delle richieste avviene attraverso un nuovo meccanismo basato sulla sessione, ottimizzato per fornire la latenza più bassa. Puoi utilizzare `CreateSession` per richiedere credenziali temporanee che forniscono un accesso a bassa latenza al bucket. Queste credenziali temporanee sono definite per un bucket di directory S3 specifico. I token di sessione vengono utilizzati solo con le operazioni di zona (a livello di oggetto) (con l'eccezione di [CopyObject](#)). Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint di zona con CreateSession](#).

Gli AWS SDK [supportati per S3 Express One Zone](#) gestiscono l'avvio e l'aggiornamento delle sessioni per tuo conto. Per proteggere le sessioni, le credenziali di sicurezza temporanee scadono dopo 5 minuti. Dopo aver scaricato e installato gli AWS SDK e configurato le autorizzazioni AWS Identity and Access Management (IAM) necessarie, puoi iniziare immediatamente a utilizzare le operazioni API.

Funzionalità di S3 Express One Zone

Le seguenti funzionalità S3 sono disponibili per S3 Express One Zone. Per un elenco completo delle operazioni API supportate e delle funzioni non supportate, consulta [Differenze per i bucket di directory](#).

Gestione degli accessi e sicurezza

È possibile utilizzare le seguenti funzioni per verificare e gestire gli accessi. Per impostazione predefinita, i bucket di directory sono privati e vi possono accedere solo gli utenti a cui è stato

esplicitamente concesso l'accesso. A differenza dei bucket per uso generico, che possono impostare il limite di controllo dell'accesso a livello di bucket, prefisso o tag dell'oggetto, il limite di controllo dell'accesso per i bucket di directory viene impostato solo a livello di bucket. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).

- [Blocco dell'accesso pubblico S3](#) - Tutte le impostazioni di Blocco dell'accesso pubblico S3 sono abilitate per impostazione predefinita a livello di bucket. Questa impostazione predefinita non può essere modificata.
- [Proprietà degli oggetti S3](#) (proprietario del bucket applicato per impostazione predefinita) - Le liste di controllo degli accessi (ACL) non sono supportate per i bucket della directory. I bucket della directory utilizzano automaticamente l'impostazione del proprietario del bucket per la proprietà degli oggetti S3. L'applicazione del proprietario del bucket significa che le ACL sono disabilitate e che il proprietario del bucket è automaticamente proprietario e ha il pieno controllo su ogni oggetto del bucket. Questa impostazione predefinita non può essere modificata.
- [AWS Identity and Access Management \(IAM\)](#): IAM ti aiuta a controllare in modo sicuro l'accesso ai tuoi bucket di directory. È possibile utilizzare IAM per concedere l'accesso alle operazioni API di gestione dei bucket (regionali) e alle operazioni API di gestione degli oggetti (di zona) tramite l'azione `s3express:CreateSession`. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#). A differenza delle azioni di gestione degli oggetti, le azioni di gestione dei bucket non possono essere multi-account. Solo il proprietario del bucket può eseguire tali azioni.
- [Bucket policy](#): utilizza il linguaggio delle IAM-based policy per configurare le autorizzazioni basate sulle risorse per i tuoi bucket di directory. È inoltre possibile utilizzare IAM per controllare l'accesso all'operazione API `CreateSession`, che consente di utilizzare le operazioni API di zona o di gestione degli oggetti. È possibile concedere l'accesso allo stesso account o multi-account alle operazioni API di zona. Per ulteriori informazioni sulle autorizzazioni e le policy di S3 Express One Zone, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).
- [IAM Access Analyzer for S3](#) - Valuta e monitora le policy di accesso per assicurarsi che forniscano solo l'accesso previsto alle risorse S3.

Registrazione di log e monitoraggio

S3 Express One Zone utilizza i seguenti strumenti di registrazione e monitoraggio S3 che possono essere utilizzati per monitorare e controllare l'utilizzo delle risorse:

- [CloudWatch Metriche Amazon](#): monitora le tue AWS risorse e le tue applicazioni raccogliendo e monitorando le metriche. CloudWatch S3 Express One Zone utilizza lo stesso CloudWatch namespace delle altre classi di storage Amazon S3 (AWS/S3) e supporta metriche di archiviazione giornaliere per i bucket di directory: e. BucketSizeBytes NumberOfObjects Per ulteriori informazioni, consulta [Metriche di monitoraggio con Amazon CloudWatch](#).
- [AWS CloudTrail logs](#): AWS CloudTrail è una soluzione Servizio AWS che ti aiuta a implementare il controllo operativo e dei rischi, la governance e la conformità della tua azienda registrando le azioni intraprese Account AWS da un utente, un ruolo o un. Servizio AWS Per S3 Express One Zone, CloudTrail acquisisce le operazioni API regionali degli endpoint (ad esempio, CreateBucket e PutBucketPolicy) come eventi di gestione e le operazioni API zonali (ad esempio, GetObject e PutObject) come eventi di dati. Questi eventi includono le azioni intraprese nelle operazioni Console di gestione AWS, AWS Command Line Interface (AWS CLI), AWS SDK e API. AWS Per ulteriori informazioni, consulta [Registrazione con AWS CloudTrail S3 Express One Zone](#).

Note

I log di accesso al server Amazon S3 non sono supportati da S3 Express One Zone.

Gestione degli oggetti

Puoi gestire lo storage di oggetti utilizzando la console Amazon S3, gli AWS SDK e. AWS CLI Le seguenti funzioni sono disponibili per la gestione degli oggetti con S3 Express One Zone:

- [S3 Batch Operations](#): utilizza Batch Operations per eseguire operazioni in blocco su oggetti nei bucket di directory, ad esempio la funzione Copy and Invoke. AWS Lambda Ad esempio, puoi utilizzare Operazioni in batch per copiare oggetti tra bucket di directory e bucket per uso generico. Con Batch Operations, puoi gestire miliardi di oggetti su larga scala con una singola richiesta S3 utilizzando gli AWS SDK AWS CLI o con pochi clic nella console Amazon S3.
- [Importa](#): dopo aver creato un bucket di directory, puoi popolarlo con oggetti utilizzando la funzionalità di importazione nella console Amazon S3. L'importazione è un metodo ottimizzato di creazione di processi Operazioni in batch per copiare oggetti da bucket per uso generico in bucket di directory.

AWS SDK e librerie client

Puoi gestire il tuo object storage utilizzando gli AWS SDK e le librerie client.

- [Mountpoint per Amazon S3](#) - Mountpoint per Amazon S3 è un client di file open source che offre un accesso con throughput elevato, riducendo i costi di calcolo per i data lake su Amazon S3. Mountpoint per Amazon S3 traduce le chiamate API del file system locale in chiamate API di oggetti S3 come GET e LIST. È ideale per i carichi di lavoro di data lake ad alta intensità di lettura che elaborano petabyte di dati e necessitano dell'elevato throughput elastico fornito da Amazon S3 per aumentare e ridurre verticalmente le risorse su migliaia di istanze.
- [S3A](#) - S3A è un'interfaccia raccomandata compatibile con Hadoop per l'accesso agli archivi di dati in Amazon S3. S3A sostituisce il client del file system S3N Hadoop.
- [PyTorch on AWS](#) — PyTorch on AWS è un framework di deep learning open source che semplifica lo sviluppo di modelli di machine learning e la loro distribuzione in produzione.
- [AWS SDK](#): puoi utilizzare gli AWS SDK per sviluppare applicazioni con Amazon S3. Gli AWS SDK semplificano le attività di programmazione racchiudendo l'API REST di Amazon S3 sottostante. Per ulteriori informazioni sull'utilizzo degli AWS SDK con S3 Express One Zone, consulta [the section called "AWS SDK"](#)

Crittografia e protezione dei dati

Gli oggetti in S3 Express One Zone vengono crittografati automaticamente tramite crittografia lato server con chiavi gestite da Amazon S3 (`SSE-S3`). S3 Express One Zone supporta anche la crittografia lato server con chiavi (`SSE-KMS`). AWS Key Management Service (AWS KMS) `SSE-KMS` S3 Express One Zone non supporta la crittografia lato server con chiavi di crittografia fornite dal cliente (`SSE-C`) o la crittografia lato server a doppio livello con (`DSSE-KMS`). AWS KMS keys `DSSE-KMS` Per ulteriori informazioni, consulta [Protezione e crittografia dei dati](#).

S3 Express One Zone offre la possibilità di scegliere l'algoritmo di checksum utilizzato per convalidare i dati durante il caricamento o il download. È possibile selezionare uno dei seguenti algoritmi di controllo dell'integrità dei dati Secure Hash Algorithms (SHA) o Cyclic Redundancy Check (CRC): CRC32, CRC32C e SHA-1 SHA-256 MD5-based i checksum non sono supportati con la classe di storage S3 Express One Zone.

Per ulteriori informazioni, consulta [Best practice per il checksum S3 aggiuntivo](#).

AWS Signature versione 4 (SigV4)

S3 Express One Zone utilizza AWS la versione Signature 4 (SigV4). SigV4 è un protocollo di firma utilizzato per autenticare le richieste ad Amazon S3 tramite HTTPS. S3 Express One Zone firma le richieste utilizzando AWS Sigv4. Per ulteriori informazioni, consulta [Authenticating Requests \(AWS Signature Version 4\)](#) nell'Amazon Simple Storage Service API Reference.

Forte coerenza

S3 Express One Zone fornisce una forte coerenza di lettura e scrittura per le richieste PUT e DELETE di oggetti nei bucket della directory in ogni Regione AWS. Per ulteriori informazioni, consulta [Modello di consistenza dati Amazon S3](#).

Servizi correlati

Puoi utilizzare quanto segue Servizi AWS con la classe di storage S3 Express One Zone per supportare il tuo caso d'uso specifico a bassa latenza.

- [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) - Amazon EC2 fornisce capacità di calcolo sicura e scalabile in Cloud AWS. L'utilizzo Amazon EC2 riduce la necessità di investimenti anticipati in hardware e ti permette di sviluppare e distribuire più rapidamente le applicazioni. Puoi utilizzare Amazon EC2 per avviare il numero di server virtuali necessari, configurare la sicurezza e i servizi di rete, nonché gestire l'archiviazione.
- [AWS Lambda](#): Lambda è un servizio di calcolo che consente di eseguire il codice senza provisioning o gestire server. Si configurano le impostazioni di notifica su un bucket e si concede ad Amazon S3 l'autorizzazione a invocare una funzione in base alle policy di autorizzazione basati sulle risorse della funzione.
- [Amazon Elastic Kubernetes Service \(Amazon EKS\)](#): Amazon EKS è un servizio gestito che elimina la necessità di installare, utilizzare e mantenere attivo il proprio piano di controllo. Kubernetes [AWSKubernetes](#) è un sistema open source che automatizza la gestione, il ridimensionamento e la distribuzione di applicazioni containerizzate.
- [Amazon Elastic Container Service \(Amazon ECS\)](#): Amazon ECS è un servizio di orchestrazione di container completamente gestito che facilita l'implementazione, la gestione e il dimensionamento di applicazioni distribuite in container.
- [AWS Key Management Service \(AWS KMS\)](#) — AWS Key Management Service (AWS KMS) è un servizio AWS gestito che semplifica la creazione e il controllo delle chiavi di crittografia utilizzate per crittografare i dati. Le chiavi AWS KMS create in AWS KMS sono protette da moduli di sicurezza hardware (HSM) convalidati FIPS 140-2. Per utilizzare o gestire le tue chiavi KMS, interagisci con KMS. AWS
- [Amazon Athena](#): Athena è un servizio di query interattivo che semplifica l'analisi dei dati direttamente in Amazon S3 utilizzando [SQL](#) standard. È inoltre possibile utilizzare Athena per eseguire in modo interattivo l'analisi dei dati utilizzando Apache Spark senza dover pianificare, configurare o gestire le risorse. Quando si eseguono applicazioni Apache Spark su Athena, si invia il codice Spark per l'elaborazione e si ricevono direttamente i risultati.

- [Amazon SageMaker Training](#): esamina le opzioni per la formazione dei modelli con AmazonSageMaker, inclusi algoritmi integrati, algoritmi personalizzati, librerie e modelli disponibili sul Marketplace. AWS
- [AWS Glue](#)— AWS Glue è un servizio di integrazione dei dati senza server che consente agli utenti di analisi di scoprire, preparare, spostare e integrare facilmente i dati da più fonti. È possibile utilizzarlo AWS Glue per l'analisi, l'apprendimento automatico e lo sviluppo di applicazioni. AWS Glue include anche strumenti aggiuntivi per la produttività e le operazioni sui dati per la creazione, l'esecuzione di lavori e l'implementazione di flussi di lavoro aziendali.
- [Amazon EMR](#): Amazon EMR è una piattaforma cluster gestita che semplifica l'esecuzione di framework di big data, ad esempio, per elaborare Apache Hadoop e Apache Spark analizzare grandi quantità di dati. AWS
- [AWS CloudTrail](#)— AWS CloudTrail è un AWS servizio che ti aiuta ad abilitare il controllo operativo e dei rischi, la governance e la conformità del tuo account. AWS Le azioni intraprese da un utente, ruolo o AWS servizio vengono registrate come eventi in CloudTrail. Gli eventi includono le azioni intraprese nella console di AWS gestione, nell'interfaccia a riga di AWS comando, negli AWS SDK e nelle API.
- [AWS CloudFormation](#) — è un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla gestione di tali risorse e più tempo a concentrarsi sulle applicazioni in esecuzione. AWS Crei un modello che descrive tutte le AWS risorse che desideri (come le istanze Amazon EC2 o le istanze DB di Amazon RDS) e CloudFormation si occupa del provisioning e della configurazione di tali risorse per te. Non è necessario creare e configurare le AWS risorse individualmente e capire cosa dipende da cosa; se ne occupa. CloudFormation

Fasi successive

Per ulteriori informazioni sull'utilizzo della classe di archiviazione S3 Express One Zone e dei bucket di directory, consulta gli argomenti seguenti:

- [Esercitazione: nozioni di base su S3 Express One Zone](#)
- [Zone di disponibilità e regioni S3 Express One Zone](#)
- [Collegamento in rete per i bucket di directory in una zona di disponibilità](#)
- [Creazione di bucket di directory in una zona di disponibilità](#)
- [Endpoint regionali e di zona per i bucket di directory in una zona di disponibilità](#)
- [Ottimizzazione delle prestazioni di S3 Express One Zone](#)

Esercitazione: nozioni di base su S3 Express One Zone

Amazon S3 Express One Zone è la prima classe di storage S3 in cui è possibile selezionare un'unica zona di disponibilità con la possibilità di co-localizzare lo storage di oggetti con le risorse di calcolo, per ottenere la massima velocità di accesso possibile. I dati in S3 Express One Zone sono archiviati in bucket di directory situati nelle zone di disponibilità. Per ulteriori informazioni sui bucket di directory, consulta [Bucket di directory](#).

S3 Express One Zone è ideale per tutte le applicazioni in cui è fondamentale ridurre al minimo la latenza delle richieste. Tali applicazioni possono essere flussi di processo interattivi, come l'editing video, in cui i professionisti della creatività hanno bisogno di un accesso reattivo ai contenuti dalle loro interfacce utente. La soluzione S3 Express One Zone è vantaggiosa anche per i carichi di lavoro di analisi e machine learning che hanno requisiti simili di reattività dei dati, in particolare i carichi di lavoro con molti accessi minori o un gran numero di accessi casuali. S3 Express One Zone può essere utilizzato con altri AWS servizi come Amazon EMR, Amazon Athena, AWS Glue Data Catalog e Amazon SageMaker Model Training per supportare carichi di lavoro di analisi, intelligenza artificiale e machine learning (AI/ML). Puoi lavorare con la classe di storage e i bucket di directory S3 Express One Zone utilizzando la console Amazon S3, gli AWS SDK, l'interfaccia a riga di AWS comando (AWS CLI) e l'API REST di Amazon S3. Per ulteriori informazioni, consulta [Che cos'è S3 Express One Zone?](#) e [In che modo S3 Express One Zone è diverso?](#)

Questo è un diagramma del flusso di lavoro S3 Express One Zone.

Obiettivo

In questa esercitazione si apprenderà come creare un endpoint gateway, creare e allegare una policy IAM, creare un bucket di directory e quindi utilizzare l'azione Importa per popolare il bucket di directory con gli oggetti attualmente memorizzati nel bucket per uso generico. In alternativa, è possibile caricare manualmente gli oggetti nel bucket della directory.

Argomenti

- [Prerequisiti](#)
- [Fase 1. Configurazione di un endpoint VPC del gateway per raggiungere i bucket di directory S3 Express One Zone](#)
- [Fase 2. Creazione di un bucket di directory S3 Express One Zone](#)
- [Fase 3. Importazione dei dati in un bucket di directory S3 Express One Zone](#)
- [Fase 4. Caricamento manuale di oggetti nel bucket di directory S3 Express One Zone](#)
- [Fase 5. Eliminazione del contenuto del bucket di directory S3 Express One Zone](#)

- [Fase 6. Eliminazione del bucket di directory S3 Express One Zone](#)
- [Fasi successive](#)

Prerequisiti

Prima di iniziare questo tutorial, devi disporre di un account a Account AWS cui accedere come utente AWS Identity and Access Management (IAM) con le autorizzazioni corrette.

Fasi secondarie

- [Crea un Account AWS](#)
- [Crea un utente IAM nel tuo Account AWS \(console\)](#)
- [Creazione di una policy IAM per collegarla a un utente o a un ruolo IAM \(console\)](#)

Crea un Account AWS

Per completare questo tutorial, è necessario un Account AWS. Quando ti iscrivi AWS, vieni Account AWS automaticamente registrato a tutti i servizi in AWS, incluso Amazon S3. Ti vengono addebitati solo i servizi che utilizzi. Per ulteriori informazioni sui prezzi, consulta [Prezzi di S3](#).

Crea un utente IAM nel tuo Account AWS (console)

AWS Identity and Access Management (IAM) è una soluzione Servizio AWS che aiuta gli amministratori a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (signed in) e autorizzato (dispone di autorizzazioni) ad accedere agli oggetti e a utilizzare i bucket della directory in S3 Express One Zone. Puoi utilizzare IAM senza alcun costo aggiuntivo.

Per impostazione predefinita, gli utenti non hanno le autorizzazioni per accedere ai bucket della directory ed eseguire operazioni S3 Express One Zone. Per concedere le autorizzazioni di accesso per i bucket di directory e le operazioni S3 Express One Zone, puoi utilizzare IAM per creare utenti o ruoli e collegare autorizzazioni a tali identità. Per ulteriori informazioni su come creare un utente IAM, consulta [Creazione di utenti IAM \(console\)](#) nella Guida per l'utente di IAM. Per ulteriori informazioni su come creare un ruolo IAM, consulta [Creazione di un ruolo per delegare le autorizzazioni a un utente IAM](#) nella Guida all'utente IAM.

Per semplicità, questo tutorial crea e utilizza un utente IAM. Dopo aver completato il tutorial, ricordati di [Eliminazione dell'utente IAM](#). Per l'uso in produzione, consigliamo di seguire le [best practice di sicurezza in IAM](#) disponibili nella Guida per l'utente di IAM. Come best practice, richiedi agli utenti

di utilizzare la federazione con un gestore dell'identità digitale per accedere a AWS utilizzando credenziali temporanee. Un'ulteriore suggerimento derivante dalle best practice è richiedere ai carichi di lavoro di utilizzare credenziali temporanee con ruoli IAM per l'accesso ad AWS. Per saperne di più sull'uso della creazione Centro identità AWS IAM di utenti con credenziali temporanee, consulta la [Guida introduttiva](#) nella Guida per l'Centro identità AWS IAM utente.

 Warning

Gli utenti IAM dispongono di credenziali a lungo termine, il che rappresenta un rischio per la sicurezza. Per ridurre questo rischio, si consiglia di fornire a questi utenti solo le autorizzazioni necessarie per eseguire l'attività e di rimuoverli quando non sono più necessari.

Creazione di una policy IAM per collegarla a un utente o a un ruolo IAM (console)

Per impostazione predefinita, gli utenti non dispongono delle autorizzazioni per i bucket di directory e le operazioni S3 Express One Zone. Per concedere le autorizzazioni di accesso per i bucket di directory, puoi utilizzare IAM per creare utenti, gruppi o ruoli e collegare le autorizzazioni a tali identità. I bucket di directory sono l'unica risorsa che è possibile includere nelle policy di bucket o nelle policy di identità IAM per l'accesso a S3 Express One Zone.

Per utilizzare le operazioni API endpoint regionali (a livello di bucket o di piano di controllo (control-plane)) con S3 Express One Zone, si utilizza il modello di autorizzazione IAM, che non prevede la gestione delle sessioni. Le autorizzazioni sono concesse per le singole azioni. Per utilizzare le operazioni API endpoint di zona (operazioni a livello di oggetto o di piano dati), si usa [CreateSession](#) per creare e gestire sessioni ottimizzate per l'autorizzazione a bassa latenza delle richieste di dati. Per recuperare e utilizzare un token di sessione, è necessario consentire l'azione `s3express:CreateSession` per il bucket della directory in una basata sull'identità o in una policy di bucket. Se accedi a S3 Express One Zone nella console Amazon S3, tramite l'interfaccia a riga di AWS comando (AWS CLI) o utilizzando gli AWS SDK, S3 Express One Zone crea una sessione per tuo conto. Per ulteriori informazioni, consulta [CreateSession autorizzazione](#) e [AWS Identity and Access Management \(IAM\) per S3 Express One Zone](#).

Per creare una policy IAM e associarla a un utente (o ruolo) IAM

1. Accedi alla console di gestione e apri la console di AWS gestione IAM.
2. Nel riquadro di navigazione, scegli Policy.

3. Scegli Crea policy.
4. Seleziona JSON.
5. Copia la policy sottostante nella finestra di Editor di policy. Prima di poter creare bucket di directory o utilizzare S3 Express One Zone, devi concedere le autorizzazioni necessarie al tuo ruolo o ai tuoi utenti AWS Identity and Access Management (IAM). Questa policy di esempio consente l'accesso all'operazione API `CreateSession` (da utilizzare con altre operazioni API a livello di zona o di oggetto) e a tutte le operazioni API a livello di endpoint regionale (bucket). Questa policy consente l'utilizzo dell'operazione API `CreateSession` con tutti i bucket di directory, ma le operazioni API dell'endpoint regionale sono consentite solo con il bucket di directory specificato. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessRegionalEndpointAPIs",
      "Effect": "Allow",
      "Action": [
        "s3express:DeleteBucket",
        "s3express:DeleteBucketPolicy",
        "s3express>CreateBucket",
        "s3express:PutBucketPolicy",
        "s3express:GetBucketPolicy",
        "s3express>ListAllMyDirectoryBuckets"
      ],
      "Resource": "arn:aws:s3express:us-east-1:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3/*"
    },
    {
      "Sid": "AllowCreateSession",
      "Effect": "Allow",
      "Action": "s3express>CreateSession",
      "Resource": "*"
    }
  ]
}
```

6. Scegli Avanti.
7. Rinomina la policy.

 Note

I tag dei bucket non sono supportati per S3 Express One Zone.

8. Seleziona Crea policy.
9. Ora che è stata creata una policy IAM, è possibile associarla a un utente IAM. Nel riquadro di navigazione, scegli Policy.
10. Nella barra di ricerca, inserisci il nome della policy.
11. Dal menu Azioni, seleziona Allega.
12. In Filtro per tipo di entità, seleziona Utenti IAM o Ruoli.
13. Nel campo di ricerca, digita il nome dell'utente o del ruolo da utilizzare.
14. Scegli Attach Policy (Collega policy).

Fase 1. Configurazione di un endpoint VPC del gateway per raggiungere i bucket di directory S3 Express One Zone

È possibile accedere alle operazioni API di zona e regionali attraverso gli endpoint del gateway cloud privato virtuale (VPC). Gli endpoint del gateway possono consentire al traffico di raggiungere la zona S3 Express One senza attraversare un gateway NAT. Si consiglia vivamente di utilizzare endpoint gateway, in quanto forniscono il percorso di rete più ottimale quando si lavora con S3 Express One Zone. È possibile accedere ai bucket di directory S3 Express One Zone dal VPC senza un gateway Internet o un dispositivo NAT per il VPC e senza costi aggiuntivi. Utilizza la seguente procedura per configurare un endpoint gateway che si connetta agli oggetti di classe di storage S3 Express One Zone e ai bucket della directory.

Per accedere a S3 Express One Zone, si utilizzano endpoint regionali e zonali diversi dagli endpoint Amazon S3 standard. A seconda dell'operazione API Amazon S3 utilizzata, è richiesto un endpoint regionale o zonale. Per un elenco completo delle operazioni API supportate per tipo di endpoint, consulta [Operazioni API supportate da S3 Express One Zone](#). È necessario accedere agli endpoint regionali e zonali tramite un endpoint del cloud privato virtuale (VPC) del gateway.

Utilizza la seguente procedura per creare un endpoint gateway che si connetta agli oggetti della classe di storage S3 Express One Zone e ai bucket della directory.

Per configurare gli endpoint VPC del gateway

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione laterale, alla voce Cloud privato virtuale, scegli Endpoint.
3. Seleziona Crea endpoint.
4. Crea un nome per l'endpoint.
5. Per Service category (Categoria servizio), scegli Servizi AWS.
6. In Servizi, cerca utilizzando il filtro Type=Gateway, quindi scegli il pulsante di opzione accanto a com.amazonaws. **region**.s3express.
7. Per VPC, scegli un VPC in cui creare l'endpoint.
8. Per le tabelle delle rotte, scegli la tabella delle rotte nella tua zona locale da utilizzare dall'endpoint. Dopo la creazione dell'endpoint, verrà aggiunto un record di routing alla tabella di routing selezionata in questo passaggio.
9. Per Policy, scegli Accesso completo per consentire a tutti i principali di eseguire tutte le operazioni su tutte le risorse dell'endpoint VPC. Altrimenti, scegli Personalizzato per allegare una policy dell'endpoint VPC che controlla le autorizzazioni dei principali a eseguire azioni sulle risorse attraverso l'endpoint VPC.
10. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:
 - IPv4: assegna gli indirizzi IPv4 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e il servizio accetta richieste IPv4.
 - IPv6: assegna gli indirizzi IPv6 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6 e il servizio accetta richieste IPv6.
 - Dualstack: assegna gli indirizzi IPv4 e IPv6 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6 e il servizio accetta sia richieste IPv4 e IPv6.
11. (Facoltativo) Per aggiungere un tag, scegli Aggiungi nuovo tag e immetti la chiave e il valore del tag.
12. Seleziona Crea endpoint.

Dopo aver creato un endpoint del gateway, puoi utilizzare gli endpoint API regionali e gli endpoint API zonali per accedere agli oggetti della classe di archiviazione Amazon S3 Express One Zone e ai bucket di directory.

Fase 2. Creazione di un bucket di directory S3 Express One Zone

1. Accedi e apri la console Amazon S3 all'indirizzo. Console di gestione AWS <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare un bucket.

Note

Scegli una regione nelle tue vicinanze per ridurre al minimo la latenza e i costi o essere conforme ai requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione. Per un elenco di Amazon S3 Regioni AWS, consulta gli [Servizio AWS endpoint](#) in. Riferimenti generali di Amazon Web Services

3. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
4. Scegliere Create bucket (Crea bucket). Viene visualizzata la pagina Create bucket (Crea bucket).
5. In Configurazione generale, visualizza Regione AWS dove verrà creato il bucket.

In Tipo di bucket, scegli Directory.

Note

- Se si è scelta una Regione che non supporta i bucket di directory, l'opzione Tipo di bucket scompare e il tipo di bucket viene impostato su un bucket per uso generico. Per creare un bucket di directory, è necessario scegliere una Regione supportata. Per un elenco delle Regioni che supportano i bucket di directory e la classe di storage Amazon S3 Express One Zone, consulta [the section called “Zone di disponibilità e regioni S3 Express One Zone”](#).
- Dopo aver creato il bucket, non è possibile modificare il tipo di bucket.

 Note

La zona di disponibilità non può essere modificata dopo che il bucket è stato creato.

6. Per Zona di disponibilità, scegli una zona di disponibilità locale nei servizi di calcolo. Per un elenco delle zone di disponibilità che supportano i bucket di directory e la classe di storage S3 Express One Zone, consulta [the section called “Zone di disponibilità e regioni S3 Express One Zone”](#).

In Zona di disponibilità, seleziona la casella di controllo per riconoscere che, in caso di interruzione della zona di disponibilità, i dati potrebbero essere non disponibili o persi.

 Important

Sebbene i bucket di directory siano archiviati su più dispositivi all'interno di una singola Zona di disponibilità, i bucket di directory non archiviano i dati in modo ridondante tra le varie Zona di disponibilità.

7. Per Nome bucket, immetti il nome del bucket di directory.

Le seguenti regole di denominazione si applicano ai bucket della directory.

- Sii unico all'interno della zona scelta (zona di AWS disponibilità o zona AWS locale).
- Il nome deve avere una lunghezza compresa tra 3 (min) e 63 (max) caratteri, incluso il suffisso.
- Essere costituiti solo da lettere minuscole, numeri e trattini (-).
- Iniziare e finire con una lettera o un numero.
- Deve includere il seguente suffisso: `--zone-id--x-s3`.
- I nomi dei bucket non devono iniziare con il prefisso `xn--`.
- I nomi dei bucket non devono iniziare con il prefisso `sthree-`.
- I nomi dei bucket non devono iniziare con il prefisso `sthree-configurator`.
- I nomi dei bucket non devono iniziare con il prefisso `amzn-s3-demo-`.
- I nomi dei bucket non devono terminare con il suffisso `-s3alias`. Questo suffisso è riservato ai nomi alias dei punti di accesso. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

- I nomi dei bucket non devono terminare con il suffisso `-o1-s3`. Questo suffisso è riservato ai nomi alias dei punti di accesso Lambda per oggetti. Per ulteriori informazioni, consulta [Come utilizzare un alias in stile bucket per il punto di accesso Lambda per oggetti del bucket S3](#).
- I nomi dei bucket non devono terminare con il suffisso `.mrp`. Questo suffisso è riservato ai nomi dei punti di Multi-Region accesso. Per ulteriori informazioni, consulta [Regole per la denominazione degli Access Point di Amazon S3 Multi-Region](#).

Un suffisso viene aggiunto automaticamente al nome di base fornito quando si crea un bucket di directory tramite la console. Questo suffisso include l'ID zona di disponibilità della zona di disponibilità scelta.

Una volta creato il bucket, non è possibile modificarne il nome. Per ulteriori informazioni sulla denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#).

 Important

Non includere informazioni sensibili, come i numeri di conto, nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

8. In Proprietà dell'oggetto, l'impostazione Proprietario del bucket è automaticamente abilitata e tutte le liste di controllo degli accessi (ACL) sono disabilitate. Per i bucket di directory, le ACL non possono essere abilitate.

Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket ha automaticamente il controllo completo di ogni oggetto di proprietà nel bucket per uso generico. Le liste di controllo degli accessi (ACL) non influiscono più sulle autorizzazioni di accesso ai dati nel bucket per uso generico S3. Il bucket utilizza esclusivamente le policy per definire il controllo degli accessi.

9. In Impostazioni di blocco dell'accesso pubblico per questo bucket, tutte le impostazioni di blocco dell'accesso pubblico per il bucket di directory sono automaticamente attivate. Queste impostazioni non possono essere modificate per i bucket di directory. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).
10. Per configurare la crittografia predefinita, in Tipo di crittografia scegli una delle seguenti opzioni:
 - Server-side crittografia con chiave gestita Amazon S3 () SSE-S3
 - Server-side crittografia con AWS Key Management Service chiave () SSE-KMS

Per ulteriori informazioni sull'utilizzo della crittografia lato server di Amazon S3 per crittografare i dati, consulta [Protezione e crittografia dei dati](#).

⚠ Important

Se si utilizza l' SSE-KMS opzione per la configurazione di crittografia predefinita, si è soggetti alla quota di richieste al secondo (RPS) di AWS KMS. Per ulteriori informazioni sulle quote AWS KMS e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Potrebbe essere necessario aggiornare le policy di bucket quando si abilita la crittografia predefinita. Per ulteriori informazioni, consulta [Utilizzo della SSE-KMS crittografia per le operazioni tra account](#).

11. Se hai scelto Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3), in Bucket Key viene visualizzato Enabled. Le chiavi S3 Bucket sono sempre abilitate quando configuri il bucket di directory con cui utilizzare la crittografia predefinita. SSE-S3 Le S3 Bucket Keys sono sempre abilitate per le operazioni GET e PUT in un bucket di directory e non possono essere disabilitate. Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket generici o tra bucket di directory, tramite [CopyObject](#) [UploadPartCopy](#), [l'operazione in Batch Operations o i job](#). [Copy import](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia di un oggetto. KMS-encrypted

Le chiavi S3 Bucket riducono il costo della crittografia diminuendo il traffico di richieste da Amazon S3 a AWS KMS. Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

12. Se hai scelto Server-side la crittografia con AWS Key Management Service key (SSE-KMS), in AWS KMS key, specifica la tua AWS Key Management Service chiave in uno dei seguenti modi o crea una nuova chiave.
 - Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS keys e scegli la tua chiave KMS da Disponibile. AWS KMS keys

In questo elenco vengono visualizzate solo le chiavi gestite dal cliente. La Chiave gestita da AWS (aws/s3) non è supportata nei bucket di directory. Per ulteriori informazioni sulle

chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per specificare l'ARN o l'alias della chiave KMS, scegli Inserisci l'ARN della AWS KMS key e immetti l'ARN o l'alias della chiave KMS in ARN della AWS KMS key .
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

Important

- La SSE-KMS configurazione può supportare solo 1 chiave gestita [dal cliente](#) per bucket di directory per tutta la durata del bucket. [Chiave gestita da AWS](#) (aws/s3) non è supportato. Inoltre, dopo aver specificato una chiave gestita dal cliente per SSE-KMS, non è possibile sovrascrivere la chiave gestita dal cliente per la configurazione del bucket. SSE-KMS

Puoi identificare la chiave gestita dal cliente che hai specificato per la SSE-KMS configurazione del bucket nel modo seguente:

- Si effettua una richiesta di operazione API HeadObject per trovare il valore di x-amz-server-side-encryption-aws-kms-key-id nella risposta.

Per utilizzare una nuova chiave gestita dal cliente per i propri dati, si consiglia di copiare gli oggetti esistenti in un nuovo bucket della directory con una nuova chiave gestita dal cliente.

- È possibile utilizzare solo le chiavi KMS disponibili nello stesso bucket della Regione AWS. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, devi inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione necessaria per l'uso della chiave e quindi inserire l'ARN della chiave KMS. Per ulteriori informazioni sulle autorizzazioni tra account per le chiavi KMS, consulta [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service . Per ulteriori informazioni su SSE-KMS, consulta [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\) per il caricamento di nuovi oggetti nei bucket di directory](#)

- Quando si utilizza una AWS KMS key crittografia lato server nei bucket di directory, è necessario scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni sull'utilizzo AWS KMS con Amazon S3, consulta. [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket di directory](#)

13. Seleziona Crea bucket. Dopo aver creato il bucket, puoi aggiungere file e cartelle al bucket. Per ulteriori informazioni, consulta [the section called “Utilizzo di oggetti in un bucket di directory”](#).

Fase 3. Importazione dei dati in un bucket di directory S3 Express One Zone

Per completare questo passaggio, è necessario disporre di un bucket generico che contenga oggetti e si trovi nello Regione AWS stesso bucket di directory.

Dopo aver creato un bucket di directory in Amazon S3, è possibile riempire il nuovo bucket con i dati utilizzando l'azione Importa nella console di Amazon S3. L'importazione semplifica la copia dei dati nei bucket di directory, consentendo di scegli un prefisso o un bucket per uso generico da cui importare i dati senza dover specificare singolarmente tutti gli oggetti da copiare. L'importazione utilizza Operazioni in batch S3 che copia gli oggetti nel prefisso o nel bucket per uso generico selezionato. È possibile monitorare l'avanzamento del processo di copia di importazione attraverso la pagina dei dettagli del processo di Operazioni in batch S3.

Per utilizzare l'azione Importa

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome di Regione AWS attualmente visualizzato. Quindi, scegli la Regione associata alla zona di disponibilità in cui si trova il bucket della directory.
3. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
4. Seleziona il pulsante di opzione accanto al nome del bucket in cui desideri importare gli oggetti.
5. Scegli Importa.

6. Per Origine, inserisci il bucket per uso generico (o il percorso del bucket incluso il prefisso) contenente gli oggetti che desideri importare. Per scegliere un bucket per uso generico esistente da un elenco, scegli Sfoglia S3.
7. Nella sezione Autorizzazioni, si può scegliere di far generare automaticamente un ruolo IAM. In alternativa, è possibile selezionare un ruolo IAM da un elenco o inserire direttamente un ARN del ruolo IAM.
 - Per consentire ad Amazon S3 di creare automaticamente un nuovo ruolo IAM, scegli Crea un nuovo ruolo IAM.

 Note

Se i tuoi oggetti sorgente sono crittografati con crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS), non scegliere l'opzione Crea nuovo ruolo IAM. Specifica invece un ruolo IAM esistente che disponga dell'autorizzazione `kms:Decrypt`.

Amazon S3 utilizzerà questa autorizzazione per decrittografare gli oggetti. Durante il processo di importazione, Amazon S3 crittograferà quindi nuovamente tali oggetti utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3

- Per scegliere un ruolo IAM esistente da un elenco, seleziona Scegli tra ruoli IAM esistenti.
 - Per specificare un ruolo IAM esistente inserendo il relativo nome della risorsa Amazon (ARN), seleziona Inserisci ARN ruolo IAM, quindi inserisci l'ARN nel campo corrispondente.
8. Rivedi le informazioni visualizzate nelle sezioni Destinazione e Impostazioni degli oggetti copiati. Se le informazioni nella sezione Destinazione sono corrette, scegli Importa per avviare il processo di copia.

La console Amazon S3 visualizza lo stato del nuovo processo nella pagina Operazioni in batch. Per ulteriori informazioni sul processo, scegli il pulsante di opzione accanto al nome del processo, quindi nel menu Azioni, scegli Visualizza dettagli. Per aprire il bucket di directory in cui verranno importati gli oggetti, scegli Visualizza la destinazione di importazione.

Fase 4. Caricamento manuale di oggetti nel bucket di directory S3 Express One Zone

È anche possibile caricare manualmente gli oggetti nel bucket della directory.

Per caricare manualmente gli oggetti

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione associata alla zona di disponibilità in cui si trova il bucket della directory.
3. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
4. Scegli il nome del bucket in cui caricare le cartelle o i file.

Note

Se si è scelto lo stesso bucket di directory utilizzato nelle fasi precedenti di questa esercitazione, il bucket di directory conterrà gli oggetti caricati dallo strumento Importa. Si noti che questi oggetti sono ora memorizzati nella classe di storage S3 Express One Zone.

5. Nell'elenco Oggetti, scegli Carica.
6. Nella pagina di caricamento, esegui una delle seguenti operazioni:
 - Trascina e rilascia i file e le cartelle nell'area di caricamento tratteggiata.
 - Scegli Aggiungi file o Aggiungi cartella, scegli i file o le cartelle da caricare, quindi scegli Apri o Carica.
7. In Checksum, scegli la funzione Checksum da utilizzare.

Note

Si consiglia di utilizzare CRC32 e CRC32C per ottenere le migliori prestazioni con la classe di storage S3 Express One Zone. Per ulteriori informazioni, consulta le [Best practice aggiuntive sui checksum S3](#).

(Facoltativo) Se si sta caricando un singolo oggetto di dimensioni inferiori a 16 MB, si può anche specificare un valore di checksum precalcolato. Quando si fornisce un valore precalcolato, Amazon S3 lo confronta con il valore calcolato utilizzando la funzione di checksum selezionata. Se i valori non corrispondono, il caricamento non viene avviato.

8. Le opzioni delle sezioni Autorizzazioni e Proprietà sono impostate automaticamente come predefinite e non possono essere modificate. Blocco dell'accesso pubblico è abilitato automaticamente; Controllo delle versioni S3 e S3 Object Lock non possono essere abilitati per i bucket della directory.

(Facoltativo) Se desideri aggiungere metadati in coppie chiave-valore agli oggetti, espandi la sezione Proprietà e scegli Aggiungi metadati nella sezione Metadati.

9. Per caricare i file e le cartelle elencati, scegli Carica.

Amazon S3 caricherà i tuoi oggetti e le tue cartelle. Al termine del caricamento viene visualizzato un messaggio di esito positivo nella pagina Carica: stato.

È stato creato con successo un bucket di directory e sono stati caricati gli oggetti nel bucket.

Fase 5. Eliminazione del contenuto del bucket di directory S3 Express One Zone

È possibile svuotare il bucket di directory Amazon S3 utilizzando la console Amazon S3.

Per svuotare un bucket di directory

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione associata alla zona di disponibilità in cui si trova il bucket della directory.
3. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
4. Scegli il pulsante di opzione accanto al nome del bucket che si desidera svuotare, quindi scegli Svuota.
5. Nella pagina Svuota bucket conferma che desideri svuotare il bucket inserendo **permanently delete** nel campo di testo e quindi scegli Svuota.
6. Monitora l'avanzamento del processo di svuotamento del bucket nella pagina Svuota bucket: stato.

Fase 6. Eliminazione del bucket di directory S3 Express One Zone

Dopo aver svuotato il bucket della directory e aver interrotto tutti i caricamenti multiparte in corso, è possibile eliminare il bucket utilizzando la console Amazon S3.

Per eliminare un bucket di directory

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione associata alla zona di disponibilità in cui si trova il bucket della directory.
3. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
4. Nell'elenco dei Bucket di directory, scegli il pulsante di opzione accanto al bucket che si desidera eliminare.
5. Scegliere Elimina.
6. Nella pagina Elimina bucket inserisci il nome del bucket nel campo di testo per confermare l'eliminazione del bucket.

Important

L'eliminazione di un bucket di directory non può essere annullata.

7. Per eliminare il bucket di directory, scegli Elimina bucket.

Fasi successive

In questa esercitazione si è appreso come creare un bucket di directory e come utilizzare la classe di storage S3 Express One Zone. Dopo aver completato questa esercitazione, è possibile esplorare i servizi AWS correlati da utilizzare con la classe di storage S3 Express One Zone.

Puoi utilizzare quanto segue Servizi AWS con la classe di storage S3 Express One Zone per supportare il tuo caso d'uso specifico a bassa latenza.

- [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) - Amazon EC2 fornisce capacità di calcolo sicura e scalabile in Cloud AWS. L'utilizzo Amazon EC2 riduce la necessità di investimenti anticipati in hardware e ti permette di sviluppare e distribuire più rapidamente le applicazioni. Puoi utilizzare Amazon EC2 per avviare il numero di server virtuali necessari, configurare la sicurezza e i servizi di rete, nonché gestire l'archiviazione.
- [AWS Lambda](#): Lambda è un servizio di calcolo che consente di eseguire il codice senza provisioning o gestire server. Si configurano le impostazioni di notifica su un bucket e si concede

ad Amazon S3 l'autorizzazione a invocare una funzione in base alle policy di autorizzazione basati sulle risorse della funzione.

- [Amazon Elastic Kubernetes Service \(Amazon EKS\)](#): Amazon EKS è un servizio gestito che elimina la necessità di installare, utilizzare e mantenere attivo il proprio piano di controllo. Kubernetes AWS [Kubernetes](#) è un sistema open source che automatizza la gestione, il ridimensionamento e la distribuzione di applicazioni containerizzate.
- [Amazon Elastic Container Service \(Amazon ECS\)](#): Amazon ECS è un servizio di orchestrazione di container completamente gestito che facilita l'implementazione, la gestione e il dimensionamento di applicazioni distribuite in container.
- [Amazon EMR](#): Amazon EMR è una piattaforma cluster gestita che semplifica l'esecuzione di framework di big data, ad esempio per elaborare e analizzare grandi quantità di dati. Apache Hadoop Apache Spark AWS
- [Amazon Athena](#): Athena è un servizio di query interattivo che semplifica l'analisi dei dati direttamente in Amazon S3 utilizzando [SQL](#) standard. È inoltre possibile utilizzare Athena per eseguire in modo interattivo l'analisi dei dati utilizzando Apache Spark senza dover pianificare, configurare o gestire le risorse. Quando si eseguono applicazioni Apache Spark su Athena, si invia il codice Spark per l'elaborazione e si ricevono direttamente i risultati.
- [AWS Glue Data Catalog](#): AWS Glue è un servizio di integrazione dei dati senza server che consente agli utenti di analisi di scoprire, preparare, spostare e integrare facilmente i dati da più fonti. Puoi utilizzarlo AWS Glue per l'analisi, l'apprendimento automatico e lo sviluppo di applicazioni. AWS Glue Data Catalog è un repository centralizzato che memorizza i metadati sui set di dati della tua organizzazione. Funge da indice per la posizione, lo schema e le metriche di esecuzione delle origini dati.
- [Amazon SageMaker Runtime Model Training](#): Amazon SageMaker Runtime è un servizio di machine learning completamente gestito. Con SageMaker Runtime, i data scientist e gli sviluppatori possono creare e addestrare modelli di machine learning in modo rapido e semplice, per poi distribuirli direttamente in un ambiente ospitato pronto per la produzione.

Per ulteriori informazioni su S3 Express One Zone, consulta [Che cos'è S3 Express One Zone?](#) e [In che modo S3 Express One Zone è diverso?](#)

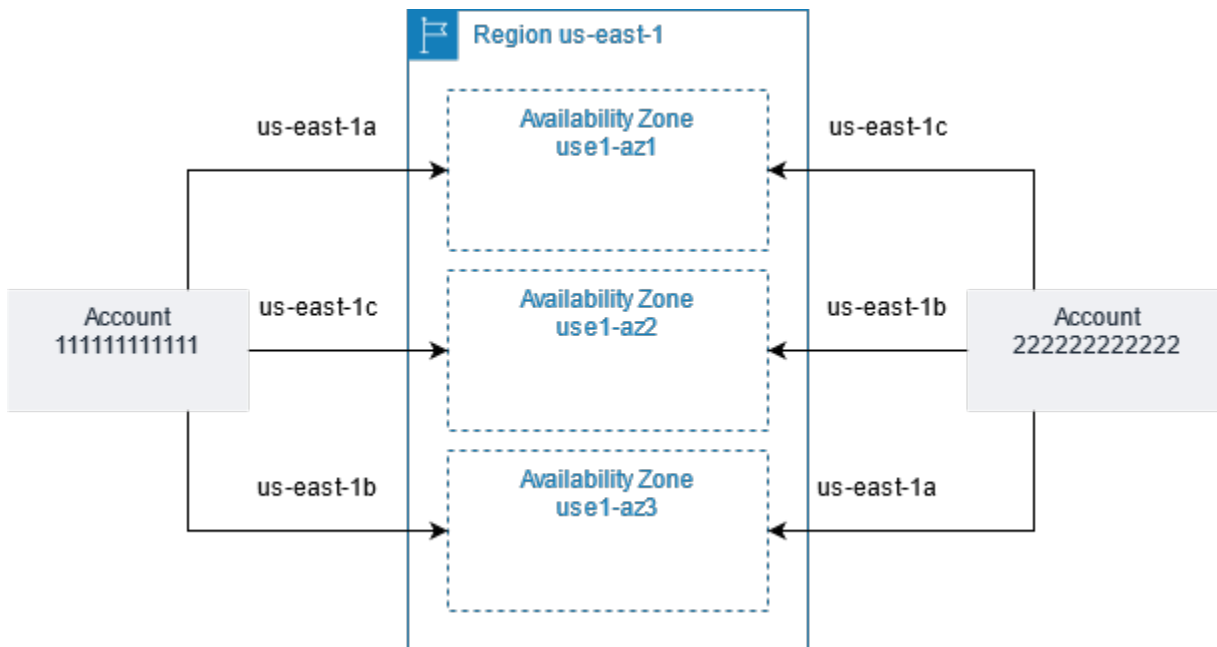
Zone di disponibilità e regioni S3 Express One Zone

Una zona di disponibilità consiste in uno o più data center separati con alimentazione, rete e connettività ridondanti in una Regione AWS. Per ottimizzare i recuperi a bassa latenza, gli oggetti

della classe di archiviazione Amazon S3 Express One Zone vengono archiviati in modo ridondante in bucket di directory S3 in una singola zona di disponibilità che è locale per il carico di lavoro di calcolo. Quando crei un bucket di directory, scegli la zona di disponibilità e Regione AWS dove verrà collocato il bucket.

AWS mappa le zone di disponibilità fisiche in modo casuale sui nomi delle zone di disponibilità di ciascuna. Account AWS Questo approccio aiuta a distribuire le risorse tra le zone di disponibilità in un Regione AWS, invece di concentrarle probabilmente nella prima zona di disponibilità di ciascuna regione. Di conseguenza, la tua zona us-east-1a di disponibilità Account AWS potrebbe non corrispondere alla stessa ubicazione fisica us-east-1a di un'altra Account AWS. Per ulteriori informazioni, consulta [Regioni e zone di disponibilità](#) nella Guida all'utente di Amazon EC2.

Per coordinare le zone di disponibilità tra account, devi utilizzare l'ID AZ, identificatore unico e coerente per una zona di disponibilità. Ad esempio, use1-az1 è un ID AZ per la us-east-1 regione e ha la stessa posizione fisica in ogni regione Account AWS. L'illustrazione seguente mostra come gli ID AZ siano gli stessi per ogni account, anche se i nomi delle zone di disponibilità potrebbero essere mappati in modo diverso per ciascun account.



Con S3 Express One Zone, i dati vengono archiviati in modo ridondante su più dispositivi all'interno di una singola zona di disponibilità. S3 Express One Zone è progettato per una disponibilità del 99,95% all'interno di una singola zona di disponibilità ed è supportato dall'[Accordo sul livello di servizio di Amazon S3](#). Per ulteriori informazioni, consulta [Zone di disponibilità](#)

La tabella seguente mostra le Regioni e le zone di disponibilità S3 Express One Zone supportate.

Nome della Regione	Codice regione	ID zona di disponibilità				
Stati Uniti orientali (Virginia settentrionale)	us-east-1	use1-az4				
		use1-az5				
		use1-az6				
Stati Uniti orientali (Ohio)	us-east-2	use2-az1				
		use2-az2				
Stati Uniti occidentali (Oregon)	us-west-2	usw2-az1				
		usw2-az3				
		usw2-az4				
Asia Pacifico (Mumbai)	ap-south-1	aps1-az1				
		aps1-az3				
Asia Pacifico (Tokyo)	ap-northeast-1	apne1-az1				
		apne1-az4				
Europa (Francoforte)	eu-central-1	euc1-az1				
		euc1-az2				
Europa (Irlanda)	eu-west-1	euw1-az1				
		euw1-az3				
Europa (Stoccolma)	eu-north-1	eun1-az1				
		eun1-az2				
		eun1-az3				

Collegamento in rete per i bucket di directory in una zona di disponibilità

Per ridurre il tempo che i pacchetti trascorrono sulla rete, configura il cloud privato virtuale (VPC) con un endpoint gateway per accedere ai bucket di directory nelle zone di disponibilità mantenendo il traffico all'interno della AWS rete e senza costi aggiuntivi.

Argomenti

- [Endpoint per i bucket di directory nelle zone di disponibilità](#)
- [Configurazione degli endpoint VPC del gateway](#)

Endpoint per i bucket di directory nelle zone di disponibilità

Nella tabella seguente vengono mostrati gli endpoint API regionali e zonali disponibili per ogni regione e zona di disponibilità.

Configurazione degli endpoint VPC del gateway

Utilizza la procedura seguente per creare un endpoint del gateway che si connette agli oggetti della classe di archiviazione Amazon S3 Express One Zone e ai bucket di directory.

Per configurare gli endpoint VPC del gateway

1. Apri la [Console VPC di Amazon](#).
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Crea un nome per l'endpoint.
5. Per Service category (Categoria servizio), scegli Servizi AWS.
6. Per Services, aggiungi il filtro Type=Gateway e quindi scegli il pulsante di opzione accanto a com.amazonaws. **region**.s3express.
7. Per VPC, scegli un VPC in cui creare l'endpoint.
8. Per le tabelle di percorso, scegli la tabella di percorso nel tuo VPC da utilizzare dall'endpoint. Dopo la creazione dell'endpoint, verrà aggiunto un record di routing alla tabella di routing selezionata in questo passaggio.
9. Per Policy, scegli Accesso completo per consentire a tutti i principali di eseguire tutte le operazioni su tutte le risorse dell'endpoint VPC. Altrimenti, scegli Personalizzato per allegare una policy dell'endpoint VPC che controlla le autorizzazioni dei principali a eseguire azioni sulle risorse attraverso l'endpoint VPC.

10. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:
 - IPv4: assegna gli indirizzi IPv4 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e il servizio accetta richieste IPv4.
 - IPv6: assegna gli indirizzi IPv6 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6 e il servizio accetta richieste IPv6.
 - Dualstack: assegna gli indirizzi IPv4 e IPv6 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6 e il servizio accetta sia richieste IPv4 e IPv6.
11. (Facoltativo) Per aggiungere un tag, scegli Aggiungi nuovo tag e immetti la chiave e il valore del tag.
12. Seleziona Crea endpoint.

Dopo aver creato un endpoint del gateway, puoi utilizzare gli endpoint API regionali e gli endpoint API zonali per accedere agli oggetti della classe di archiviazione Amazon S3 Express One Zone e ai bucket di directory.

Per saperne di più sugli endpoint VPC gateway, consulta [Endpoint gateway](#) nella Guida a AWS PrivateLink . Per i casi d'uso della residenza dei dati, si consiglia di abilitare l'accesso ai bucket solo dal VPC utilizzando gli endpoint del gateway VPC. Quando l'accesso è limitato a un VPC o a un endpoint VPC, puoi accedere agli oggetti tramite l'API REST e gli SDK. Console di gestione AWS
AWS CLI AWS

Note

Per limitare l'accesso a un VPC o a un endpoint VPC utilizzando il Console di gestione AWS, è necessario utilizzare Private Access. Console di gestione AWS Per ulteriori informazioni, consulta [Console di gestione AWS Private Access](#) nella Console di gestione AWS guida.
Console di gestione AWS

Creazione di bucket di directory in una zona di disponibilità

Per iniziare a utilizzare la classe di archiviazione Amazon S3 Express One Zone, crea una bucket di directory. La classe di archiviazione S3 Express One Zone può essere utilizzata solo con i bucket

di directory. La classe di archiviazione S3 Express One Zone supporta casi d'uso a bassa latenza e fornisce un'elaborazione dei dati più rapida all'interno di una singola zona di disponibilità. Se l'applicazione è sensibile alle prestazioni e beneficia di latenze PUT e GET di pochi millisecondi, si consiglia di creare un bucket di directory in modo da poter utilizzare la classe di archiviazione S3 Express One Zone.

Esistono due tipi di bucket Amazon S3: i bucket per uso generico e i bucket di directory. È opportuno scegliere il tipo di bucket più adatto ai requisiti applicativi e di prestazioni. I bucket per uso generico sono il tipo di bucket S3 originale. I bucket per uso generico sono consigliati per la maggior parte dei casi d'uso e dei modelli di accesso e consentono di archiviare oggetti in tutte le classi di storage, ad eccezione di S3 Express One Zone. Per ulteriori informazioni sui bucket per uso generico, consulta [Panoramica dei bucket per uso generico](#).

I bucket di directory utilizzano la classe di archiviazione S3 Express One Zone, che è progettata per l'utilizzo con carichi di lavoro o applicazioni con prestazioni critiche che richiedono una latenza costante di pochi millisecondi. S3 Express One Zone è la prima classe di storage S3 in cui è possibile selezionare una singola zona di disponibilità con la possibilità di co-ubicare l'archiviazione di oggetti con le risorse di calcolo, che offre la massima velocità di accesso possibile. Quando crei un bucket di directory, puoi facoltativamente specificare una Regione AWS e una zona di disponibilità locali alle tue istanze di calcolo Amazon EC2, Amazon Elastic Kubernetes Service o Amazon Elastic Container Service (Amazon ECS) per ottimizzare le prestazioni.

Con S3 Express One Zone, i dati vengono archiviati in modo ridondante su più dispositivi all'interno di una singola zona di disponibilità. S3 Express One Zone è progettato per una disponibilità del 99,95% all'interno di una singola zona di disponibilità ed è supportato dall'[Accordo sul livello di servizio di Amazon S3](#). Per ulteriori informazioni, consulta [Zone di disponibilità](#)

I bucket di directory organizzano i dati in modo gerarchico in directory, a differenza della struttura di archiviazione piatta dei bucket per uso generico. Non ci sono limiti di prefisso per i bucket di directory e le singole directory possono scalare orizzontalmente.

Per ulteriori informazioni sui bucket di directory, consulta [Operazioni con i bucket di directory](#).

Nomi dei bucket di directory

I nomi dei bucket di directory devono seguire questo formato e rispettare le regole di denominazione dei bucket di directory:

```
bucket-base-name--zone-id--x-s3
```

Ad esempio, il seguente nome del bucket di directory contiene l'ID zona di disponibilità `usw2-az1`:

```
bucket-base-name--usw2-az1--x-s3
```

Per ulteriori informazioni sulle regole di denominazione dei bucket di directory, consulta [Regole di denominazione dei bucket di directory](#).

Utilizzo della console S3

1. Accedi e apri la console Amazon S3 all'indirizzo. Console di gestione AWS <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare un bucket.

Note

Scegli una regione nelle tue vicinanze per ridurre al minimo la latenza e i costi o essere conforme ai requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione. Per un elenco di Amazon S3 Regioni AWS, consulta gli [Servizio AWS endpoint](#) in. Riferimenti generali di Amazon Web Services

3. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
4. Scegliere Create bucket (Crea bucket). Viene visualizzata la pagina Create bucket (Crea bucket).
5. In Configurazione generale, visualizza Regione AWS dove verrà creato il bucket.

In Tipo di bucket, scegli Directory.

Note

- Se si è scelta una Regione che non supporta i bucket di directory, l'opzione Tipo di bucket scompare e il tipo di bucket viene impostato su un bucket per uso generico. Per creare un bucket di directory, è necessario scegliere una Regione supportata. Per un elenco delle Regioni che supportano i bucket di directory e la classe di storage Amazon S3 Express One Zone, consulta [the section called “Zone di disponibilità e regioni S3 Express One Zone”](#).
- Dopo aver creato il bucket, non è possibile modificare il tipo di bucket.

 Note

La zona di disponibilità non può essere modificata dopo che il bucket è stato creato.

6. Per Zona di disponibilità, scegli una zona di disponibilità locale nei servizi di calcolo. Per un elenco delle zone di disponibilità che supportano i bucket di directory e la classe di storage S3 Express One Zone, consulta [the section called “Zone di disponibilità e regioni S3 Express One Zone”](#).

In Zona di disponibilità, seleziona la casella di controllo per riconoscere che, in caso di interruzione della zona di disponibilità, i dati potrebbero essere non disponibili o persi.

 Important

Sebbene i bucket di directory siano archiviati su più dispositivi all'interno di una singola Zona di disponibilità, i bucket di directory non archiviano i dati in modo ridondante tra le varie Zona di disponibilità.

7. Per Nome bucket, immetti il nome del bucket di directory.

Le seguenti regole di denominazione si applicano ai bucket della directory.

- Sii unico all'interno della zona scelta (zona di AWS disponibilità o zona AWS locale).
- Il nome deve avere una lunghezza compresa tra 3 (min) e 63 (max) caratteri, incluso il suffisso.
- Essere costituiti solo da lettere minuscole, numeri e trattini (-).
- Iniziare e finire con una lettera o un numero.
- Deve includere il seguente suffisso: `--zone-id--x-s3`.
- I nomi dei bucket non devono iniziare con il prefisso `xn--`.
- I nomi dei bucket non devono iniziare con il prefisso `sthree-`.
- I nomi dei bucket non devono iniziare con il prefisso `sthree-configurator`.
- I nomi dei bucket non devono iniziare con il prefisso `amzn-s3-demo-`.
- I nomi dei bucket non devono terminare con il suffisso `-s3alias`. Questo suffisso è riservato ai nomi alias dei punti di accesso. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

- I nomi dei bucket non devono terminare con il suffisso -o1-s3. Questo suffisso è riservato ai nomi alias dei punti di accesso Lambda per oggetti. Per ulteriori informazioni, consulta [Come utilizzare un alias in stile bucket per il punto di accesso Lambda per oggetti del bucket S3](#).
- I nomi dei bucket non devono terminare con il suffisso .mr.ap. Questo suffisso è riservato ai nomi dei punti di Multi-Region accesso. Per ulteriori informazioni, consulta [Regole per la denominazione degli Access Point di Amazon S3 Multi-Region](#).

Un suffisso viene aggiunto automaticamente al nome di base fornito quando si crea un bucket di directory tramite la console. Questo suffisso include l'ID zona di disponibilità della zona di disponibilità scelta.

Una volta creato il bucket, non è possibile modificarne il nome. Per ulteriori informazioni sulla denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#).

 Important

Non includere informazioni sensibili, come i numeri di conto, nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

8. In Proprietà dell'oggetto, l'impostazione Proprietario del bucket è automaticamente abilitata e tutte le liste di controllo degli accessi (ACL) sono disabilitate. Per i bucket di directory, le ACL non possono essere abilitate.

Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket ha automaticamente il controllo completo di ogni oggetto di proprietà nel bucket per uso generico. Le liste di controllo degli accessi (ACL) non influiscono più sulle autorizzazioni di accesso ai dati nel bucket per uso generico S3. Il bucket utilizza esclusivamente le policy per definire il controllo degli accessi.

9. In Impostazioni di blocco dell'accesso pubblico per questo bucket, tutte le impostazioni di blocco dell'accesso pubblico per il bucket di directory sono automaticamente attivate. Queste impostazioni non possono essere modificate per i bucket di directory. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).
10. Per configurare la crittografia predefinita, in Tipo di crittografia scegli una delle seguenti opzioni:
 - Server-side crittografia con chiave gestita Amazon S3 () SSE-S3
 - Server-side crittografia con AWS Key Management Service chiave () SSE-KMS

Per ulteriori informazioni sull'utilizzo della crittografia lato server di Amazon S3 per crittografare i dati, consulta [Protezione e crittografia dei dati](#).

⚠ Important

Se si utilizza l' SSE-KMS opzione per la configurazione di crittografia predefinita, si è soggetti alla quota di richieste al secondo (RPS) di AWS KMS. Per ulteriori informazioni sulle quote AWS KMS e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Potrebbe essere necessario aggiornare le policy di bucket quando si abilita la crittografia predefinita. Per ulteriori informazioni, consulta [Utilizzo della SSE-KMS crittografia per le operazioni tra account](#).

11. Se hai scelto Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3), in Bucket Key viene visualizzato Enabled. Le chiavi S3 Bucket sono sempre abilitate quando configuri il bucket di directory con cui utilizzare la crittografia predefinita. SSE-S3 Le S3 Bucket Keys sono sempre abilitate per le operazioni GET e PUT in un bucket di directory e non possono essere disabilitate. Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket generici o tra bucket di directory, tramite [CopyObject](#) [UploadPartCopy](#), [l'operazione in Batch Operations o i job](#). [Copy import](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia di un oggetto. KMS-encrypted

Le chiavi S3 Bucket riducono il costo della crittografia diminuendo il traffico di richieste da Amazon S3 a AWS KMS. Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

12. Se hai scelto Server-side la crittografia con AWS Key Management Service key (SSE-KMS), in AWS KMS key, specifica la tua AWS Key Management Service chiave in uno dei seguenti modi o crea una nuova chiave.
 - Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS keys e scegli la tua chiave KMS da Disponibile. AWS KMS keys

In questo elenco vengono visualizzate solo le chiavi gestite dal cliente. La Chiave gestita da AWS (aws/s3) non è supportata nei bucket di directory. Per ulteriori informazioni sulle

chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per specificare l'ARN o l'alias della chiave KMS, scegli Inserisci l'ARN della AWS KMS key e immetti l'ARN o l'alias della chiave KMS in ARN della AWS KMS key .
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

Important

- La SSE-KMS configurazione può supportare solo 1 chiave gestita [dal cliente](#) per bucket di directory per tutta la durata del bucket. [Chiave gestita da AWS](#) (aws/s3) non è supportato. Inoltre, dopo aver specificato una chiave gestita dal cliente per SSE-KMS, non è possibile sovrascrivere la chiave gestita dal cliente per la configurazione del bucket. SSE-KMS

Puoi identificare la chiave gestita dal cliente che hai specificato per la SSE-KMS configurazione del bucket nel modo seguente:

- Si effettua una richiesta di operazione API HeadObject per trovare il valore di x-amz-server-side-encryption-aws-kms-key-id nella risposta.

Per utilizzare una nuova chiave gestita dal cliente per i propri dati, si consiglia di copiare gli oggetti esistenti in un nuovo bucket della directory con una nuova chiave gestita dal cliente.

- È possibile utilizzare solo le chiavi KMS disponibili nello stesso bucket della Regione AWS. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, devi inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione necessaria per l'uso della chiave e quindi inserire l'ARN della chiave KMS. Per ulteriori informazioni sulle autorizzazioni tra account per le chiavi KMS, consulta [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service . Per ulteriori informazioni su SSE-KMS, consulta [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\) per il caricamento di nuovi oggetti nei bucket di directory](#)

- Quando si utilizza una AWS KMS key crittografia lato server nei bucket di directory, è necessario scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni sull'utilizzo AWS KMS con Amazon S3, consulta. [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket di directory](#)

13. Seleziona Crea bucket. Dopo aver creato il bucket, puoi aggiungere file e cartelle al bucket. Per ulteriori informazioni, consulta [the section called “Utilizzo di oggetti in un bucket di directory”](#).

Utilizzo di AWS SDK

SDK for Go

Questo esempio mostra come creare un bucket di directory utilizzando il comando AWS SDK per Go.

Example

```
var bucket = "..."  
  
func runCreateBucket(c *s3.Client) {  
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{  
        Bucket: &bucket,  
        CreateBucketConfiguration: &types.CreateBucketConfiguration{  
            Location: &types.LocationInfo{  
                Name: aws.String("usw2-az1"),  
                Type: types.LocationTypeAvailabilityZone,  
            },  
            Bucket: &types.BucketInfo{  
                DataRedundancy: types.DataRedundancySingleAvailabilityZone,  
                Type: types.BucketTypeDirectory,  
            },  
        },  
    })  
    var terr *types.BucketAlreadyOwnedByYou  
    if errors.As(err, &terr) {  
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))  
    }  
}
```

```

        fmt.Printf("noop...\n")
        return
    }
    if err != nil {
        log.Fatal(err)
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}

```

SDK for Java 2.x

Questo esempio mostra come creare un bucket di directory utilizzando il comando AWS SDK for Java 2.x.

Example

```

public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{az-id}--x-s3
    //example: doc-example-bucket--usw2-az1--x-s3 is a valid name for a directory
    bucket created in
    //Region us-west-2, Availability Zone 2

    CreateBucketConfiguration bucketConfiguration =
    CreateBucketConfiguration.builder()
        .location(LocationInfo.builder()
            .type(LocationType.AVAILABILITY_ZONE)
            .name("usw2-az1").build()) //this must match the Region and
    Availability Zone in your bucket name
        .bucket(BucketInfo.builder()
            .type(BucketType.DIRECTORY)
            .dataRedundancy(DataRedundancy.SINGLE_AVAILABILITY_ZONE)
            .build()).build();

    try {

        CreateBucketRequest bucketRequest =
        CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfiguration)
        CreateBucketResponse response = s3Client.createBucket(bucketRequest);
        System.out.println(response);
    }

    catch (S3Exception e) {

```

```
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

AWS SDK per JavaScript

Questo esempio mostra come creare un bucket di directory utilizzando il comando AWS SDK per JavaScript.

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "us-east-1";
const zone = "use1-az4";
const suffix = `${zone}--x-s3`;

const s3 = new S3({ region });

const bucketName = `...--${suffix}`;

const createResponse = await s3.createBucket(
  { Bucket: bucketName,
    CreateBucketConfiguration: {Location: {Type: "AvailabilityZone", Name: zone},
    Bucket: { Type: "Directory", DataRedundancy: "SingleAvailabilityZone" }}
  );
```

SDK per .NET

Questo esempio mostra come creare un bucket di directory utilizzando il comando SDK per .NET.

Example

```
using (var amazonS3Client = new AmazonS3Client())
```

```
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {
        BucketName = "DOC-EXAMPLE-BUCKET--usw2-az1--x-s3",
        PutBucketConfiguration = new PutBucketConfiguration
        {
            BucketInfo = new BucketInfo { DataRedundancy =
            DataRedundancy.SingleAvailabilityZone, Type = BucketType.Directory },
            Location = new LocationInfo { Name = "usw2-az1", Type =
            LocationType.AvailabilityZone }
        }
    }).ConfigureAwait(false);
}
```

SDK for PHP

Questo esempio mostra come creare un bucket di directory utilizzando il comando AWS SDK for PHP.

Example

```
require 'vendor/autoload.php';

$s3Client = new S3Client([

    'region'      => 'us-east-1',
]);

$result = $s3Client->createBucket([
    'Bucket' => 'doc-example-bucket--use1-az4--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'use1-az4', 'Type'=> 'AvailabilityZone'],
        'Bucket' => ["DataRedundancy" => "SingleAvailabilityZone" ,"Type" =>
        "Directory"]    ],
    ]);
```

SDK for Python

Questo esempio mostra come creare un bucket di directory utilizzando il comando AWS SDK per Python (Boto3).

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def create_bucket(s3_client, bucket_name, availability_zone):
    """
    Create a directory bucket in a specified Availability Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'doc-example-bucket--usw2-az1--x-s3'
    :param availability_zone: String; Availability Zone ID to create the bucket in,
    for example, 'usw2-az1'
    :return: True if bucket is created, else False
    """

    try:
        bucket_config = {
            'Location': {
                'Type': 'AvailabilityZone',
                'Name': availability_zone
            },
            'Bucket': {
                'Type': 'Directory',
                'DataRedundancy': 'SingleAvailabilityZone'
            }
        }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    availability_zone = 'usw2-az1'
    s3_client = boto3.client('s3', region_name = region)
```

```
create_bucket(s3_client, bucket_name, availability_zone)
```

SDK for Ruby

Questo esempio mostra come creare un bucket di directory utilizzando il comando AWS SDK per Ruby.

Example

```
s3 = Aws::S3::Client.new(region:'us-west-2')
s3.create_bucket(
  bucket: "bucket_base_name--az_id--x-s3",
  create_bucket_configuration: {
    location: { name: 'usw2-az1', type: 'AvailabilityZone' },
    bucket: { data_redundancy: 'SingleAvailabilityZone', type: 'Directory' }
  }
)
```

Utilizzo di AWS CLI

Questo esempio mostra come creare un bucket di directory utilizzando il comando AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Quando si crea un bucket di directory, è necessario fornire i dettagli di configurazione e utilizzare la seguente convenzione di denominazione: *bucket-base-name--zone-id--x-s3*

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=AvailabilityZone,Name=usw2-az1},Bucket={DataRedundancy=SingleAvailabilityZone,Type=Directory}'
--region us-west-2
```

Per ulteriori informazioni, consulta [create-bucket](#) in AWS Command Line Interface.

Endpoint regionali e di zona per i bucket di directory in una zona di disponibilità

Per accedere agli oggetti e ai bucket della directory archiviati in S3 Express One Zone, si utilizzano gli endpoint del gateway VPC. I bucket della directory utilizzano gli endpoint API regionali e di zona. A seconda dell'operazione API Amazon S3 utilizzata, è necessario un endpoint regionale o zonale. L'utilizzo di endpoint gateway non comporta costi supplementari.

Bucket-level Le operazioni API (o piano di controllo) sono disponibili tramite gli endpoint regionali e sono denominate operazioni API per endpoint regionali. Esempi di operazioni API degli endpoint regionali sono `CreateBucket` e `DeleteBucket`.

Quando si creano bucket di directory archiviati in S3 Express One Zone, si sceglie la zona di disponibilità in cui si trova il bucket. È possibile utilizzare le operazioni API endpoint di zona per caricare e gestire gli oggetti nel bucket della directory.

Object-level Le operazioni API (o piano dati) sono disponibili tramite gli endpoint zonali e sono denominate operazioni API degli endpoint zonali. Esempi di operazioni API degli endpoint zonali sono `CreateSession` e `PutObject`.

Ottimizzazione delle prestazioni di S3 Express One Zone

Amazon S3 Express One Zone è una classe di storage S3 ad alte prestazioni e a singola zona di disponibilità (AZ), creata appositamente per offrire un accesso ai dati costante e a una cifra al millisecondo per le applicazioni più sensibili alla latenza. S3 Express One Zone è la prima classe di storage S3 che offre la possibilità di co-localizzare risorse di storage e calcolo di oggetti ad alte prestazioni, come Amazon Elastic AWS Compute Cloud, Amazon Elastic Kubernetes Service e Amazon Elastic Container Service, all'interno di un'unica zona di disponibilità. Co-locating le tue risorse di storage ed elaborazione ottimizzano le prestazioni e i costi di elaborazione e forniscono una maggiore velocità di elaborazione dei dati.

S3 Express One Zone fornisce elasticità delle prestazioni simile a quella delle altre classi di storage S3, ma con latenze coerenti di richiesta di lettura e scrittura per il primo byte di pochi millisecondi, fino a 10 volte più rapidamente di S3 Standard. S3 Express One Zone è progettato da zero per supportare un throughput ottimale fino a livelli di aggregazione molto elevati. La classe di storage S3 Express One Zone utilizza un'architettura personalizzata per ottimizzare le prestazioni e offrire una latenza di richiesta costantemente bassa archiviando i dati su hardware ad alte prestazioni. Il protocollo a oggetti per S3 Express One Zone è stato migliorato per ottimizzare l'autenticazione e il sovraccarico di metadati.

Per ridurre ulteriormente la latenza e supportare fino a 2 milioni di letture e fino a 200.000 scritture al secondo, S3 Express One Zone archivia i dati in un bucket di directory Amazon S3. Per impostazione predefinita, ogni bucket di directory supporta fino a 200.000 letture e fino a 100.000 scritture al secondo. Se il carico di lavoro richiede limiti TPS superiori a quelli predefiniti, è possibile richiedere un aumento tramite il [Supporto AWS](#).

La combinazione di hardware e software dedicati ad alte prestazioni che forniscono una velocità di accesso ai dati di pochi millisecondi e bucket di directory in grado di dimensionarsi per un numero

elevato di transazioni al secondo, rende S3 Express One Zone la classe di storage Amazon S3 migliore per operazioni con un elevato numero di richieste o applicazioni con prestazioni critiche.

Nei seguenti argomenti vengono descritte le linee guida sulle best practice e i modelli di progettazione per l'ottimizzazione delle prestazioni con applicazioni che utilizzano la classe di storage S3 Express One Zone.

Argomenti

- [Best practice per ottimizzare le prestazioni di S3 Express One Zone](#)

Best practice per ottimizzare le prestazioni di S3 Express One Zone

Durante la creazione di applicazioni che caricano e recuperano oggetti da Amazon S3 Express One Zone, segui le nostre linee guida sulle best practice per ottimizzare le prestazioni. Per utilizzare la classe di archiviazione S3 Express One Zone, devi creare una directory di bucket S3. La classe di archiviazione S3 Express One Zone non è supportata per l'utilizzo con bucket per uso generico S3.

Per le linee guida sulle prestazioni per tutte le altre classi di archiviazione Amazon S3 e i bucket per uso generico S3, consulta [Best practice e modelli di progettazione: ottimizzazione delle prestazioni di Amazon S3](#).

Per prestazioni e scalabilità ottimali con la classe di archiviazione S3 Express One Zone e i bucket di directory in carichi di lavoro su larga scala, è importante capire in che modo i bucket di directory sono diversi dai bucket generici. Pertanto, di seguito sono fornite le best practice per allineare le applicazioni al modo in cui funzionano i bucket di directory.

Come funzionano i bucket di directory

La classe di archiviazione Amazon S3 Express One Zone può supportare carichi di lavoro con un massimo di 2.000.000 transazioni GET e fino a 200.000 transazioni PUT al secondo (TPS) per ogni bucket di directory. Con S3 Express One Zone, i dati sono archiviati in bucket di directory S3 situati nelle zone di disponibilità. Gli oggetti nei bucket di directory sono accessibili all'interno di un namespace gerarchico, simile a un file system, a differenza dei bucket per uso generico S3 che hanno un namespace semplice. A differenza dei bucket per uso generico, i bucket di directory organizzano le chiavi in maniera gerarchica in directory anziché prefissi. Un prefisso è una stringa di caratteri all'inizio del nome della chiave dell'oggetto. È possibile utilizzare i prefissi per organizzare i dati e gestire un'architettura di archiviazione degli oggetti semplice in bucket per uso generico. Per ulteriori informazioni, consulta [Organizzazione degli oggetti utilizzando i prefissi](#).

Nei bucket di directory, gli oggetti sono organizzati in un namespace gerarchico utilizzando la barra (/) come unico delimitatore supportato. Quando carichi un oggetto con una chiave come `dir1/dir2/file1.txt`, le directory `dir1/` e `dir2/` vengono create e gestite automaticamente da Amazon S3. Le directory vengono create durante le operazioni `PutObject` o `CreateMultiPartUpload` e rimosse automaticamente quando sono vuote dopo le operazioni `DeleteObject` o `AbortMultiPartUpload`. Non esiste alcun limite massimo al numero di oggetti e sottodirectory presenti in una directory.

Le directory create quando gli oggetti vengono caricati nei bucket di directory possono scalare istantaneamente per ridurre la possibilità di errori HTTP 503 (`Slow Down`). Questo dimensionamento automatico consente alle applicazioni di parallelizzare le richieste di lettura e scrittura all'interno e tra le directory in base alle esigenze. Per S3 Express One Zone, le singole directory sono progettate per supportare la frequenza massima di richieste di un bucket di directory. Non è necessario applicare la randomizzazione dei prefissi delle chiavi per ottenere prestazioni ottimali perché il sistema distribuisce automaticamente gli oggetti con una distribuzione uniforme del carico, ma di conseguenza, le chiavi non vengono archiviate in base all'ordine lessicografico nei bucket di directory. Questo comportamento è in contrasto con i bucket per uso generico S3, in cui è più probabile che le chiavi simili dal punto di vista lessicografico siano collocate sullo stesso server.

Per ulteriori informazioni sugli esempi di operazioni di bucket di directory e interazioni tra directory, consulta [Esempi di funzionamento del bucket di directory e di interazione con le directory](#).

Best practice

Segui le best practice per ottimizzare le prestazioni del bucket di directory e consentire ai carichi di lavoro di scalare nel tempo.

Utilizzare directory contenenti molte voci (oggetti o sottodirectory)

I bucket di directory offrono prestazioni elevate per impostazione predefinita per tutti i carichi di lavoro. Per un'ottimizzazione ancora maggiore delle prestazioni con determinate operazioni, il consolidamento di più voci (ossia oggetti o sottodirectory) nelle directory comporta una latenza inferiore e una frequenza di richieste più elevata:

- Le operazioni API mutanti, come `PutObject`, `DeleteObject`, `CreateMultiPartUpload` e `AbortMultiPartUpload`, ottengono prestazioni ottimali se implementate con un numero contenuto di directory più dense con migliaia di voci, anziché con un numero elevato di directory più piccole.

- Le operazioni `ListObjectsV2` funzionano meglio quando si devono attraversare meno directory per popolare una pagina di risultati.

Non utilizzare l'entropia nei prefissi

Nelle operazioni di Amazon S3, l'entropia si riferisce alla randomizzazione nella denominazione dei prefissi che aiuta a distribuire i carichi di lavoro in modo uniforme tra le partizioni di archiviazione. Tuttavia, poiché i bucket di directory gestiscono internamente la distribuzione del carico, non è consigliabile utilizzare l'entropia nei prefissi per migliorare le prestazioni. Questo perché per i bucket di directory, l'entropia può rallentare le richieste non riutilizzando le directory che sono già state create.

Un modello di chiave come `$HASH/directory/object` potrebbe finire per creare molte directory intermedie. Nel seguente esempio, tutti i `job-1` sono directory diverse perché gli elementi principali sono diversi. Le directory saranno piccole e le richieste di mutazione e di elenco saranno più lente. In questo esempio ci sono 12 directory intermedie che hanno tutte una singola voce.

```
s3://my-bucket/0cc175b9c0f1b6a831c399e269772661/job-1/file1
s3://my-bucket/92eb5ffee6ae2fec3ad71c777531578f/job-1/file2
s3://my-bucket/4a8a08f09d37b73795649038408b5f33/job-1/file3
s3://my-bucket/8277e0910d750195b448797616e091ad/job-1/file4
s3://my-bucket/e1671797c52e15f763380b45e841ec32/job-1/file5
s3://my-bucket/8fa14cdd754f91cc6554c9e71929cce7/job-1/file6
```

Per ottenere prestazioni ottimali, è possibile rimuovere il componente `$HASH` e consentire a `job-1` di diventare una singola directory, migliorando la densità della directory. Nell'esempio seguente, la singola directory intermedia con sei voci può ottenere prestazioni migliori rispetto all'esempio precedente.

```
s3://my-bucket/job-1/file1
s3://my-bucket/job-1/file2
s3://my-bucket/job-1/file3
```

```
s3://my-bucket/job-1/file4  
  
s3://my-bucket/job-1/file5  
  
s3://my-bucket/job-1/file6
```

Questo vantaggio in termini di prestazioni si verifica perché quando una chiave dell'oggetto viene inizialmente creata e il relativo nome della chiave include una directory, la directory viene creata automaticamente per l'oggetto. I successivi caricamenti di oggetti nella stessa directory non richiedono la creazione della directory, riducendo pertanto la latenza su caricamenti di oggetti nelle directory esistenti.

Usa un separatore diverso dal delimitatore/ per separare le parti della chiave se non hai bisogno della capacità di raggruppare logicamente gli oggetti durante le chiamate V2 **ListObjects**

Poiché il delimitatore / è trattato in modo speciale per i bucket di directory, deve essere utilizzato intenzionalmente. Sebbene i bucket di directory non dispongano gli oggetti in base all'ordine lessicografico, gli oggetti all'interno di una directory sono comunque raggruppati in output **ListObjectsV2**. Se non è necessaria questa funzionalità, puoi sostituire / con un altro carattere come separatore per evitare la creazione di directory intermedie.

Ad esempio, supponi che le seguenti chiavi siano nel modello di prefisso YYYY/MM/DD/HH/

```
s3://my-bucket/2024/04/00/01/file1  
  
s3://my-bucket/2024/04/00/02/file2  
  
s3://my-bucket/2024/04/00/03/file3  
  
s3://my-bucket/2024/04/01/01/file4  
  
s3://my-bucket/2024/04/01/02/file5  
  
s3://my-bucket/2024/04/01/03/file6
```

Se non è necessario raggruppare gli oggetti in base all'ora o al giorno nei risultati di **ListObjectsV2**, ma è necessario raggruppare gli oggetti in base al mese, il seguente modello di chiave YYYY/MM/DD-HH- consente di ridurre notevolmente il numero di directory e di migliorare le prestazioni dell'operazione **ListObjectsV2**.

```
s3://my-bucket/2024/04/00-01-file1
```

```
s3://my-bucket/2024/04/00-01-file2  
  
s3://my-bucket/2024/04/00-01-file3  
  
s3://my-bucket/2024/04/01-02-file4  
  
s3://my-bucket/2024/04/01-02-file5  
  
s3://my-bucket/2024/04/01-02-file6
```

Utilizzare operazioni con elenchi delimitati se possibile

Una richiesta `ListObjectsV2` senza `delimiter` esegue l'attraversamento ricorsivo `depth-first` di tutte le directory. Una richiesta `ListObjectsV2` con `delimiter` recupera solo le voci nella directory specificata dal parametro `prefix`, riducendo la latenza della richiesta e aumentando le chiavi aggregate al secondo. Per i bucket di directory, utilizza operazioni con elenchi delimitati, ove possibile. Gli elenchi delimitati fanno sì che le directory vengano visitate meno volte, il che comporta più chiavi al secondo e una minore latenza delle richieste.

Ad esempio, considera le directory e gli oggetti seguenti presenti nel bucket di directory:

```
s3://my-bucket/2024/04/12-01-file1  
  
s3://my-bucket/2024/04/12-01-file2  
  
...  
  
s3://my-bucket/2024/05/12-01-file1  
  
s3://my-bucket/2024/05/12-01-file2  
  
...  
  
s3://my-bucket/2024/06/12-01-file1  
  
s3://my-bucket/2024/06/12-01-file2  
  
...  
  
s3://my-bucket/2024/07/12-01-file1  
  
s3://my-bucket/2024/07/12-01-file2
```

...

Per migliorare le prestazioni di `ListObjectsV2`, utilizza un elenco delimitato per elencare le sottodirectory e gli oggetti, se la logica dell'applicazione lo consente. Ad esempio, puoi eseguire il comando seguente per l'operazione con elenco delimitato:

```
aws s3api list-objects-v2 --bucket my-bucket --prefix '2024/' --delimiter '/'
```

L'output è l'elenco delle sottodirectory.

```
{
  "CommonPrefixes": [
    {
      "Prefix": "2024/04/"
    },
    {
      "Prefix": "2024/05/"
    },
    {
      "Prefix": "2024/06/"
    },
    {
      "Prefix": "2024/07/"
    }
  ]
}
```

Per elencare ogni sottodirectory con le prestazioni migliori, puoi eseguire un comando simile all'esempio seguente.

Comando:

```
aws s3api list-objects-v2 --bucket my-bucket --prefix '2024/04' --delimiter '/'
```

Output:

```
{
  "Contents": [
    {
      "Key": "2024/04/12-01-file1"
    },
  ],
}
```

```
{
  "Key": "2024/04/12-01-file2"
}
```

Co-locate Storage S3 Express One Zone con le tue risorse di elaborazione

Con S3 Express One Zone, ogni bucket di directory si trova in una singola zona di disponibilità che selezioni quando crei il bucket. Puoi iniziare creando un nuovo bucket di directory in una zona di disponibilità locale nei carichi di lavoro o nelle risorse di calcolo. Quindi, puoi iniziare immediatamente letture e scritture a latenza molto bassa. I bucket Directory sono un tipo di bucket S3 in cui è possibile scegliere la zona di disponibilità in una Regione AWS per ridurre la latenza tra elaborazione e archiviazione.

Se accedi ai bucket di directory tra zone di disponibilità, è possibile che si verifichi un leggero aumento della latenza. Per ottimizzare le prestazioni, ti consigliamo di accedere a un bucket di directory dalle istanze di Amazon Elastic Container Service, Amazon Elastic Kubernetes Service e Amazon Elastic Compute Cloud che si trovano nella stessa zona di disponibilità, se possibile.

Utilizzare connessioni simultanee per ottenere un throughput elevato con oggetti superiori a 1 MB

Puoi ottenere prestazioni ottimali inviando più richieste simultanee ai bucket di directory per distribuire le richieste su connessioni separate per massimizzare la larghezza di banda accessibile. Come per i bucket per uso generico, S3 Express One Zone non impone limiti al numero di connessioni effettuate al bucket di directory. Le singole directory possono dimensionare le prestazioni orizzontalmente e automaticamente quando si verifica un numero elevato di scritture simultanee nella stessa directory.

Le singole connessioni TCP ai bucket di directory hanno un limite massimo fisso per il numero di byte che possono essere caricati o scaricati al secondo. Quando gli oggetti diventano più grandi, i tempi di richiesta vengono dominati dallo streaming di byte anziché dall'elaborazione della transazione. Per utilizzare più connessioni per parallelizzare il caricamento o il download di oggetti di grandi dimensioni, puoi ridurre la latenza end-to-end. Se utilizzi Java 2.x SDK, dovrai prendere in considerazione l'utilizzo di [S3 Transfer Manager](#), che sfrutta i miglioramenti delle prestazioni come le [operazioni API di caricamento in più parti](#) e il recupero di intervalli di byte per accedere ai dati in parallelo.

Utilizzare gli endpoint VPC del gateway

Gli endpoint del gateway forniscono la connessione diretta dal VPC ai bucket di directory, senza richiedere un gateway Internet o un dispositivo NAT per il VPC. Per ridurre il tempo che i pacchetti

trascorrono sulla rete, è necessario configurare il VPC con un endpoint VPC del gateway per i bucket di directory. Per ulteriori informazioni, consulta [Collegamento in rete per i bucket di directory](#).

Utilizzare l'autenticazione della sessione e riutilizzare i token di sessione finché validi

I bucket di directory forniscono un meccanismo di autenticazione dei token di sessione per ridurre la latenza sulle operazioni API sensibili alle prestazioni. È possibile effettuare una singola chiamata a `CreateSession` per ottenere un token di sessione valido per tutte le richieste nei 5 minuti successivi. Per ottenere la latenza più bassa nelle chiamate API, assicurati di acquisire un token di sessione e riutilizzarlo per la sua intera durata prima di aggiornarlo.

Se utilizzi gli SDK, AWS gli SDK gestiscono automaticamente gli aggiornamenti del token di sessione per evitare interruzioni del servizio alla scadenza di una sessione. Ti consigliamo di utilizzare gli AWS SDK per avviare e gestire le richieste al funzionamento dell'API. `CreateSession`

Per ulteriori informazioni su `CreateSession`, consultare [Autorizzazione delle operazioni API dell'endpoint di zona con `CreateSession`](#).

Usa un client CRT-based

Il AWS Common Runtime (CRT) è un insieme di librerie modulari, performanti ed efficienti scritte in C e destinate a fungere da base per gli SDK. AWS CRT offre un maggiore throughput, una migliore gestione delle connessioni e tempi di avvio più rapidi. Il CRT è disponibile tramite tutti gli SDK tranne Go. AWS

Per ulteriori informazioni su come configurare il CRT per l'SDK che utilizzi, consulta le librerie [AWS Common Runtime \(CRT\)](#), [Accelerate il throughput di Amazon S3 con AWS Common Runtime](#), [Introducing CRT-based S3 client e S3 Transfer Manager nell' AWS SDK for Java 2.x](#), [Using for Amazon S3 operations e Configurazione dei client HTTP. S3CrtClient](#) [AWS CRT-based](#)

Usa la versione più recente di AWS SDK

Gli AWS SDK forniscono il supporto integrato per molte delle linee guida consigliate per l'ottimizzazione delle prestazioni di Amazon S3. Gli SDK offrono un'API più semplice per utilizzare al meglio Amazon S3 internamente a un'applicazione e vengono aggiornati regolarmente in modo da seguire le best practice più recenti. Ad esempio, gli SDK riprovano automaticamente le richieste dopo gli errori HTTP 503 e gestiscono le risposte di connessioni lente.

Se utilizzi l'Java 2.x SDK, dovresti prendere in considerazione l'utilizzo di [S3 Transfer Manager](#), che ridimensiona automaticamente le connessioni orizzontalmente per ottenere migliaia di richieste al secondo utilizzando richieste con intervallo di byte, se necessario. Byte-range le richieste possono

migliorare le prestazioni perché è possibile utilizzare connessioni simultanee a S3 per recuperare intervalli di byte diversi dall'interno dello stesso oggetto. Questa operazione ti permette di ottenere un throughput aggregato superiore rispetto a una singola richiesta whole-object. Quindi è importante utilizzare l'ultima versione degli AWS SDK per ottenere le ultime funzionalità di ottimizzazione delle prestazioni.

Risoluzione dei problemi relativi alle prestazioni

Si impostano le richieste dei tentativi per applicazioni sensibili alla latenza?

S3 Express One Zone è progettato appositamente per offrire livelli costanti di alte prestazioni senza ulteriori regolazioni. Tuttavia, l'impostazione di valori di timeout aggressivi e nuovi tentativi possono contribuire ulteriormente a garantire latenza e prestazioni costanti. Gli AWS SDK hanno valori di timeout e ripetizione configurabili che puoi adattare alle tolleranze della tua applicazione specifica.

Stai usando AWS Librerie Common Runtime (CRT) e tipi di istanze Amazon EC2 ottimali?

Le applicazioni che eseguono un elevato numero di operazioni di lettura e scrittura richiedono una capacità di memoria o calcolo superiore rispetto alle applicazioni che non eseguono tali operazioni. Durante il lancio delle istanze Amazon Elastic Compute Cloud (Amazon EC2) per carichi di lavoro esigenti in termini di prestazioni, scegli i tipi di istanza che dispongono della quantità di risorse necessaria per l'applicazione. L'archiviazione ad alte prestazioni S3 Express One Zone è abbinata idealmente a tipi di istanza più recenti con quantità maggiori di memoria di sistema, nonché CPU e GPU più potenti che possono sfruttare l'archiviazione ad alte prestazioni. Consigliamo inoltre di utilizzare le versioni più recenti degli CRT-enabled AWS SDK, che possono accelerare meglio le richieste di lettura e scrittura in parallelo.

Stai usando AWS SDK per l'autenticazione basata sulla sessione?

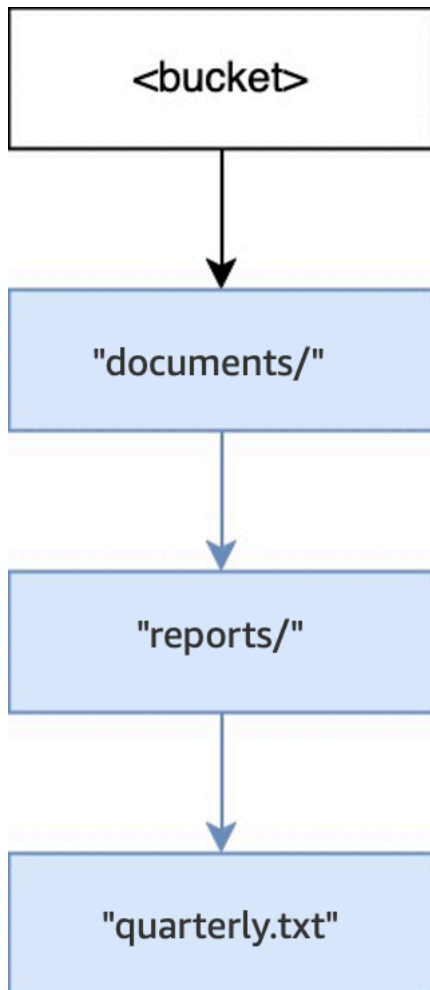
Con Amazon S3, puoi anche ottimizzare le prestazioni quando usi le richieste HTTP REST API seguendo le stesse best practice che fanno parte degli SDK. AWS Tuttavia, con il meccanismo di autorizzazione e autenticazione basato sulla sessione utilizzato da S3 Express One Zone, consigliamo vivamente di utilizzare gli AWS SDK per la gestione e il relativo token di sessione gestito `CreateSession`. Gli AWS SDK creano e aggiornano automaticamente i token per tuo conto utilizzando l'operazione `API. CreateSession`. Utilizzo dei `CreateSession` salvataggi sulla latenza di andata e ritorno per richiesta su (IAM) per AWS Identity and Access Management autorizzare ogni richiesta.

Esempi di funzionamento del bucket di directory e di interazione con le directory

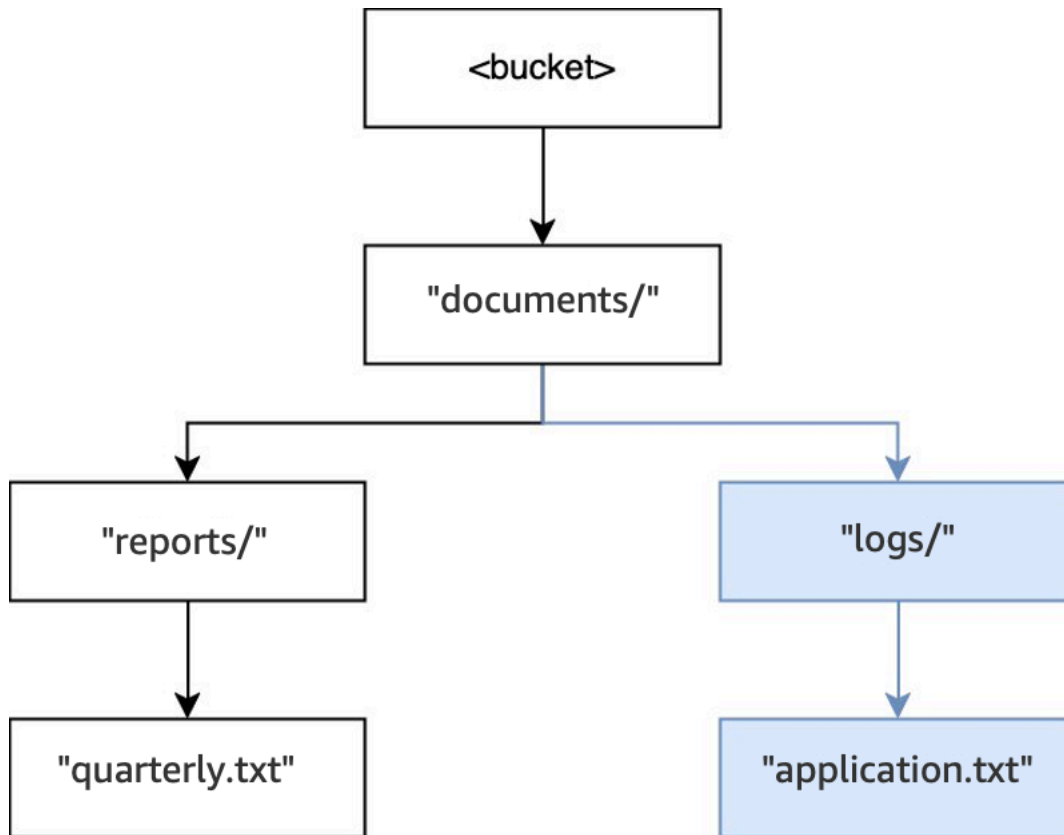
Di seguito vengono illustrati tre esempi su come funzionano i bucket di directory.

Esempio 1: in che modo le richieste **PutObject** S3 a un bucket di directory interagiscono con le directory

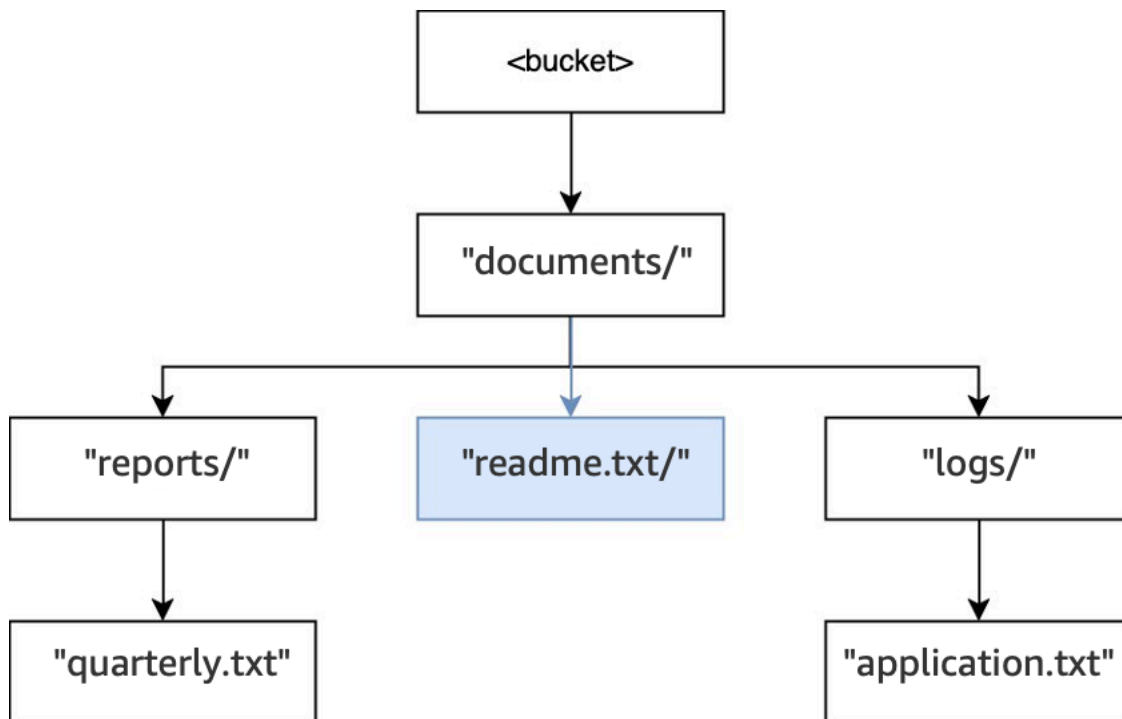
1. Quando l'operazione `PUT(<bucket>, "documents/reports/quarterly.txt")` viene eseguita in un bucket vuoto, viene creata la directory `documents/` all'interno della root del bucket, viene creata la directory `reports/` all'interno di `documents/` e viene creato l'oggetto `quarterly.txt` all'interno di `reports/`. Per questa operazione, sono state create due directory oltre all'oggetto.



2. Quindi, quando viene eseguita un'altra operazione `PUT(<bucket>, "documents/logs/application.txt")`, la directory `documents/` esiste già, la directory `logs/` non esiste all'interno di `documents/` e viene creata e viene creato l'oggetto `application.txt` all'interno di `logs/`. Per questa operazione, è stata creata una sola directory oltre all'oggetto.



3. Infine, quando viene eseguita un'operazione PUT(`<bucket>`, `"documents/readme.txt"`), la directory `documents/` all'interno della root esiste già e l'oggetto `readme.txt` viene creato. Per questa operazione, non viene creata alcuna directory.



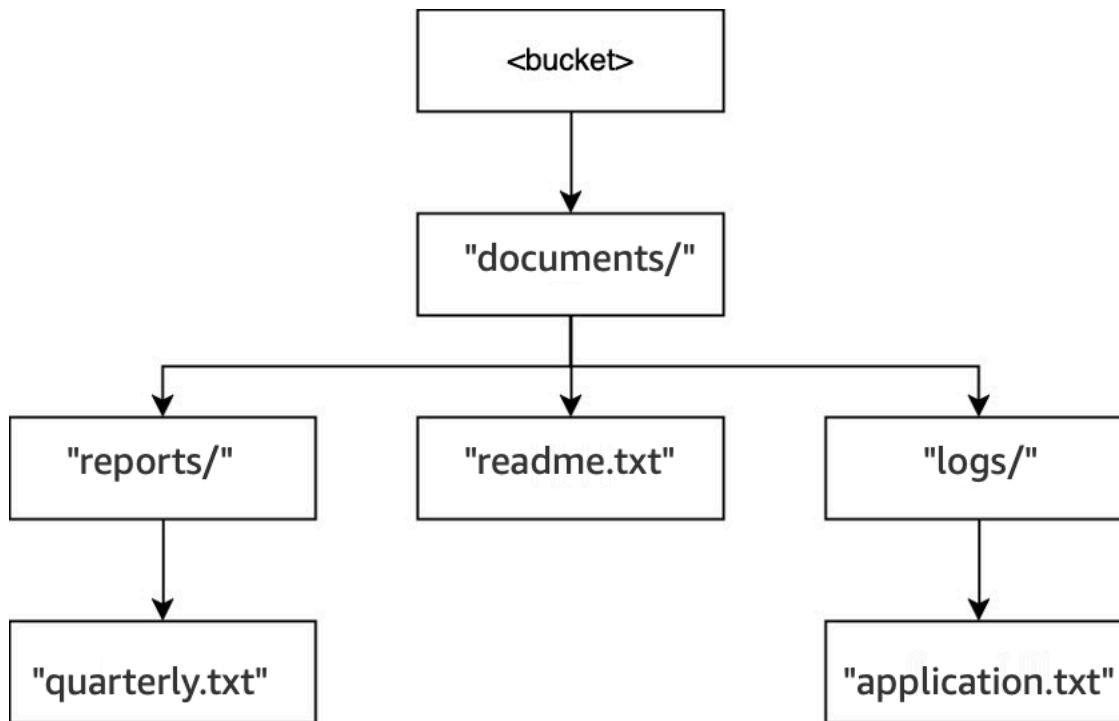
Esempio 2: come le **richieste S3 ListObjects V2** a un bucket di directory interagiscono con le directory

Per le richieste `ListObjectsV2` S3 senza un delimitatore, un bucket viene attraversato in modalità `depth-first`. Gli output vengono restituiti in un ordine coerente. Tuttavia, sebbene questa disposizione rimanga la stessa tra le richieste, non è in ordine lessicografico. Per il bucket e le directory creati nell'esempio precedente:

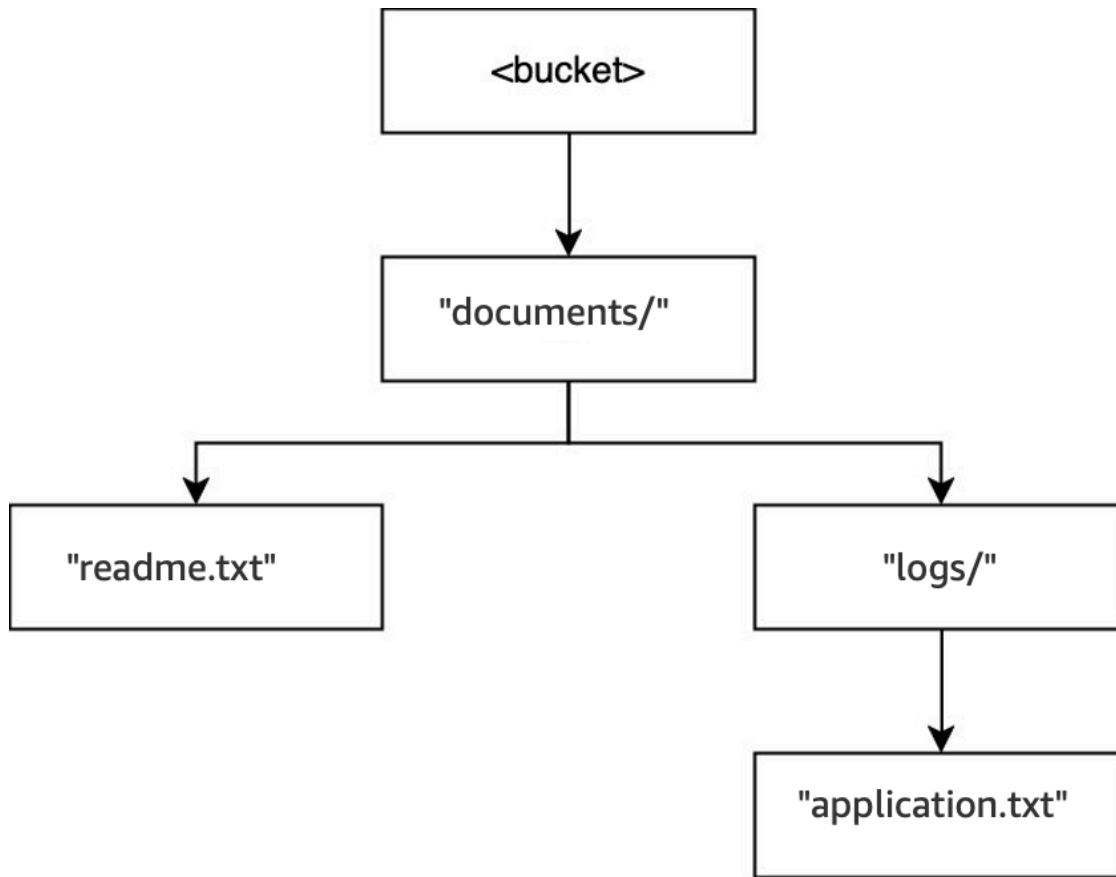
1. Quando viene eseguito `LIST(<bucket>)`, la directory `documents/` viene inserita e ha inizio l'attraversamento.
2. La sottodirectory `logs/` viene inserita e ha inizio l'attraversamento.
3. L'oggetto `application.txt` si trova all'interno di `logs/`.
4. All'interno di `logs/` non esistono altre voci. L'operazione `List` esce da `logs/` ed entra nuovamente in `documents/`.
5. La directory `documents/` continua a essere attraversata e l'oggetto `readme.txt` viene trovato.
6. La directory `documents/` continua a essere attraversata, la sottodirectory `reports/` viene inserita e l'attraversamento ha inizio.
7. L'oggetto `quarterly.txt` si trova all'interno di `reports/`.
8. All'interno di `reports/` non esistono altre voci. L'elenco esce da `reports/` ed entra di nuovo in `documents/`.
9. Non esistono altre voci all'interno di `documents/` e viene restituito l'elenco.

In questo esempio, `logs/` viene ordinato prima di `readme.txt` e `readme.txt` viene ordinato prima di `reports/`.

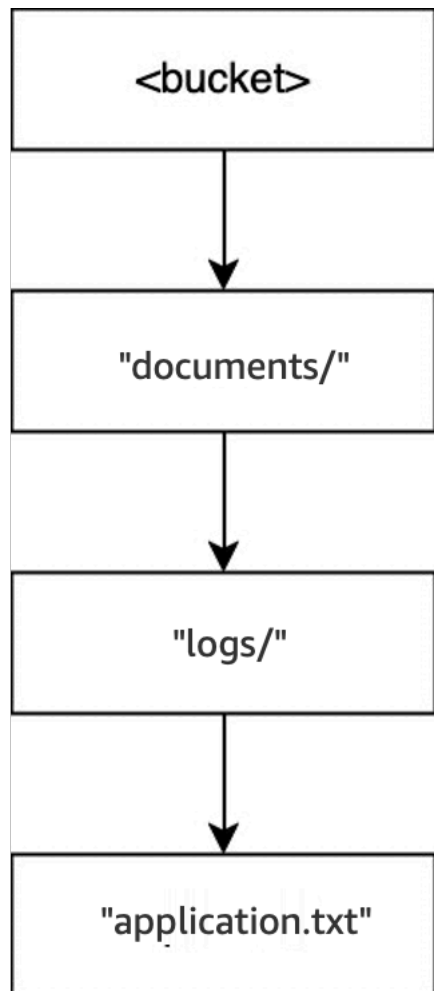
Esempio 3: in che modo le richieste **DeleteObject** S3 a un bucket di directory interagiscono con le directory



1. Nello stesso bucket, quando viene eseguita l'operazione `DELETE(<bucket>, "documents/reports/quarterly.txt")`, l'oggetto `quarterly.txt` viene eliminato, lasciando la directory `reports/` vuota e provocandone l'eliminazione immediata. La directory `documents/` non è vuota perché contiene sia la directory `logs/` sia l'oggetto `readme.txt`, quindi non viene eliminata. Per questa operazione, sono stati eliminati un solo oggetto e una sola directory.



2. Quando l'operazione `DELETE(<bucket>, "documents/readme.txt")` viene eseguita, l'oggetto `readme.txt` viene eliminato. `documents/` non è ancora vuota perché contiene la directory `logs/`, quindi non viene eliminata. Per questa operazione, non viene eliminata alcuna directory e viene eliminato solo l'oggetto.



3. Infine, quando viene eseguita l'operazione `DELETE(<bucket>, "documents/logs/application.txt")`, `application.txt` viene eliminato, lasciando `logs/` vuota e provocandone l'eliminazione immediata. Questa operazione lascia `documents/` vuota e viene anch'essa eliminata immediatamente. Per questa operazione, vengono eliminati due directory e un oggetto. Il bucket ora è vuoto.



Carichi di lavoro di residenza dei dati

I bucket di directory S3 sono disponibili in zone locali AWS dedicate e in zone locali selezionate. AWS Le zone locali dedicate (zone locali dedicate) sono un tipo di AWS infrastruttura completamente gestita da AWS, creata per l'uso esclusivo dell'utente o della comunità e collocata in una posizione

o in un data center specificato dall'utente per contribuire alla conformità ai requisiti normativi. Le zone locali dedicate sono un tipo di offerta di zone AWS locali (zone locali). Per ulteriori informazioni, consulta [Zone locali AWS dedicate](#).

Nelle zone locali dedicate è possibile creare bucket di directory S3 per archiviare i dati in un perimetro dei dati specifico, che aiuta a supportare i casi d'uso dell'isolamento e della residenza dei dati. I bucket di directory nelle zone locali dedicate possono supportare le classi di archiviazione S3 Express One Zone e S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA).

Una zona locale è un tipo di AWS infrastruttura che colloca determinati servizi di elaborazione, storage e altri servizi vicino a grandi popolazioni e centri industriali. Per saperne di più, consulta [Zone AWS locali](#). Puoi creare bucket di directory S3 per archiviare i dati in un perimetro di dati specifico, il che aiuta a supportare i casi d'uso della residenza dei dati. I bucket di directory nelle zone locali supportano la classe di archiviazione S3 One Zone-Infrequent Access (S3 One-IA; Z-IA). Per ulteriori informazioni sulle località supportate, consulta [AWS Local Zones](#).

Puoi utilizzare i bucket di directory nelle zone locali utilizzando l' Console di gestione AWS API REST, AWS Command Line Interface (AWS CLI) e gli AWS SDK.

Per ulteriori informazioni sull'utilizzo dei bucket di directory nelle Zone locali, consulta i seguenti argomenti:

Argomenti

- [Concetti per i bucket di directory nelle Zone locali](#)
- [Abilitazione di account per le zone locali](#)
- [Connettività privata dalla VPC](#)
- [Creazione di un bucket di directory in una zona locale](#)
- [Autenticazione e autorizzazione per i bucket di directory nelle Zone locali](#)

Concetti per i bucket di directory nelle Zone locali

Prima di creare un bucket di directory in una zona locale, è essenziale conoscere l'ID della zona locale in cui creare il bucket. Puoi trovare tutte le informazioni sulle zone locali utilizzando l'operazione [DescribeAvailabilityZones](#) API. Questa operazione API elenca le informazioni sulle zone locali, inclusi i relativi ID, i nomi delle Regioni principali, i gruppi di confine di rete e lo stato di adesione. Dopo aver ottenuto l'ID della zona locale e aver effettuato l'adesione, è possibile creare un bucket di directory nella zona locale. Un nome di bucket di directory è costituito da un nome di base

fornito dall'utente e da un suffisso che contiene l'ID della zona della posizione del bucket, seguito da --x-s3.

Una zona locale è collegata alla Regione padre utilizzando la rete privata ridondante e ad altissima larghezza di banda di Amazon. Ciò offre alle applicazioni in esecuzione nella zona locale un accesso rapido, sicuro e senza interruzioni al resto della Servizi AWS regione principale. ID zona principale è l'ID della zona che gestisce le operazioni del piano di controllo (control-plane) della zona locale. Network Border Group è un gruppo unico da cui AWS pubblica indirizzi IP pubblici. Per ulteriori informazioni sulle zone locali, sulla regione principale e sull'ID di zona principale, consulta i concetti relativi [AWS alle zone locali](#) nella Guida per l'utente delle zone AWS locali.

Tutti i bucket di directory utilizzano il namespace s3express, che è diverso dal namespace s3 per i bucket per uso generico. Per i bucket di directory, le richieste sono indirizzate a un endpoint regionale o a un endpoint di zona. Il routing viene gestito automaticamente per te se utilizzi gli SDK Console di gestione AWS, AWS CLI, o AWS .

Le maggior parte delle operazioni API a livello di bucket (come CreateBucket e DeleteBucket) viene indirizzata agli endpoint regionali e pertanto tali operazioni sono denominate operazioni API dell'endpoint regionale. Gli endpoint regionali sono nel formato s3express-control.ParentRegionCode.amazonaws.com. Tutte le operazioni API a livello di oggetto (come PutObject) e le due operazioni API a livello di bucket (CreateSession e HeadBucket) sono indirizzate agli endpoint di zona e sono denominate operazioni API endpoint di zona. Gli endpoint di zona sono nel formato s3express-LocalZoneID.ParentRegionCode.amazonaws.com. Per un elenco completo delle operazioni API per tipo di endpoint, consulta [Directory bucket API operations](#).

S3 è disponibile nella zona locale Pechino:

ID della zona locale: cnn1-pkx1-az1

Nome della Regione principale: China (Beijing)

Codice della Regione principale: cn-north-1

ID della zona principale: cnn1-az1

Nome della zona locale: China (Beijing)

Codice della zona locale: cnn1-pkx1-az1

Gruppo di confine di rete: cn-north-1-pkx-1

ARN del bucket di esempio: `arn:aws-cn:s3express:cn-north-1:123456789012:bucket/amzn-s3-demo-bucket--cn1-pkx1-az1--x-s3`

Endpoint regionale: `s3express-control.cn-north-1.amazonaws.com.cn`

Endpoint zonale: `s3express-cn1-pkx1-az1.cn-north-1.amazonaws.com.cn`

Classe di archiviazione: S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA)

Per accedere ai bucket di directory nelle Zone locali dal cloud privato virtuale (VPC), è possibile utilizzare endpoint VPC gateway. L'utilizzo di endpoint gateway non comporta costi supplementari. Per configurare gli endpoint del gateway VPC per accedere ai bucket di directory e agli oggetti nelle Zone locali, consulta [Connettività privata dalla VPC](#).

Abilitazione di account per le zone locali

I seguenti argomenti descrivono come vengono abilitati gli account per AWS le zone locali:

AWS Local Zones

Per iniziare a utilizzare le zone AWS locali, devi prima attivare una zona locale tramite la console AWS Global View o il AWS CLI. Per saperne di più, consulta [Guida introduttiva alle zone AWS locali](#). Puoi utilizzare l'operazione [DescribeAvailabilityZones](#) API per confermare l'accesso tramite ID account a un elenco di zone AWS locali.

AWS Zone locali dedicate

Per tutti i servizi nelle zone locali AWS dedicate (zone locali dedicate), incluso Amazon S3, l'amministratore deve abilitare la tua Account AWS prima di poter creare o accedere a qualsiasi risorsa nella zona locale dedicata. Puoi utilizzare l'operazione [DescribeAvailabilityZones](#) API per confermare l'accesso tramite ID account a una zona locale.

Protezione dei dati per i bucket di directory nelle zone locali

Per proteggere ulteriormente i dati in Amazon S3, per impostazione predefinita si ha accesso solo alle risorse S3 create dall'utente. I bucket nelle Zone locali hanno tutte le impostazioni di Blocco dell'accesso pubblico S3 abilitate per impostazione predefinita e S3 Object Ownership è impostato sull'applicazione del proprietario del bucket. Queste impostazioni non possono essere modificate. Opzionalmente, per limitare l'accesso solo ai gruppi di confine di rete della zona locale, è possibile

utilizzare la chiave di condizione `s3express:AllAccessRestrictedToLocalZoneGroup` nelle policy IAM. Per ulteriori informazioni, consulta [Autenticazione e autorizzazione per i bucket di directory nelle Zone locali](#).

Connettività privata dalla VPC

Per ridurre la latenza di rete, configura il tuo cloud privato virtuale (VPC) con un endpoint gateway per accedere ai bucket di directory nelle zone di disponibilità. Ciò consente di mantenere il traffico all'interno della AWS rete senza costi aggiuntivi.

Per configurare gli endpoint VPC del gateway

1. Apri la [Console VPC di Amazon](#).
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Crea un nome per l'endpoint.
5. Per Service category (Categoria servizio), scegli Servizi AWS.
6. Per Servizi, aggiungi il filtro `Type=Gateway` e poi scegli il pulsante di opzione accanto a `com.amazonaws.region.s3express`.
7. Per VPC, scegli un VPC in cui creare l'endpoint.
8. Per le tabelle di percorso, scegli la tabella di percorso nel tuo VPC da utilizzare dall'endpoint. Dopo la creazione dell'endpoint, verrà aggiunto un record di routing alla tabella di routing selezionata in questo passaggio.
9. Per Policy, scegli Accesso completo per consentire a tutti i principali di eseguire tutte le operazioni su tutte le risorse dell'endpoint VPC. Altrimenti, scegli Personalizzato per allegare una policy dell'endpoint VPC che controlla le autorizzazioni dei principali a eseguire azioni sulle risorse attraverso l'endpoint VPC.
10. Per IP address type (Tipo di indirizzo IP), seleziona una delle opzioni seguenti:
 - IPv4: assegna gli indirizzi IPv4 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e il servizio accetta richieste IPv4.
 - IPv6: assegna gli indirizzi IPv6 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6 e il servizio accetta richieste IPv6.

- **Dualstack:** assegna gli indirizzi IPv4 e IPv6 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6 e il servizio accetta sia richieste IPv4 e IPv6.
11. (Facoltativo) Per aggiungere un tag, scegli **Aggiungi nuovo tag** e immetti la chiave e il valore del tag.
 12. Seleziona **Crea endpoint**.

Per saperne di più sugli endpoint VPC gateway, consulta [Endpoint gateway](#) nella Guida a AWS PrivateLink . Per i casi d'uso relativi alla residenza dei dati, abilita l'accesso ai bucket solo dal tuo VPC utilizzando endpoint gateway VPC. Quando l'accesso è limitato a un VPC o a un endpoint VPC, puoi accedere agli oggetti tramite l'API REST e gli Console di gestione AWS SDK. AWS CLI AWS

Note

Per limitare l'accesso a un VPC o a un endpoint VPC utilizzando il Console di gestione AWS, è necessario utilizzare Private Access. Console di gestione AWS Per ulteriori informazioni, consulta [Console di gestione AWS Private Access](#) nella Guida a Console di gestione AWS .

Creazione di un bucket di directory in una zona locale

Nelle zone locali, puoi creare bucket di directory per archiviare e recuperare oggetti in un perimetro di dati specifico per soddisfare i tuoi casi d'uso relativi alla residenza dei dati. I bucket di directory S3 sono l'unico tipo di bucket supportato nelle Zone locali e contengono un tipo di posizione del bucket chiamato `LocalZone`. Il nome di un bucket di directory è composto da un nome di base fornito dall'utente e da un suffisso che contiene l'ID di zona della posizione del bucket e `--x-s3`. È possibile ottenere un elenco di ID delle zone locali utilizzando l'operazione API. [DescribeAvailabilityZones](#) Per ulteriori informazioni, consulta [Regole di denominazione dei bucket di directory](#).

Note

- Per tutti i servizi nelle zone locali AWS dedicate (zone locali dedicate), incluso S3, l'amministratore deve abilitarle Account AWS prima di poter creare o accedere a qualsiasi risorsa nella zona locale dedicata. Per ulteriori informazioni, consulta [Abilitazione di account per le zone locali](#).

- Per i requisiti di residenza dei dati, si consiglia di abilitare l'accesso ai bucket solo dagli endpoint del gateway VPC. Per ulteriori informazioni, consulta [Connettività privata dalla VPC](#).
- Per limitare l'accesso solo ai gruppi di confine di rete della zona locale, è possibile utilizzare la chiave di condizione `s3express:AllAccessRestrictedToLocalZoneGroup` nelle policy IAM. Per ulteriori informazioni, consulta [Autenticazione e autorizzazione per i bucket di directory nelle Zone locali](#).

Di seguito vengono descritti i modi per creare un bucket di directory in una singola zona locale con gli SDK Console di gestione AWS, AWS CLI, e AWS .

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione padre di una zona locale in cui desideri creare un bucket di directory.

Note

Per ulteriori informazioni sulle Regioni padre, consulta [Concetti per i bucket di directory nelle Zone locali](#).

3. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
4. Scegliere Create bucket (Crea bucket).

Viene visualizzata la pagina Create bucket (Crea bucket).

5. In Configurazione generale, visualizza la Regione AWS in cui verrà creato il bucket.
6. In Tipo di bucket, scegli Directory.

Note

- Se si è scelta una Regione che non supporta i bucket di directory, il tipo di bucket viene impostato su un bucket per uso generico. Per creare un bucket di directory, è necessario scegliere una Regione supportata. Per un elenco delle Regioni che

supportano i bucket di directory, consulta [the section called “Endpoint regionali e di zona per i bucket di directory”](#).

- Dopo aver creato il bucket, non è possibile modificare il tipo di bucket.

7. In Posizione bucket, scegli la zona locale che desideri utilizzare.

 Note

La zona locale non può essere modificata dopo la creazione del bucket.

8. In Posizione del bucket, seleziona la casella di controllo per accettare che, in caso di interruzione della zona locale, i dati potrebbero non essere disponibili o andare persi.

 Important

Sebbene i bucket di directory siano archiviati su più dispositivi all'interno di una singola zona locale, i bucket di directory non archiviano i dati in modo ridondante tra le Zone locali.

9. Per Nome bucket, immetti il nome del bucket di directory.

Per ulteriori informazioni sulle regole di denominazione dei bucket di directory, consulta [Regole di denominazione dei bucket per uso generico](#). Un suffisso viene aggiunto automaticamente al nome di base fornito quando si crea un bucket di directory tramite la console. Questo suffisso include l'ID di zona della zona locale scelta.

Una volta creato il bucket, non è possibile modificarne il nome.

 Important

Non includete informazioni sensibili, come i numeri di conto, nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

10. In Proprietà dell'oggetto, l'impostazione Proprietario del bucket è automaticamente abilitata e tutte le liste di controllo degli accessi (ACL) sono disabilitate. Per i bucket di directory, le ACL sono disabilitate e non possono essere abilitate.

Con l'impostazione Proprietario del bucket applicato attivata, il proprietario del bucket possiede automaticamente e ha il pieno controllo su ogni oggetto del bucket. Le liste di controllo degli

accessi (ACL) non influiscono più sulle autorizzazioni di accesso ai dati nel bucket S3. Il bucket utilizza esclusivamente le policy per definire il controllo degli accessi. La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

11. In Impostazioni di blocco dell'accesso pubblico per questo bucket, tutte le impostazioni di blocco dell'accesso pubblico per il bucket di directory sono automaticamente attivate. Queste impostazioni non possono essere modificate per i bucket di directory. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).
12. In Crittografia predefinita, i bucket di directory utilizzano Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) per crittografare i dati per impostazione predefinita. Hai anche la possibilità di crittografare i dati nei bucket di directory con la Server-side crittografia con chiavi (). AWS Key Management Service SSE-KMS
13. Seleziona Crea bucket.

Dopo aver creato il bucket, puoi aggiungere file e cartelle al bucket. Per ulteriori informazioni, consulta [the section called “Utilizzo di oggetti in un bucket di directory”](#).

Utilizzo di AWS CLI

Questo esempio mostra come creare un bucket di directory in una zona locale usando AWS CLI. Per utilizzare il comando, sostituisci *user input placeholders* con le informazioni appropriate.

Quando si crea un bucket di directory, è necessario fornire i dettagli di configurazione e utilizzare la seguente convenzione di denominazione: *bucket-base-name--zone-id--x-s3*.

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=LocalZone,Name=local-zone-id},Bucket={DataRedundancy=SingleLocalZone,Type=Directory}'
--region parent-region-code
```

Per ulteriori informazioni sull'ID zona locale e sul codice della Regione padre, consulta [Concetti per i bucket di directory nelle Zone locali](#). Per ulteriori informazioni sul comando AWS CLI, consulta [create-bucket](#) nella documentazione di riferimento dei comandi della AWS CLI.

Utilizzo di AWS SDK

SDK for Go

Questo esempio mostra come creare un bucket di directory in una zona locale usando AWS SDK per Go.

Example

```
var bucket = "bucket-base-name--zone-id--x-s3" // The full directory bucket name

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("local-zone-id"),
                Type: types.LocationTypeLocalZone,
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleLocalZone,
                Type:              types.BucketTypeDirectory,
            },
        },
    })
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n") // No operation performed, just printing a message
        return
    }
    if err != nil {
        log.Fatal(err)
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

Questo esempio mostra come creare un bucket di directory in una zona locale usando AWS SDK for Java 2.x.

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{local-zone-id}--x-s3
    //example: doc-example-bucket--local-zone-id--x-s3 is a valid name for a
    directory bucket created in a Local Zone.

    CreateBucketConfiguration bucketConfiguration =
    CreateBucketConfiguration.builder()
        .location(LocationInfo.builder()
            .type(LocationType.LOCAL_ZONE)
            .name("local-zone-id").build()) //this must match the Local
    Zone ID in your bucket name
        .bucket(BucketInfo.builder()
            .type(BucketType.DIRECTORY)
            .dataRedundancy(DataRedundancy.SINGLE_LOCAL_ZONE)
            .build()).build();

    try {

        CreateBucketRequest bucketRequest =
        CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfiguration)
        CreateBucketResponse response = s3Client.createBucket(bucketRequest);
        System.out.println(response);

    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

AWS SDK per JavaScript

Questo esempio mostra come creare un bucket di directory in una zona locale usando AWS SDK per JavaScript.

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
```

```
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "parent-region-code";
const zone = "local-zone-id";
const suffix = `${zone}--x-s3`;

const s3 = new S3({ region });

const bucketName = `bucket-base-name--${suffix}`; // Full directory bucket name

const createResponse = await s3.createBucket(
  { Bucket: bucketName,
    CreateBucketConfiguration: {Location: {Type: "LocalZone", Name: "local-zone-id"},
    Bucket: { Type: "Directory", DataRedundancy: "SingleLocalZone" }}
  );
```

SDK per .NET

Questo esempio mostra come creare un bucket di directory in una zona locale usando SDK per .NET.

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {

        BucketName = "bucket-base-name--local-zone-id--x-s3",
        PutBucketConfiguration = new PutBucketConfiguration
        {
            BucketInfo = new BucketInfo { DataRedundancy =
DataRedundancy.SingleLocalZone, Type = BucketType.Directory },
            Location = new LocationInfo { Name = "local-zone-id", Type =
LocationType.LocalZone }
        }
    }).ConfigureAwait(false);
}
```

SDK for PHP

Questo esempio mostra come creare un bucket di directory in una zona locale usando AWS SDK for PHP.

Example

```
require 'vendor/autoload.php';

$s3Client = new S3Client([

    'region'      => 'parent-region-code',
]);

$result = $s3Client->createBucket([
    'Bucket' => 'bucket-base-name--local-zone-id--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'local-zone-id', 'Type'=> 'LocalZone'],
        'Bucket' => ["DataRedundancy" => "SingleLocalZone" ,"Type" => "Directory"]
    ],
]);
```

SDK for Python

Questo esempio mostra come creare un bucket di directory in una zona locale usando AWS SDK per Python (Boto3).

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def create_bucket(s3_client, bucket_name, local_zone):
    """
    Create a directory bucket in a specified Local Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'bucket-base-name--local-zone-id--x-s3'
    :param local_zone: String; Local Zone ID to create the bucket in
```

```

: return: True if bucket is created, else False
'''

try:
    bucket_config = {
        'Location': {
            'Type': 'LocalZone',
            'Name': local_zone
        },
        'Bucket': {
            'Type': 'Directory',
            'DataRedundancy': 'SingleLocalZone'
        }
    }
    s3_client.create_bucket(
        Bucket = bucket_name,
        CreateBucketConfiguration = bucket_config
    )
except ClientError as e:
    logging.error(e)
    return False
return True

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'parent-region-code'
    local_zone = 'local-zone-id'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, local_zone)

```

SDK for Ruby

Questo esempio mostra come creare un bucket di directory in una zona locale usando il comando AWS SDK per Ruby.

Example

```

s3 = Aws::S3::Client.new(region:'parent-region-code')
s3.create_bucket(
  bucket: "bucket-base-name--local-zone-id--x-s3",
  create_bucket_configuration: {
    location: { name: 'local-zone-id', type: 'LocalZone' },

```

```
bucket: { data_redundancy: 'SingleLocalZone', type: 'Directory' }  
}  
)
```

Autenticazione e autorizzazione per i bucket di directory nelle Zone locali

I bucket di directory nelle zone locali supportano sia l'autorizzazione AWS Identity and Access Management (IAM) che l'autorizzazione basata sulla sessione. Per ulteriori informazioni sull'autenticazione e l'autorizzazione per i bucket di directory, consulta [Autenticazione e autorizzazione delle richieste](#).

Resources

Gli Amazon Resource Names (ARN) per i bucket di directory contengono lo spazio dei s3express nomi, la regione AWS principale, l'ID e il nome del bucket di directory che include l' Account AWS ID di zona. Per accedere ed eseguire azioni sul bucket di directory, è necessario utilizzare il seguente formato ARN:

```
arn:aws:s3express:region-code:account-id:bucket/bucket-base-name--ZoneID--x-s3
```

Per i bucket della directory in una zona locale, l'ID della zona è l'ID della zona locale. Per ulteriori informazioni sui bucket di directory in Zone locali, consulta [Concetti per i bucket di directory nelle Zone locali](#). Per maggiori informazioni sugli ARN, consulta [Nomi della risorsa Amazon \(ARN\)](#) nella Guida per l'utente di IAM. Per ulteriori informazioni sulle risorse, consulta [Elementi di policy IAM JSON: Resource](#) nella Guida all'utente IAM.

Chiavi di condizione per i bucket di directory nelle Zone locali

Nelle zone locali, è possibile utilizzare le [chiavi di condizione](#) nelle policy IAM. Inoltre, per creare un perimetro di dati intorno ai gruppi di confine di rete della zona locale, è possibile utilizzare la chiave di condizione `s3express:AllAccessRestrictedToLocalZoneGroup` per negare tutte le richieste provenienti dall'esterno dei gruppi.

La seguente chiave di condizione può essere utilizzata per affinare ulteriormente le condizioni di applicazione di un'istruzione di policy IAM. Per un elenco completo delle operazioni API, delle azioni di policy e delle chiavi di condizione supportate dai bucket di directory, consulta [Azioni di policy per i bucket di directory](#).

Note

La seguente chiave di condizione si applica solo alle Zone locali e non è supportata nelle zone di disponibilità e in Regioni AWS.

operazioni API	Azioni di policy	Description	Chiave di condizione	Description	Tipo
Operazioni API dell'endpoint di zona	s3express:CreateSession	Concede il permesso di creare un token di sessione, utilizzato per concedere l'accesso a tutte le operazioni API dell'endpoint di zona, come CreateSession, HeadBucket, CopyObject, PutObject e GetObject.	s3express:AllAccessRestrictedToLocalZoneGroup	Filtra tutti gli accessi al bucket a meno che la richiesta non provenga dai gruppi di confine della rete della zona AWS locale forniti in questa chiave di condizione. Valori: valore del gruppo di confine di rete della zona locale	String

Policy di esempio

Per limitare l'accesso agli oggetti alle richieste provenienti dall'interno di un confine di residenza dei dati definito dall'utente (in particolare, un gruppo di Zone locali che è un insieme di Zone locali associate gerarchicamente alla stessa Regione AWS), è possibile impostare una delle seguenti policy:

- La policy di controllo dei servizi (SCP). Per informazioni sulle SCP, consulta [Policy di controllo dei servizi \(SCP\)](#) nella Guida all'utente AWS Organizations.
- La policy basata sull'identità IAM per il ruolo IAM.
- La policy dell'endpoint VPC. Per ulteriori informazioni sulle policy degli endpoint VPC, consulta [Controllo dell'accesso agli endpoint VPC mediante le policy degli endpoint](#) nella Guida a AWS PrivateLink.

- La policy del bucket S3.

Note

La chiave di condizione `s3express:AllAccessRestrictedToLocalZoneGroup` non supporta l'accesso da un ambiente on-premises. Per supportare l'accesso da un ambiente on-premises, è necessario aggiungere l'IP di origine alle policy. Per ulteriori informazioni, consulta [aws: SourceIp](#) nella IAM User Guide.

Example- Policy SCP

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-LocalZones-only",
      "Effect": "Deny",
      "Action": [
        "s3express:*",
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "s3express:AllAccessRestrictedToLocalZoneGroup": [
            "local-zone-network-border-group-value"
          ]
        }
      }
    }
  ]
}
```

Example- Policy basata sull'identità IAM (collegato al ruolo IAM)

JSON


```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "s3express:CreateSession",
    "Resource": "*",
    "Condition": {
      "StringNotEqualsIfExists": {
        "s3express:AllAccessRestrictedToLocalZoneGroup": [
          "local-zone-network-border-group-value"
        ]
      }
    }
  }
}
```

Example– Policy degli endpoint VPC

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-LocalZones-only",
      "Principal": "*",
      "Action": "s3express:CreateSession",
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "s3express:AllAccessRestrictedToLocalZoneGroup": [
            "local-zone-network-border-group-value"
          ]
        }
      }
    }
  ]
}
```

Example- Policy di bucket

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-LocalZones-only",
      "Principal": "*",
      "Action": "s3express:CreateSession",
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "s3express:AllAccessRestrictedToLocalZoneGroup": [
            "local-zone-network-border-group-value"
          ]
        }
      }
    }
  ]
}
```

Differenze per i bucket di directory

Quando si utilizza Amazon S3, è possibile scegliere il tipo di bucket più adatto alle applicazioni e alle prestazioni richieste. Un bucket di directory è un tipo di bucket che viene utilizzato al meglio per casi d'uso della bassa latenza o della residenza dei dati. Per ulteriori informazioni sui bucket di directory, consulta [Operazioni con i bucket di directory](#).

Per ulteriori informazioni sulle differenze tra i bucket di directory, consulta i seguenti argomenti.

Argomenti

- [Differenze per i bucket di directory](#)

- [Operazioni API supportate per i bucket della directory](#)
- [Funzioni di Amazon S3 non supportate dai bucket della directory](#)

Differenze per i bucket di directory

- Nomi dei bucket di directory
 - Il nome di un bucket di directory è composto da un nome di base fornito e da un suffisso che contiene l'ID della AWS zona (una zona di disponibilità o una zona locale) in cui si trova il bucket, seguito da. --x-s Per un elenco di regole ed esempi di nomi di bucket di directory, consulta [Regole di denominazione dei bucket di directory](#).
- Comportamento di **ListObjectsV2**
 - Per i bucket di directory, ListObjectsV2 non restituisce gli oggetti in ordine lessicografico (alfabetico). Inoltre, i prefissi devono terminare con un delimitatore che può corrispondere solo a "/".
 - Per i bucket di directory, la risposta di ListObjectsV2 include i prefissi relativi solo ai caricamenti multipart in corso.
- Comportamento di eliminazione: quando si elimina un oggetto in un bucket di directory, Amazon S3 elimina in modo ricorsivo tutte le directory vuote nel percorso dell'oggetto. Ad esempio, se si elimina la chiave dell'oggetto dir1/dir2/file1.txt, Amazon S3 elimina file1.txt. Se le directory dir1/ e dir2/ sono vuote e non contengono altri oggetti, Amazon S3 elimina anche tali directory.
- ETag e checksum: i tag entità (ETag) per i bucket di directory sono stringhe alfanumeriche casuali univoche per l'oggetto e checksum non MD5. Per ulteriori informazioni sull'utilizzo di checksum aggiuntivi con i bucket di directory, consulta [Best practice per il checksum S3 aggiuntivo](#).
- Chiavi degli oggetti nelle richieste **DeleteObjects**
 - Le chiavi degli oggetti nelle richieste DeleteObjects devono contenere almeno un carattere diverso dallo spazio. Le stringhe con tutti caratteri spaziatura non sono supportate nelle richieste DeleteObjects.
 - Le chiavi degli oggetti nelle richieste DeleteObjects non possono contenere caratteri di controllo Unicode, fatta eccezione per newline (\n) tab (\t) e carriage feed (\r).
- Endpoint regionali e zonali: le operazioni Bucket-management API per i bucket di directory sono disponibili tramite un endpoint regionale e sono denominate operazioni API per endpoint regionali. Esempi di operazioni API per endpoint regionali sono e. CreateBucket DeleteBucket Dopo aver creato un bucket di directory, puoi utilizzare le operazioni API degli endpoint zonali per caricare e

gestire gli oggetti nel bucket di directory. Le operazioni API degli endpoint zionali sono disponibili tramite un endpoint zonale. Esempi di operazioni API degli endpoint zionali sono `PutObject` e `CopyObject`. Quando si utilizzano i bucket di directory, è necessario specificare la Regione in tutte le richieste. Per gli endpoint regionali, si specifica la regione, ad esempio `s3express-control.us-west-2.amazonaws.com`. Per gli endpoint zionali, si specificano la regione e la zona di disponibilità, ad esempio `s3express-usw2-az1.us-west-2.amazonaws.com`. Per ulteriori informazioni, consulta [Endpoint regionali e di zona per i bucket di directory](#).

- Caricamenti multiparte - È possibile caricare e copiare oggetti di grandi dimensioni memorizzati nei bucket della directory utilizzando il processo di caricamento multiparte. Tuttavia, di seguito sono riportate alcune differenze quando si utilizza il processo di caricamento multiparte con oggetti memorizzati nei bucket della directory. Per ulteriori informazioni, consulta [the section called "Utilizzo dei caricamenti multiparte con i bucket di directory"](#).
 - L'ora di creazione dell'oggetto è la data di completamento del caricamento in più parti.
 - I numeri parte in più parti devono utilizzare numeri parte consecutivi. Se si tenta di completare una richiesta caricamento in più parti con numeri parte non consecutivi, Amazon S3 genera un errore 400 (Bad Request) HTTP.
 - L'iniziatore di un caricamento in più parti può interrompere la richiesta di caricamento in più parti solo se è stata concesso esplicitamente l'accesso a `AbortMultipartUpload` tramite l'autorizzazione `s3express:CreateSession`. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).
- Svuotamento di un bucket di directory: il `s3 rm` comando tramite AWS Command Line Interface (CLI), l'`delete` operazione tramite Mountpoint e il pulsante di opzione Empty bucket tramite il pulsante di opzione Empty bucket tramite il non Console di gestione AWS sono in grado di eliminare i caricamenti multiparte in corso in un bucket di directory. Per eliminare i caricamenti multiparte in corso, usare l'operazione `ListMultipartUploads` per elencare i caricamenti multiparte in corso nel bucket e usare l'operazione `AbortMultipartUpload` per interrompere tutti i caricamenti multiparte in corso.
- AWS Command Line Interface Comando (CLI): il **`s3 sync`** comando non è supportato con i bucket di directory. Usalo `s3 cp --recursive` come alternativa per trasferire file da o verso bucket di directory.
- AWS Zone locali: le zone locali sono supportate solo per i bucket di directory e non per i bucket generici.
 - L'aggiunta di dati a oggetti esistenti non è supportata per i bucket di directory che risiedono nelle zone locali. È possibile aggiungere dati agli oggetti esistenti solo nei bucket di directory che risiedono nelle zone di disponibilità.

Operazioni API supportate per i bucket della directory

I bucket di directory supportano operazioni API degli endpoint regionali a livello di bucket o piano di controllo (control-plane) e zonali a livello di oggetto o piano dati. Per ulteriori informazioni, consulta [Collegamento in rete per i bucket di directory](#) e [Endpoint ed endpoint VPC del gateway](#). Per l'elenco delle operazioni API supportate, consulta [Operazioni API del bucket della directory](#).

Funzioni di Amazon S3 non supportate dai bucket della directory

Le seguenti funzionalità di Amazon S3 non sono supportate dai bucket di directory:

- AWS politiche gestite
- AWS PrivateLink per S3
- Checksum MD5
- Multi-factor eliminazione dell'autenticazione (MFA)
- Blocco di oggetti in S3
- pagamento a carico del richiedente
- Contributi di accesso S3
- Notifiche di eventi di Amazon S3
- Azioni di transizione del ciclo di vita S3
- Punti di accesso S3 Multi-Region
- Punti di accesso Lambda per oggetti S3
- Funzione Controllo delle versioni S3
- Replica di Amazon S3
- Tag dell'oggetto
- S3 Select
- Log di accesso al server
- Hosting di siti Web statici
- S3 Storage Lens
- Gruppi Storage Lens S3
- Transfer Acceleration S3

- Dual-layer crittografia lato server con chiavi AWS Key Management Service (AWS KMS) () DSSE-KMS
- Server-side crittografia con chiavi fornite dal cliente () SSE-C
- L'opzione per copiare le impostazioni di un bucket esistente quando si crea un nuovo bucket nella console di Amazon S3
- Messaggi di errore di accesso negato migliorato (HTTP 403 Forbidden)

Collegamento in rete per i bucket di directory

Per accedere ai bucket della directory e agli oggetti al suo interno, si utilizzano endpoint API regionali e di zona, diversi da quelli standard di Amazon S3. A seconda dell'operazione API S3 utilizzata, è richiesto un endpoint regionale o zonale. Per un elenco completo di operazioni API per tipo di endpoint, consulta [Differenze per i bucket di directory](#).

Puoi accedere alle operazioni API regionali e zonali tramite gli endpoint del cloud privato virtuale (VPC) del gateway.

Nei seguenti argomenti vengono descritti i requisiti di rete per accedere a S3 Express One Zone mediante un endpoint VPC del gateway.

Argomenti

- [Endpoints](#)
- [Configurazione degli endpoint VPC del gateway](#)

Endpoints

È possibile accedere ai bucket della directory e agli oggetti al suo interno dalla VPC utilizzando gli endpoint del gateway VPC. I bucket della directory utilizzano gli endpoint API regionali e di zona. A seconda dell'operazione API Amazon S3 utilizzata, è necessario un endpoint regionale o zonale. L'utilizzo di endpoint gateway non comporta costi supplementari.

Bucket-level (o piano di controllo) le operazioni API sono disponibili tramite endpoint regionali e sono denominate operazioni API per endpoint regionali. Esempi di operazioni API degli endpoint regionali sono `CreateBucket` e `DeleteBucket`. Quando si crea un bucket di directory, si sceglie una singola zona (di disponibilità o locale) in cui verrà creato il bucket di directory. Dopo aver creato un bucket di directory, puoi utilizzare le operazioni API degli endpoint zonali per caricare e gestire gli oggetti nel bucket di directory.

Object-level Le operazioni API (o piano dati) sono disponibili tramite gli endpoint zionali e sono denominate operazioni API degli endpoint zionali. Esempi di operazioni API degli endpoint zionali sono `CreateSession` e `PutObject`.

Per ulteriori informazioni sugli endpoint e sulle posizioni che supportano i bucket di directory nelle zone di disponibilità, consulta [Endpoint per i bucket di directory nelle zone di disponibilità](#).

Per ulteriori informazioni sugli endpoint e le posizioni che supportano i bucket di directory nelle Zone locali, consulta [Abilitazione di account per le zone locali](#).

Configurazione degli endpoint VPC del gateway

Per configurare gli endpoint dei gateway VPC per i bucket di directory di accesso nelle zone di disponibilità, consulta [the section called “Configurazione degli endpoint VPC del gateway”](#).

Per configurare gli endpoint del gateway VPC per i bucket di directory di accesso nelle Zone locali, consulta [Connettività privata dalla VPC](#).

Regole di denominazione dei bucket di directory

Quando si crea un bucket di directory in Amazon S3, si applicano le seguenti regole di denominazione dei bucket. Per le regole di denominazione dei bucket per uso generico, consulta [Regole di denominazione dei bucket per uso generico](#).

Il nome di un bucket di directory è costituito da un nome di base fornito dall'utente e da un suffisso che contiene l'ID della AWS zona (una zona di disponibilità o una zona locale) in cui si trova il bucket e. --x-s3 *zone-id* Può essere l'ID di una zona di disponibilità o di una zona locale.

```
base-name--zoneid--x-s3
```

Ad esempio, il seguente nome del bucket di directory contiene l'ID zona di disponibilità `usw2-az1`:

```
bucket-base-name--usw2-az1--x-s3
```

Note

Quando si crea un bucket di directory tramite la console, viene aggiunto automaticamente un suffisso al nome di base fornito. Questo suffisso include l'ID della zona (zona di disponibilità o zona locale) scelta.

Quando si crea un bucket di directory utilizzando un'API, è necessario fornire il suffisso completo, compreso l'ID di zona, nella richiesta. Per un elenco di ID zona, consulta [Endpoints](#).

Le seguenti regole di denominazione si applicano ai bucket della directory.

- Sii univoco all'interno della zona scelta (zona di AWS disponibilità o zona AWS locale).
- Il nome deve avere una lunghezza compresa tra 3 (min) e 63 (max) caratteri, incluso il suffisso.
- Essere costituiti solo da lettere minuscole, numeri e trattini (-).
- Iniziare e finire con una lettera o un numero.
- Deve includere il seguente suffisso: `--zone-id--x-s3`.
- I nomi dei bucket non devono iniziare con il prefisso `xn--`.
- I nomi dei bucket non devono iniziare con il prefisso `sthree-`.
- I nomi dei bucket non devono iniziare con il prefisso `sthree-configurator`.
- I nomi dei bucket non devono iniziare con il prefisso `amzn-s3-demo-`.
- I nomi dei bucket non devono terminare con il suffisso `-s3alias`. Questo suffisso è riservato ai nomi alias dei punti di accesso. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).
- I nomi dei bucket non devono terminare con il suffisso `-o1-s3`. Questo suffisso è riservato ai nomi alias dei punti di accesso Lambda per oggetti. Per ulteriori informazioni, consulta [Come utilizzare un alias in stile bucket per il punto di accesso Lambda per oggetti del bucket S3](#).
- I nomi dei bucket non devono terminare con il suffisso `.mr.ap`. Questo suffisso è riservato ai nomi dei punti di Multi-Region accesso. Per ulteriori informazioni, consulta [Regole per la denominazione degli Access Point di Amazon S3 Multi-Region](#).

Visualizzazione delle proprietà dei bucket di directory

È possibile visualizzare e configurare le proprietà di un bucket di directory Amazon S3 utilizzando la console Amazon S3. Per ulteriori informazioni, consulta [Operazioni con i bucket di directory](#).

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Nell'elenco Bucket di directory, scegli il nome del bucket per il quale desideri visualizzare le proprietà.
4. Scegliere la scheda Properties (Proprietà).
5. Nella scheda Proprietà è possibile visualizzare le seguenti proprietà del bucket:
 - Panoramica del bucket della directory - È possibile visualizzare la Regione AWS, la zona (zona di disponibilità o zona locale), il nome della risorsa Amazon (ARN) e la data di creazione del bucket.
 - Server-side impostazioni di crittografia: Amazon S3 applica la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) come livello base di crittografia per tutti i bucket S3. Amazon S3 crittografa di un oggetto prima di salvarlo su disco e lo decrittografa quando lo scarichi. Per ulteriori informazioni, consulta [Impostazione e monitoraggio della crittografia predefinita per i bucket di directory](#).

Per ulteriori informazioni sulle funzionalità supportate per i bucket di directory, consulta [Creazione e utilizzo di bucket di directory](#).

Gestione delle policy dei bucket di directory

Puoi aggiungere, eliminare, aggiornare e visualizzare le policy dei bucket per i bucket di directory Amazon S3 utilizzando la console Amazon S3, gli SDK e l'interfaccia a riga di comando. AWS AWS Per ulteriori informazioni, consulta i seguenti argomenti. Per ulteriori informazioni sulle azioni supportate AWS Identity and Access Management (IAM), consulta. [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#) Per policy dei bucket di esempio per bucket di directory, consulta [Esempi di policy di bucket per i bucket di directory](#).

Argomenti

- [Aggiunta di una policy di bucket](#)
- [Visualizzazione di una policy del bucket](#)
- [Eliminazione di una policy del bucket](#)

Aggiunta di una policy di bucket

Per aggiungere una policy di bucket a un bucket di directory, è possibile utilizzare la console Amazon S3, gli SDK AWS o AWS CLI.

Utilizzo della console S3

Per creare o modificare una policy del bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Nell'elenco Bucket di directory scegli il nome del bucket al quale desideri aggiungere una policy.
4. Scegli la scheda Autorizzazioni.
5. In Policy del bucket, scegli Modifica. Viene visualizzata la pagina Modifica la policy del bucket.
6. Per generare automaticamente una policy, scegli Generatore di policy.

Se scegli Policy Generator, il AWS Policy Generator si apre in una nuova finestra.

Se non desideri utilizzare il AWS Policy Generator, puoi aggiungere o modificare le dichiarazioni JSON nella sezione Policy.

- a. Nella pagina del Generatore di policy AWS , per Seleziona il tipo di policy, scegli Policy del bucket S3.
- b. Aggiungi un'istruzione inserendo le informazioni nei campi previsti, quindi scegli Aggiungi istruzione. Ripeti questo passaggio per il numero di istruzioni che desideri aggiungere. Per ulteriori informazioni su questi campi, consulta [Riferimento agli elementi delle policy IAM JSON](#) nella Guida per l'utente IAM.

Note

Per comodità, la pagina Modifica la policy bucket visualizza un ARN (nome della risorsa Amazon) del bucket corrente sopra il campo di testo Policy. È possibile copiare questo ARN per utilizzarlo nelle istruzioni della pagina del Generatore di policy AWS .

- c. Dopo aver aggiunto le istruzioni, scegli Genera policy.
 - d. Copia il testo della policy generata, scegli Chiudi e torna alla pagina Modifica policy del bucket nella console di Amazon S3.
7. Nella casella Policy, modifica la policy esistente o incolla la policy bucket dal Policy Generator AWS . Assicurati di risolvere gli avvisi di sicurezza, gli errori, gli avvisi generali e i suggerimenti prima di salvare la policy.

Note

Le policy di bucket sono limitate a dimensioni di 20 KB.

8. Scegli **Save changes** (Salva modifiche), che ti riporterà alla pagina **Permissions** (Autorizzazioni).

Utilizzo di AWS SDK

SDK for Java 2.x

Example

PutBucketPolicy AWS SDK for Java 2.x

```
public static void setBucketPolicy(S3Client s3Client, String bucketName, String
policyText) {

    //sample policy text
    /**
     * policy_statement = {
     *     'Version': '2012-10-17',
     *     'Statement': [
     *         {
     *             'Sid': 'AdminPolicy',
     *             'Effect': 'Allow',
     *             'Principal': {
     *                 "AWS": "111122223333"
     *             },
     *             'Action': 's3express:*',
     *             'Resource':
'arn:aws:s3express:region:111122223333:bucket/bucket-base-name--zone-id--x-s3'
     *         }
     *     ]
     * }
    */
    System.out.println("Setting policy:");
    System.out.println("----");
    System.out.println(policyText);
    System.out.println("----");
    System.out.format("On Amazon S3 bucket: \"%s\"\n", bucketName);

    try {
```

```
        PutBucketPolicyRequest policyReq = PutBucketPolicyRequest.builder()
            .bucket(bucketName)
            .policy(policyText)
            .build();
        s3Client.putBucketPolicy(policyReq);
        System.out.println("Done!");
    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

Utilizzo di AWS CLI

Questo esempio mostra come aggiungere una policy di bucket a un bucket di directory utilizzando il comando AWS CLI. Per utilizzare il comando, sostituiscili *user input placeholders* con le tue informazioni.

```
aws s3api put-bucket-policy --bucket bucket-base-name--zone-id--x-s3 --policy file://
bucket_policy.json
```

bucket_policy.json:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AdminPolicy",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3express*",
      "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-
demo-bucket--usw2-az1--x-s3"
    }
  ]
}
```

```
]
}
```

Per ulteriori informazioni, consulta [put-bucket-policy](#) in AWS Command Line Interface.

Visualizzazione di una policy del bucket

Per visualizzare una policy di bucket per un bucket di directory, utilizza gli esempi seguenti.

Utilizzo di AWS CLI

Questo esempio mostra come visualizzare la policy di bucket collegata a un bucket di directory usando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3api get-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

Per ulteriori informazioni, consulta [get-bucket-policy](#) in AWS Command Line Interface.

Eliminazione di una policy del bucket

Per eliminare una policy di bucket per un bucket di directory, utilizza gli esempi seguenti.

Utilizzo di AWS SDK

SDK for Java 2.x

Example

DeleteBucketPolicy AWS SDK for Java 2.x

```
public static void deleteBucketPolicy(S3Client s3Client, String bucketName) {
    try {
        DeleteBucketPolicyRequest deleteBucketPolicyRequest =
            DeleteBucketPolicyRequest
                .builder()
                .bucket(bucketName)
                .build()
        s3Client.deleteBucketPolicy(deleteBucketPolicyRequest);
    }
}
```

```
        System.out.println("Successfully deleted bucket policy");
    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

Utilizzo di AWS CLI

Questo esempio mostra come eliminare una policy di bucket per un bucket di directory utilizzando il comando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3api delete-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

Per ulteriori informazioni, consulta [delete-bucket-policy](#) in AWS Command Line Interface.

Svuotamento di un bucket di directory

È possibile svuotare un bucket di directory Amazon S3 utilizzando la console Amazon S3. Per ulteriori informazioni sui bucket di directory, consulta [Operazioni con i bucket di directory](#).

Prima di svuotare un bucket di directory, tieni presente quanto segue:

- Quando si svuota un bucket di directory, si eliminano tutti gli oggetti ma si mantiene il bucket di directory.
- Dopo aver svuotato un bucket di directory, l'azione di svuotamento non può essere annullata.
- Gli oggetti aggiunti al bucket della directory mentre è in corso l'azione di svuotamento del bucket potrebbero essere eliminati.

Se desideri eliminare anche il bucket, osserva quanto segue:

- Tutti gli oggetti nel bucket di directory devono essere eliminati prima di poter eliminare il bucket stesso.
- In-progress i caricamenti in più parti nel bucket di directory devono essere interrotti prima che il bucket stesso possa essere eliminato.

 Note

Il `s3 rm` comando tramite AWS Command Line Interface (CLI), l'operazione `delete` tramite Mountpoint e il pulsante di opzione `Empty bucket` tramite il pulsante di opzione `Empty bucket` non Console di gestione AWS sono in grado di eliminare i caricamenti multiparte in corso in un bucket di directory. Per eliminare i caricamenti multiparte in corso, usare l'operazione `ListMultipartUploads` per elencare i caricamenti multiparte in corso nel bucket e usare l'operazione `AbortMultipartUpload` per interrompere tutti i caricamenti multiparte in corso.

Per eliminare un bucket di directory, consulta [Eliminazione di un bucket di directory](#). Per interrompere un caricamento multiparte in corso, consulta [the section called “Interruzione di un caricamento in più parti”](#).

Per svuotare un bucket per uso generico, consulta [Eliminazione del contenuto di un bucket per uso generico](#).

Utilizzo della console S3

Per svuotare un bucket di directory

1. Accedi e apri la console Amazon S3 all' Console di gestione AWS indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli `Bucket di directory`.
3. Scegli il pulsante di opzione accanto al nome del bucket che si desidera svuotare, quindi scegli `Svuota`.
4. Nella pagina `Svuota bucket` conferma che desideri svuotare il bucket inserendo **permanently delete** nel campo di testo e quindi scegli `Svuota`.
5. Monitora l'avanzamento del processo di svuotamento del bucket nella pagina `Svuota bucket`: stato.

Eliminazione di un bucket di directory

È possibile eliminare solo i bucket di directory Amazon S3 vuoti. Prima di eliminare il bucket della directory, è necessario eliminare tutti gli oggetti nel bucket e interrompere tutti i caricamenti multiparte in corso.

Se il bucket di directory è collegato a un punto di accesso, è necessario prima eliminare il punto di accesso. Per ulteriori informazioni, consulta [Eliminazione del punto di accesso per bucket di directory](#).

Per svuotare un bucket di directory, consulta [Svuotamento di un bucket di directory](#). Per interrompere un caricamento multiparte in corso, consulta [the section called “Interruzione di un caricamento in più parti”](#).

Per eliminare un bucket per uso generico, consulta [Eliminazione di un bucket per uso generico](#).

Utilizzo della console S3

Dopo aver svuotato il bucket della directory e aver interrotto tutti i caricamenti multiparte in corso, è possibile eliminare il bucket.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Nell'elenco dei Bucket di directory, scegli il pulsante di opzione accanto al bucket che si desidera eliminare.
4. Scegliere Elimina.
5. Nella pagina Elimina bucket inserisci il nome del bucket nel campo di testo per confermare l'eliminazione del bucket.

Important

L'eliminazione di un bucket di directory non può essere annullata.

6. Per eliminare il bucket di directory, scegli Elimina bucket.

Utilizzo di AWS SDK

Gli esempi seguenti eliminano un bucket di directory utilizzando il AWS SDK for Java 2.x comando and. AWS SDK per Python (Boto3)

SDK for Java 2.x

Example

```
public static void deleteBucket(S3Client s3Client, String bucketName) {  
  
    try {  
        DeleteBucketRequest del = DeleteBucketRequest.builder()  
            .bucket(bucketName)  
            .build();  
        s3Client.deleteBucket(del);  
        System.out.println("Bucket " + bucketName + " has been deleted");  
    }  
    catch (S3Exception e) {  
        System.err.println(e.awsErrorDetails().errorMessage());  
        System.exit(1);  
    }  
}
```

SDK for Python

Example

```
import logging  
import boto3  
from botocore.exceptions import ClientError  
  
def delete_bucket(s3_client, bucket_name):  
    '''  
    Delete a directory bucket in a specified Region  
  
    :param s3_client: boto3 S3 client  
    :param bucket_name: Bucket to delete; for example, 'doc-example-bucket--usw2-az1--x-s3'  
    :return: True if bucket is deleted, else False  
    '''
```

```
try:
    s3_client.delete_bucket(Bucket = bucket_name)
except ClientError as e:
    logging.error(e)
    return False
return True

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
```

Utilizzo di AWS CLI

Questo esempio mostra come eliminare un bucket di directory utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3api delete-bucket --bucket bucket-base-name--zone-id--x-s3 --region us-west-2
```

Per ulteriori informazioni, consulta [delete-bucket](#) in AWS Command Line Interface.

Elencare i bucket di directory

Gli esempi seguenti mostrano come elencare i bucket di directory utilizzando Console di gestione AWS, AWS SDK e CLI. AWS

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui visualizzare l'elenco dei bucket di directory.
3. Nel riquadro di navigazione a sinistra, scegli Bucket di directory. Viene visualizzato un elenco di bucket di directory. Scegli il nome di un bucket per visualizzare gli oggetti presenti nel bucket, le proprietà del bucket, le autorizzazioni del bucket, le metriche, i punti di accesso associati al bucket o per gestire il bucket.

Utilizzo di AWS SDK

SDK for Java 2.x

Example

L'esempio seguente elenca i bucket di directory utilizzando il comando AWS SDK for Java 2.x.

```
public static void listBuckets(S3Client s3Client) {
    try {
        ListDirectoryBucketsRequest listDirectoryBucketsRequest =
            ListDirectoryBucketsRequest.builder().build();
        ListDirectoryBucketsResponse response =
            s3Client.listDirectoryBuckets(listDirectoryBucketsRequest);
        if (response.hasBuckets()) {
            for (Bucket bucket: response.buckets()) {
                System.out.println(bucket.name());
                System.out.println(bucket.creationDate());
            }
        }
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

L'esempio seguente elenca i bucket di directory utilizzando il comando AWS SDK per Python (Boto3).

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_directory_buckets(s3_client):
    '''
    Prints a list of all directory buckets in a Region
```

```
:param s3_client: boto3 S3 client
:return: True if there are buckets in the Region, else False
'''
try:
    response = s3_client.list_directory_buckets()
    for bucket in response['Buckets']:
        print (bucket['Name'])
except ClientError as e:
    logging.error(e)
    return False
return True

if __name__ == '__main__':
    region = 'us-east-1'
    s3_client = boto3.client('s3', region_name = region)
    list_directory_buckets(s3_client)
```

SDK per .NET

Example

L'esempio seguente elenca i bucket di directory utilizzando il comando AWS SDK per .NET.

```
var listDirectoryBuckets = await amazonS3Client.ListDirectoryBucketsAsync(new
    ListDirectoryBucketsRequest
{
    MaxDirectoryBuckets = 10
}).ConfigureAwait(false);
```

SDK for PHP

Example

L'esempio seguente elenca i bucket di directory utilizzando il comando AWS SDK per PHP.

```
require 'vendor/autoload.php';

$s3Client = new S3Client([
    'region'      => 'us-east-1',
]);
```

```
$result = $s3Client->listDirectoryBuckets();
```

SDK for Ruby

Example

L'esempio seguente elenca i bucket di directory utilizzando il comando AWS SDK per Ruby.

```
s3 = Aws::S3::Client.new(region:'us-west-1')  
s3.list_directory_buckets
```

Utilizzo di AWS CLI

Il seguente comando di `list-directory-buckets` esempio mostra come è possibile utilizzare il AWS CLI per elencare i bucket di directory nella *us-east-1* regione. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api list-directory-buckets --region us-east-1
```

Per ulteriori informazioni, consulta [list-directory-buckets](#) nella documentazione di riferimento dei comandi della AWS CLI .

Determinazione del fatto che sia possibile accedere a un bucket di directory

I seguenti esempi di AWS SDK mostrano come utilizzare l'operazione HeadBucket API per determinare se esiste un bucket di directory Amazon S3 e se si dispone dell'autorizzazione per accedervi.

Utilizzo di AWS SDK

L' AWS SDK for Java 2.x esempio seguente mostra come determinare se esiste un bucket e se si dispone dell'autorizzazione per accedervi.

SDK for Java 2.x

Example

AWS SDK for Java 2.x

```
public static void headBucket(S3Client s3Client, String bucketName) {
    try {
        HeadBucketRequest headBucketRequest = HeadBucketRequest
            .builder()
            .bucket(bucketName)
            .build();
        s3Client.headBucket(headBucketRequest);
        System.out.format("Amazon S3 bucket: \"%s\" found.", bucketName);
    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

Utilizzo di AWS CLI

Il seguente comando di esempio `head-bucket` mostra come si può usare AWS CLI per determinare se un bucket di directory esiste e se si ha il permesso di accedervi. Per eseguire questo comando, sostituisci i segnaposto inseriti dall'utente con le tue informazioni.

```
aws s3api head-bucket --bucket bucket-base-name--zone-id--x-s3
```

Per ulteriori informazioni, consulta [head-bucket](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo di oggetti in un bucket di directory

Dopo aver creato un bucket di directory Amazon S3, puoi lavorare con gli oggetti utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e gli SDK. AWS

Per ulteriori informazioni sull'esecuzione di operazioni in blocco, sull'importazione, sul caricamento, sulla copia, sull'eliminazione e sul download di oggetti nei bucket della directory, consulta i seguenti argomenti.

Argomenti

- [Importazione di oggetti in un bucket di directory](#)
- [Operazioni con S3 Lifecycle per i bucket di directory](#)
- [Utilizzo di Operazioni in batch con i bucket di directory](#)
- [Aggiunta di dati agli oggetti nei bucket della directory](#)
- [Ridenominazione degli oggetti nei bucket di directory](#)
- [Caricamento di oggetti in un bucket di directory](#)
- [Copia di oggetti da o verso un bucket di directory](#)
- [Eliminazione di oggetti da un bucket di directory](#)
- [Download di un oggetto da un bucket di directory](#)
- [Generazione di URL prefirmati per condividere oggetti da bucket di directory](#)
- [Recupero dei metadati degli oggetti dai bucket della directory](#)
- [Elenco degli oggetti di un bucket di directory](#)

Importazione di oggetti in un bucket di directory

Dopo aver creato un bucket di directory in Amazon S3, puoi popolare il nuovo bucket con i dati utilizzando l'azione di importazione. L'importazione è un metodo ottimizzato di creazione di processi Operazioni in batch S3 per copiare oggetti da bucket per uso generico in bucket di directory.

Note

Le seguenti limitazioni si applicano ai processi di importazione:

- Il bucket di origine e il bucket di destinazione devono essere nello stesso account. Regione AWS
- Il bucket di origine non può essere un bucket di directory.
- Gli oggetti di dimensioni superiori a 5 GB non sono supportati e verranno omessi dall'operazione di copia.
- Gli oggetti nelle classi di storage Glacier Flexible Retrieval, Glacier Deep Archive, Intelligent-Tiering Archive Access tier e Intelligent-Tiering Deep Archive tier devono essere ripristinati prima di poter essere importati.
- Gli oggetti importati con algoritmi di checksum MD5 vengono convertiti per utilizzare i checksum CRC32.

- Gli oggetti importati utilizzano la classe di storage Express One Zone, che ha una struttura di prezzi diversa dalle classi di storage utilizzate dai bucket per uso generico. Considera questa differenza di costo durante l'importazione di un gran numero di oggetti.
- Gli oggetti con annotazioni non sono supportati.

Durante la configurazione di un processo di importazione, specifica il bucket o il prefisso di origine da cui verranno copiati gli oggetti esistenti. Fornisci anche un ruolo AWS Identity and Access Management (IAM) che dispone delle autorizzazioni per accedere agli oggetti di origine. Amazon S3 avvia quindi un processo Operazioni in batch che copia gli oggetti e applica automaticamente le impostazioni della classe di archiviazione e del checksum appropriate.

Per configurare i processi di importazione, utilizza la console Amazon S3.

Utilizzo della console Amazon S3

Per importare oggetti in un bucket di directory

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket, quindi seleziona la scheda Bucket di directory. Seleziona il pulsante di opzione accanto al bucket di directory in cui desideri importare gli oggetti.
3. Scegli Importa.
4. Per Origine, inserisci il bucket per uso generico (o il percorso del bucket incluso il prefisso) contenente gli oggetti che desideri importare. Per scegliere un bucket per uso generico esistente da un elenco, scegli S3 Browse.
5. Per Autorizzazione ad accedere e copiare gli oggetti di origine, esegui una delle seguenti operazioni per specificare un ruolo IAM con le autorizzazioni necessarie per importare gli oggetti di origine:
 - Per consentire ad Amazon S3 di creare automaticamente un nuovo ruolo IAM, scegli Crea un nuovo ruolo IAM.
 - Per scegliere un ruolo IAM esistente da un elenco, seleziona Scegli tra ruoli IAM esistenti.
 - Per specificare un ruolo IAM esistente inserendo il relativo nome della risorsa Amazon (ARN), seleziona Inserisci ARN ruolo IAM, quindi inserisci l'ARN nel campo corrispondente.

6. Rivedi le informazioni visualizzate nelle sezioni Destinazione e Impostazioni degli oggetti copiati. Se le informazioni nella sezione Destinazione sono corrette, scegli Importa per avviare il processo di copia.

La console Amazon S3 visualizza lo stato del nuovo processo nella pagina Operazioni in batch. Per ulteriori informazioni sul processo, scegli il pulsante di opzione accanto al nome del processo, quindi nel menu Azioni, scegli Visualizza dettagli. Per aprire il bucket di directory in cui verranno importati gli oggetti, scegli Visualizza la destinazione di importazione.

Operazioni con S3 Lifecycle per i bucket di directory

S3 Lifecycle aiuta a memorizzare gli oggetti in S3 Express One Zone nei bucket della directory in modo conveniente, eliminando gli oggetti scaduti per conto dell'utente. Per gestire il ciclo di vita degli oggetti, creare una configurazione S3 Lifecycle per il bucket della directory. Una configurazione del ciclo di vita di S3 è un insieme di regole che definisce le operazioni che Amazon S3 deve applicare a un gruppo di oggetti. Puoi impostare una configurazione del ciclo di vita di Amazon S3 su un bucket di directory utilizzando l'interfaccia a riga di AWS comando (AWS CLI), gli AWS SDK, l'API REST di Amazon S3 e. AWS CloudFormation

Nella configurazione del ciclo di vita, si utilizzano le regole per definire le azioni che Amazon S3 deve eseguire sugli oggetti. Per gli oggetti memorizzati nei bucket della directory, è possibile creare regole del ciclo di vita per far scadere gli oggetti man mano che diventano obsoleti. È inoltre possibile creare regole del ciclo di vita per eliminare i caricamenti multiparte incompleti nei bucket della directory con una frequenza giornaliera.

Quando si aggiunge una configurazione del ciclo di vita a un bucket, le regole di configurazione si applicano sia agli oggetti esistenti sia a quelli che vengono aggiunti in un secondo momento. Ad esempio, se oggi si aggiunge una regola di configurazione del ciclo di vita con un'azione di scadenza che fa scadere gli oggetti con un prefisso specifico 30 giorni dopo la creazione, S3 metterà in coda per la rimozione tutti gli oggetti esistenti che hanno più di 30 giorni e che hanno il prefisso specificato.

Perché S3 Lifecycle è diverso per i bucket di directory

Per gli oggetti nei bucket della directory, è possibile creare regole del ciclo di vita per far scadere gli oggetti ed eliminare i caricamenti multiparte incompleti. Tuttavia, S3 Lifecycle per i bucket di directory non supporta le azioni di transizione tra le classi di storage. S3 Lifecycle for directory buckets richiede la concessione di autorizzazioni esplicite al principale del servizio S3 Lifecycle.

Autorizzazioni per il ciclo di vita di S3

S3 Lifecycle utilizza le operazioni `DeleteObject`, e `AbortMultipartUpload` API per far scadere gli `DeleteObjects` oggetti nei bucket di directory. Per chiamare queste operazioni, S3 Lifecycle utilizza l'API per ottenere credenziali di sicurezza temporanee. `CreateSession` È necessario concedere l'`s3express:CreateSession` autorizzazione in modalità `ReadWrite` sessione al responsabile del servizio S3 Lifecycle (`lifecycle.s3.amazonaws.com`). Se non concedi questa autorizzazione o se una policy attiva nega esplicitamente le autorizzazioni di eliminazione all'entità del servizio S3 Lifecycle, S3 Lifecycle non può far scadere gli oggetti nel bucket di directory. Per ulteriori informazioni, consulta Amazon S3 API Reference. `CreateSession` [CreateSession](#)

Utilizzo di una bucket policy per concedere le autorizzazioni al principale del servizio S3 Lifecycle

La seguente policy bucket concede al principale del servizio S3 Lifecycle l'autorizzazione a creare sessioni per eseguire operazioni come `DeleteObject` `DeleteObjects`. Quando in una `CreateSession` richiesta non è specificata alcuna modalità di sessione, la sessione viene creata con il privilegio massimo consentito dalle autorizzazioni in (prima si tenta `ReadWrite`, poi se non è consentito). `ReadOnly` `ReadWrite`. Tuttavia, `ReadOnly` le sessioni non sono sufficienti per le operazioni del ciclo di vita che modificano o eliminano oggetti. Pertanto, questo esempio richiede esplicitamente una modalità `ReadWrite` sessione utilizzando la `s3express:SessionMode` chiave di condizione.

Example Politica bucket da consentire **CreateSession** con una modalità di **ReadWrite** sessione esplicita per le operazioni del ciclo di vita

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lifecycle.s3.amazonaws.com"
      },
      "Action": "s3express:CreateSession",
      "Condition": {
        "StringEquals": {
          "s3express:SessionMode": "ReadWrite"
        }
      }
    }
  ],
}
```

```
    "Resource": "arn:aws:s3express:us-east-2:412345678921:bucket/amzn-s3-demo-  
bucket--use2-az2--x-s3"  
  }  
]  
}
```

Monitoraggio delle regole del ciclo di vita

Per gli oggetti archiviati in bucket di directory, S3 Lifecycle genera registri degli eventi di gestione e dati. AWS CloudTrail Per ulteriori informazioni, consulta [CloudTrail esempi di file di registro per bucket di directory](#).

Per ulteriori informazioni sulla creazione di configurazioni del ciclo di vita e sulla risoluzione dei problemi relativi a S3 Lifecycle, consulta i seguenti argomenti:

Creazione e gestione di una configurazione del ciclo di vita per il bucket della directory

È possibile creare una configurazione del ciclo di vita per i bucket di directory utilizzando AWS Command Line Interface (AWS CLI), SDK e API REST. AWS

Utilizzo di AWS CLI

È possibile utilizzare i seguenti AWS CLI comandi per gestire le configurazioni del ciclo di vita di S3:

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

Per istruzioni sulla configurazione di AWS CLI, consulta [Developing with Amazon S3 using the AWS CLI](#) nell'Amazon S3 API Reference.

La configurazione del ciclo di vita di Amazon S3 è un file XML. Tuttavia, quando si utilizza il formato XML AWS CLI, non è possibile specificare il formato XML. È necessario invece specificare il formato JSON. Di seguito sono riportati alcuni esempi di configurazioni del ciclo di vita XML e le configurazioni JSON equivalenti che è possibile specificare in un comando. AWS CLI

Il seguente esempio AWS CLI inserisce una politica di configurazione del ciclo di vita in un bucket di directory. Questa policy specifica che tutti gli oggetti che hanno il prefisso contrassegnato (`myprefix`) e la dimensione dell'oggetto definita scadono dopo 7 giorni. Per utilizzare questo comando, sostituisci *user input placeholder* con le tue informazioni.

Salva la policy di configurazione del ciclo di vita in un file JSON. In questo esempio, il file si chiama `lifecycle1.json`.

Example

JSON

```
{
  "Rules": [
    {
      "Expiration": {
        "Days": 7
      },
      "ID": "Lifecycle expiration rule",
      "Filter": {
        "And": {
          "Prefix": "myprefix/",
          "ObjectSizeGreaterThan": 500,
          "ObjectSizeLessThan": 64000
        }
      },
      "Status": "Enabled"
    }
  ]
}
```

Inviare il file JSON come parte del comando CLI `put-bucket-lifecycle-configuration`. Per usare questo comando, sostituire *user input placeholder* con le proprie informazioni.

```
aws s3api put-bucket-lifecycle-configuration --region us-west-2 --profile default
--bucket amzn-s3-demo-bucket--usw2-az1--x-s3 --lifecycle-configuration file://lc-policy.json --checksum-algorithm crc32c
```

Example

XML

```
<LifecycleConfiguration>
  <Rule>
    <ID>Lifecycle expiration rule</ID>
    <Filter>
```

```

        <And>
            <Prefix>myprefix/</Prefix>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
            <ObjectSizeLessThan>64000</ObjectSizeLessThan>
        </And>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
        <Days>7</Days>
    </Expiration>
</Rule>
</LifecycleConfiguration>

```

Utilizzo di AWS SDK

SDK for Java

Example

```

import
    software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationRequest;
import
    software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationResponse;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.BucketLifecycleConfiguration;
import software.amazon.awssdk.services.s3.model.LifecycleRule;
import software.amazon.awssdk.services.s3.model.LifecycleRuleFilter;
import software.amazon.awssdk.services.s3.model.LifecycleExpiration;
import software.amazon.awssdk.services.s3.model.LifecycleRuleAndOperator;
import
    software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationResponse;
import
    software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleResponse;
import software.amazon.awssdk.services.s3.model.AbortIncompleteMultipartUpload;

// PUT a Lifecycle policy
LifecycleRuleFilter objectExpirationFilter =
    LifecycleRuleFilter.builder().and(LifecycleRuleAndOperator.builder().prefix("dir1/").object
LifecycleRuleFilter mpuExpirationFilter =
    LifecycleRuleFilter.builder().prefix("dir2/").build();

```

```

LifecycleRule objectExpirationRule =
    LifecycleRule.builder().id("lc").filter(objectExpirationFilter).status("Enabled").expiration(
        .days(10)
        .build())
        .build();
LifecycleRule mpuExpirationRule = LifecycleRule.builder().id("lc-
mpu").filter(mpuExpirationFilter).status("Enabled").abortIncompleteMultipartUpload(AbortInco
        .daysAfterInitiation(10)
        .build())
        .build();

PutBucketLifecycleConfigurationRequest putLifecycleRequest =
    PutBucketLifecycleConfigurationRequest.builder()
        .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3")
        .checksumAlgorithm(ChecksumAlgorithm.CRC32)
        .lifecycleConfiguration(
            BucketLifecycleConfiguration.builder()
                .rules(objectExpirationRule, mpuExpirationRule)
                .build()
        ).build();

PutBucketLifecycleConfigurationResponse resp =
    client.putBucketLifecycleConfiguration(putLifecycleRequest);

// GET the Lifecycle policy
GetBucketLifecycleConfigurationResponse getResp =
    client.getBucketLifecycleConfiguration(GetBucketLifecycleConfigurationRequest.builder().bu
s3-demo-bucket--usw2-az1--x-s3").build());

// DELETE the Lifecycle policy
DeleteBucketLifecycleResponse delResp =
    client.deleteBucketLifecycle(DeleteBucketLifecycleRequest.builder().bucket("amzn-
s3-demo-bucket--usw2-az1--x-s3").build());

```

SDK for Go

Example

```

package main

import (
    "context"
    "log"

```

```

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
    "github.com/aws/aws-sdk-go-v2/service/s3/types"
)
// PUT a Lifecycle policy
func putBucketLifecycleConfiguration(client *s3.Client, bucketName string ) error {
    lifecycleConfig := &s3.PutBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
        LifecycleConfiguration: &types.BucketLifecycleConfiguration{
            Rules: []types.LifecycleRule{
                {
                    ID:      aws.String("lc"),
                    Filter: &types.LifecycleRuleFilter{
                        And: &types.LifecycleRuleAndOperator{
                            Prefix: aws.String("foo/"),
                            ObjectSizeGreaterThan: aws.Int64(1000000),
                            ObjectSizeLessThan:    aws.Int64(1000000000),
                        },
                    },
                    Status: types.ExpirationStatusEnabled,
                    Expiration: &types.LifecycleExpiration{
                        Days: aws.Int32(int32(1)),
                    },
                },
                {
                    ID:      aws.String("abortmpu"),
                    Filter: &types.LifecycleRuleFilter{
                        Prefix: aws.String("bar/"),
                    },
                    Status: types.ExpirationStatusEnabled,
                    AbortIncompleteMultipartUpload:
&types.AbortIncompleteMultipartUpload{
                        DaysAfterInitiation: aws.Int32(int32(5)),
                    },
                },
            },
        },
    }
    _, err := client.PutBucketLifecycleConfiguration(context.Background(),
lifecycleConfig)
    return err
}

```

```
// Get the Lifecycle policy
func getBucketLifecycleConfiguration(client *s3.Client, bucketName string) error {
    getLifecycleConfig := &s3.GetBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
    }

    resp, err := client.GetBucketLifecycleConfiguration(context.Background(),
getLifecycleConfig)
    if err != nil {
        return err
    }
    return nil
}

// Delete the Lifecycle policy
func deleteBucketLifecycleConfiguration(client *s3.Client, bucketName string) error
{
    deleteLifecycleConfig := &s3.DeleteBucketLifecycleInput{
        Bucket: aws.String(bucketName),
    }
    _, err := client.DeleteBucketLifecycle(context.Background(),
deleteLifecycleConfig)
    return err
}

func main() {
    cfg, err := config.LoadDefaultConfig(context.Background(),
config.WithRegion("us-west-2")) // Specify your region here
    if err != nil {
        log.Fatalf("unable to load SDK config, %v", err)
    }
    s3Client := s3.NewFromConfig(cfg)
    bucketName := "amzn-s3-demo-bucket--usw2-az1--x-s3"
    putBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
    deleteBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
}
```

SDK for .NET

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
```



```
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "amzn-s3-demo-bucket--usw2-az1--x-s3";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List <LifecycleRule>
                    {
                        new LifecycleRule
                        {
                            Id = "delete rule",
                            Filter = new LifecycleFilter()
                            {
                                LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                {
                                    Prefix = "projectdocs/"
                                }
                            },
                            Status = LifecycleRuleStatus.Enabled,
                            Expiration = new LifecycleRuleExpiration()
                            {
                                Days = 10
                            }
                        }
                    }
                }
            }
        }
    }
}
```

```
        }
    };

    // Add the configuration to the bucket.
    await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

    // Retrieve an existing configuration.
    lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

    // Add a new rule.
    lifeCycleConfiguration.Rules.Add(new LifecycleRule
    {
        Id = "mpu abort rule",
        Filter = new LifecycleFilter()
        {
            LifecycleFilterPredicate = new LifecyclePrefixPredicate()
            {
                Prefix = "YearlyDocuments/"
            }
        },
        Expiration = new LifecycleRuleExpiration()
        {
            Days = 10
        },
        AbortIncompleteMultipartUpload = new
LifecycleRuleAbortIncompleteMultipartUpload()
        {
            DaysAfterInitiation = 10
        }
    });

    // Add the configuration to the bucket.
    await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

    // Verify that there are now two rules.
    lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
    Console.WriteLine("Expected # of rulest=2; found:{0}",
lifeCycleConfiguration.Rules.Count);

    // Delete the configuration.
    await RemoveLifecycleConfigAsync(client);
```

```
        // Retrieve a nonexistent configuration.
        lifecycleConfiguration = await RetrieveLifecycleConfigAsync(client);

    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
}

static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
{
    PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
    {
        BucketName = bucketName,
        Configuration = configuration
    };
    var response = await client.PutLifecycleConfigurationAsync(request);
}

static async Task <LifecycleConfiguration>
RetrieveLifecycleConfigAsync(IAmazonS3 client)
{
    GetLifecycleConfigurationRequest request = new
GetLifecycleConfigurationRequest
    {
        BucketName = bucketName
    };
    var response = await client.GetLifecycleConfigurationAsync(request);
    var configuration = response.Configuration;
    return configuration;
}

static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
{

```

```

        DeleteLifecycleConfigurationRequest request = new
DeleteLifecycleConfigurationRequest
    {
        BucketName = bucketName
    };
    await client.DeleteLifecycleConfigurationAsync(request);
    }
}
}

```

SDK for Python

Example

```

import boto3

client = boto3.client("s3", region_name="us-west-2")
bucket_name = 'amzn-s3-demo-bucket--usw2-az1--x-s3'

client.put_bucket_lifecycle_configuration(
    Bucket=bucket_name,
    ChecksumAlgorithm='CRC32',
    LifecycleConfiguration={
        'Rules': [
            {
                'ID': 'lc',
                'Filter': {
                    'And': {
                        'Prefix': 'foo/',
                        'ObjectSizeGreaterThan': 1000000,
                        'ObjectSizeLessThan': 100000000,
                    }
                },
                'Status': 'Enabled',
                'Expiration': {
                    'Days': 1
                }
            },
            {
                'ID': 'abortmpu',
                'Filter': {
                    'Prefix': 'bar/'
                }
            }
        ]
    }
)

```

```
        'Status': 'Enabled',
        'AbortIncompleteMultipartUpload': {
            'DaysAfterInitiation': 5
        }
    ]
}

)

result = client.get_bucket_lifecycle_configuration(
    Bucket=bucket_name
)

client.delete_bucket_lifecycle(
    Bucket=bucket_name
)
```

Risoluzione dei problemi di S3 Lifecycle per i bucket di directory

Argomenti

- [La configurazione del ciclo di vita è impostata ma gli oggetti nel bucket della directory non scadono](#)
- [Come posso monitorare le azioni intraprese dalle mie regole del ciclo di vita?](#)

La configurazione del ciclo di vita è impostata ma gli oggetti nel bucket della directory non scadono

S3 Lifecycle per i bucket della directory utilizza API pubbliche per eliminare gli oggetti in S3 Express One Zone. Per utilizzare le API pubbliche a livello di oggetto, è necessario concedere l'autorizzazione a `CreateSession` e consentire a S3 Lifecycle di eliminare gli oggetti. Se si dispone di una policy attiva che nega le eliminazioni, questa impedirà di consentire a S3 Lifecycle di eliminare gli oggetti per conto dell'utente.

È importante configurare correttamente le policy di bucket per assicurarsi che gli oggetti da eliminare siano idonei alla scadenza. Puoi controllare i AWS CloudTrail log di `AccessDenied` Trails per le chiamate `CreateSession` API per verificare se l'accesso è stato CloudTrail negato. La verifica dei CloudTrail log può aiutarti a risolvere i problemi di accesso e a identificare la causa principale degli errori di accesso negato. È quindi possibile correggere i controlli di accesso errati aggiornando le policy pertinenti.

Se si conferma che le policy di bucket sono impostate correttamente e si riscontrano ancora problemi, si consiglia di rivedere le regole del ciclo di vita per assicurarsi che siano applicate al giusto sottoinsieme di oggetti.

Come posso monitorare le azioni intraprese dalle mie regole del ciclo di vita?

È possibile utilizzare AWS CloudTrail i registri degli eventi di dati per monitorare le azioni intraprese da S3 Lifecycle nei bucket di directory. Per ulteriori informazioni, consulta [CloudTrail gli esempi di file di registro](#).

Utilizzo di Operazioni in batch con i bucket di directory

Puoi utilizzare Operazioni in batch Amazon S3 per eseguire operazioni su oggetti archiviati in bucket S3. Per ulteriori informazioni su Operazioni in batch S3, consulta [Esecuzione di operazioni in batch su larga scala su oggetti Amazon S3](#).

I seguenti argomenti trattano l'esecuzione di operazioni in batch su oggetti memorizzati nella classe di storage S3 Express One Zone in bucket di directory.

Argomenti

- [Utilizzo di Operazioni in batch con i bucket di directory](#)
- [Differenze principali](#)

Utilizzo di Operazioni in batch con i bucket di directory

È possibile eseguire l'operazione di copia e le operazioni di invocazione della funzione AWS Lambda sugli oggetti memorizzati nei bucket della directory. Con Copia, è possibile copiare oggetti tra bucket dello stesso tipo (ad esempio, da un bucket directory a un bucket directory). Inoltre, puoi copiare oggetti tra bucket per uso generico e bucket di directory. Con AWS Lambda la funzione Invoke, puoi usare una funzione Lambda per eseguire azioni sugli oggetti nel bucket di directory con il codice che definisci.

Copia di oggetti

Puoi copiare tra lo stesso tipo di bucket o tra bucket di directory e bucket per uso generico. Quando si copia in un bucket di directory, è necessario utilizzare il formato di nome della risorsa Amazon (ARN) corretto per questo tipo di bucket. Il formato ARN per un bucket di directory è `arn:aws:s3express:region:account-id:bucket/bucket-base-name--x-s3`.

 Note

La copia di oggetti tra diverse Regioni AWS non è supportata quando il bucket di origine o di destinazione si trova in una zona locale. AWS I bucket di origine e di destinazione devono avere lo stesso Regione AWS padre. I bucket di origine e di destinazione possono essere di tipo diverso (zona di disponibilità o zona locale).

Puoi anche popolare il bucket di directory con dati utilizzando l'azione **Importa** nella console S3. L'azione **Importa** è un metodo ottimizzato di creazione di processi Operazioni in batch S3 per copiare oggetti da bucket per uso generico in bucket di directory. Per i processi di copia **Importa** da bucket per uso generico a bucket di directory, S3 genera automaticamente un manifesto. Per ulteriori informazioni, consulta [Importazione di oggetti in un bucket della directory](#) e [Specifica di un manifesto](#).

Invocazione di funzioni Lambda (**LambdaInvoke**)

Esistono requisiti speciali per l'uso di Operazioni in batch per invocare funzioni Lambda che agiscono sui bucket della directory. Ad esempio, è necessario strutturare la richiesta Lambda utilizzando uno schema di invocazione JSON v2 e specificare `InvocationSchemaVersion 2.0` quando si crea il processo. Per ulteriori informazioni, consulta [Invoca funzione AWS Lambda](#).

Differenze principali

Di seguito sono elencate le differenze principali quando si utilizza Operazioni in batch per eseguire operazioni in blocco su oggetti archiviati in bucket di directory con la classe di storage S3 Express One Zone:

- Per i bucket di directory, sono SSE-S3 supportate la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (). SSE-KMS Se si effettua una `CopyObject` richiesta che specifica di utilizzare la crittografia lato server con chiavi (SSE-C) fornite dal cliente su un bucket di directory (origine o destinazione), la risposta restituisce un errore HTTP. 400 (Bad Request)

Si consiglia di utilizzare la configurazione di crittografia predefinita del bucket e di non sovrascrivere la crittografia predefinita del bucket nelle richieste `CreateSession` o nelle richieste di oggetti `PUT`. I nuovi oggetti vengono quindi crittografati automaticamente con le impostazioni di crittografia desiderate. Per ulteriori informazioni sui comportamenti di crittografia che sovrascrivono nei bucket di directory e su come crittografare le copie di nuovi oggetti in un bucket di directory con SSE-KMS, vedi [Specificare la crittografia lato server con per il caricamento di nuovi oggetti](#). [AWS KMS](#)

Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket generici o tra bucket di directory, tramite l'operazione in Batch Operations. [Copy](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia per un oggetto. KMS-encrypted Per ulteriori informazioni SSE-KMS sull'utilizzo nei bucket di directory, consulta [Impostazione e monitoraggio della crittografia predefinita per i bucket di directory](#) e [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket di directory](#)

- Gli oggetti nei bucket di directory non possono essere taggati. Puoi specificare solo un set di tag vuoto. Per impostazione predefinita, Operazioni in batch copia i tag. Se si copia un oggetto che ha dei tag tra i bucket per uso generico e i bucket di directory, si riceve una risposta 501 (Not Implemented).
- S3 Express One Zone offre la possibilità di scegli l'algoritmo di checksum utilizzato per convalidare i dati durante il caricamento o il download. È possibile selezionare uno dei seguenti algoritmi di controllo dell'integrità dei dati Secure Hash Algorithms (SHA) o Cyclic Redundancy Check (CRC): CRC32, CRC32 e. SHA-1 SHA-256 MD5-basedi checksum non sono supportati con la classe di storage S3 Express One Zone.
- Per impostazione predefinita, tutti i bucket Amazon S3 impostano la proprietà dell'oggetto S3 sul proprietario del bucket e le liste di controllo degli accessi (ACL) sono disabilitate. Per i bucket di directory, questa impostazione non può essere modificata. È possibile copiare un oggetto da bucket per uso generico in bucket di directory. Tuttavia, non è possibile sovrascrivere l'ACL predefinita quando si copia da o verso un bucket di directory.
- A prescindere dalla modalità di specifica del manifesto, l'elenco stesso deve essere archiviato in un bucket per uso generico. Operazioni in batch non può importare manifesti esistenti da (o salvare manifesti generati in) bucket di directory. Tuttavia, gli oggetti descritti all'interno del manifesto possono essere archiviati in bucket di directory.
- Puoi utilizzare i report di inventario di S3 dai bucket di directory come origine per il tuo manifest, purché il rapporto di inventario sia archiviato in un bucket generico. Puoi anche creare un file manifesto per gli oggetti all'interno di un bucket di directory utilizzando l'operazione ListObjectsV2 API per elencare gli oggetti e quindi inserire l'elenco in un file CSV.

Concessione dell'accesso per

Per eseguire processi di copia, è necessario disporre delle autorizzazioni seguenti:

- Per copiare oggetti da un bucket di directory a un altro, è necessario disporre dell'autorizzazione `s3express:CreateSession`.
- Per copiare gli oggetti dai bucket di directory ai bucket per uso generico, è necessario disporre dell'autorizzazione `s3express:CreateSession` e dell'autorizzazione `s3:PutObject` per scrivere la copia dell'oggetto nel bucket di destinazione.
- Per copiare oggetti da bucket per uso generico a bucket di directory, è necessario disporre dei permessi `s3express:CreateSession` e `s3:GetObject` per leggere l'oggetto di origine che si sta copiando.

Per ulteriori informazioni, consulta [CopyObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

- Per richiamare una funzione Lambda, è necessario concedere le autorizzazioni alla risorsa in base alla funzione Lambda. Per determinare quali autorizzazioni sono necessarie, controllare le operazioni API corrispondenti.

Aggiunta di dati agli oggetti nei bucket della directory

È possibile aggiungere dati alla fine di oggetti esistenti memorizzati nella classe di storage S3 Express One Zone in bucket di directory. Si consiglia di utilizzare la possibilità di aggiungere dati a un oggetto se i dati vengono scritti continuamente per un certo periodo di tempo o se è necessario leggere l'oggetto mentre si sta scrivendo sull'oggetto. L'aggiunta di dati agli oggetti è comune per casi d'uso quali l'aggiunta di nuove voci di log ai file di log o l'aggiunta di nuovi segmenti video ai file video durante la transcodifica e lo streaming. Aggiungendo dati agli oggetti, è possibile semplificare le applicazioni che in precedenza combinavano i dati nell'archiviazione locale prima di copiare l'oggetto finale su Amazon S3.

Non esiste un requisito di dimensione minima per i dati che si possono aggiungere a un oggetto. Tuttavia, la dimensione massima dei dati che si possono aggiungere a un oggetto in una singola richiesta è di 5 GB. Questo è lo stesso limite della dimensione massima della richiesta quando si caricano dati utilizzando qualsiasi API Amazon S3.

Con ogni operazione di aggiunta riuscita, si crea una parte dell'oggetto e ogni oggetto può avere fino a 10.000 parti. Ciò significa che è possibile aggiungere dati a un oggetto fino a 10.000 volte. Se un oggetto viene creato utilizzando il caricamento multiparte S3, ogni parte caricata viene conteggiata nel limite massimo totale di 10.000 parti. Ad esempio, è possibile aggiungere fino a 9.000 volte a un oggetto creato con un caricamento multiparte composto da 1.000 parti.

 Note

Se raggiungi il limite di parti, riceverai un [TooManyParts](#) errore. È possibile utilizzare l'API `CopyObject` per azzerare il conteggio.

Se si desidera caricare parti di un oggetto in parallelo e non è necessario leggere le parti mentre vengono caricate, si consiglia di utilizzare il caricamento multiparte di Amazon S3. Per ulteriori informazioni, consulta [Utilizzo del caricamento multiparte](#).

L'aggiunta di dati agli oggetti è supportata solo per gli oggetti nei bucket della directory archiviati nella classe di storage S3 Express One Zone. Per ulteriori informazioni su S3 Express One Zone, consulta [Introduzione a S3 Express One Zone](#).

Per iniziare ad aggiungere dati agli oggetti nei bucket di directory, puoi utilizzare gli AWS SDK, la AWS CLI e l'API. `PutObject` Quando si effettua una richiesta `PutObject`, si imposta l'intestazione `x-amz-write-offset-bytes` sulla dimensione dell'oggetto a cui si sta aggiungendo. Per utilizzare l'operazione API `PutObject`, è necessario utilizzare l'API `CreateSession` per stabilire credenziali di sicurezza temporanee per accedere agli oggetti nei bucket della directory. Per ulteriori informazioni, consulta [PutObject](#) e [CreateSession](#) nella documentazione di riferimento delle API di Amazon S3.

Ogni operazione di aggiunta andata a buon fine viene conteggiata come una richiesta di `PutObject`. Per saperne di più sui prezzi, consulta [Amazon S3 pricing](#).

 Note

A partire dalla versione 1.12, Mountpoint per Amazon S3 supporta l'aggiunta di dati agli oggetti memorizzati in S3 Express One Zone. Per iniziare, è necessario effettuare l'opt-in impostando il flag `--incremental-upload`. Per ulteriori informazioni su Mountpoint, consulta [Operazioni con Mountpoint](#).

Se utilizzi un algoritmo CRC (Cyclic Redundancy Check) durante il caricamento dei dati aggiunti, puoi recuperare i checksum completi degli oggetti utilizzando la richiesta `or. CRC-based HeadObject GetObject`. Se utilizzi l' SHA-256 algoritmo SHA-1 `or` durante il caricamento dei dati aggiunti, puoi recuperare un checksum delle parti aggiunte e verificarne l'integrità utilizzando i checksum SHA restituiti nelle risposte precedenti. `PutObject` Per ulteriori informazioni, consulta [Protezione dei dati e crittografia](#).

Aggiungere dati agli oggetti utilizzando il AWS CLI, AWS SDK e API REST

Puoi aggiungere dati ai tuoi oggetti utilizzando AWS Command Line Interface (AWS CLI), AWS SDK e API REST.

Utilizzo di AWS CLI

Il seguente comando di `put-object` esempio mostra come è possibile utilizzare la AWS CLI per aggiungere dati a un oggetto. Per eseguire questo comando, sostituiscilo *user input placeholders* con le tue informazioni

```
aws s3api put-object --bucket amzn-s3-demo-bucket--azid--x-s3 --key sampleinput/file001.bin --body bucket-seed/file001.bin --write-offset-bytes size-of-sampleinput/file001.bin
```

Utilizzo di AWS SDK

SDK for Java

Puoi usare il AWS SDK per Java per aggiungere dati ai tuoi oggetti.

```
var putObjectRequestBuilder = PutObjectRequest.builder()  
                                .key(key)  
                                .bucket(bucketName)  
                                .writeOffsetBytes(9);  
var response = s3Client.putObject(putObjectRequestBuilder.build());
```

SDK for Python

```
s3.put_object(Bucket='amzn-s3-demo-bucket--use2-az2--x-s3', Key='2024-11-05-sdk-test', Body=b'123456789', WriteOffsetBytes=9)
```

Utilizzo della REST API

È possibile inviare richieste REST per aggiungere dati a un oggetto. Per ulteriori informazioni, consulta [PutObject](#).

Ridenominazione degli oggetti nei bucket di directory

L'operazione `RenameObject` consente di rinominare automaticamente un oggetto esistente in un bucket di directory che utilizza la classe di archiviazione S3 Express One Zone, senza alcun

movimento di dati. È possibile rinominare un oggetto specificando il nome dell'oggetto esistente come origine e il nuovo nome dell'oggetto come destinazione all'interno dello stesso bucket di directory. L'operazione API `RenameObject` non ha esito positivo sugli oggetti che terminano con il carattere delimitatore barra (/). Per ulteriori informazioni, consulta [Denominazione di oggetti Amazon S3](#).

L'operazione `RenameObject` viene in genere completata nell'ordine di millisecondi indipendentemente dalla dimensione dell'oggetto. Questa funzionalità accelera applicazioni come la gestione dei file di log, l'elaborazione multimediale e l'analisi dei dati. Inoltre, `RenameObject` conserva tutte le proprietà dei metadati degli oggetti, tra cui la classe di archiviazione, il tipo di crittografia, la data di creazione, la data dell'ultima modifica e le proprietà del checksum.

Note

L'operazione `RenameObject` è supportata solo per gli oggetti archiviati nella classe di archiviazione S3 Express One Zone.

Per fornire l'accesso all'operazione `RenameObject`, è consigliabile utilizzare l'operazione `CreateSession` per l'autorizzazione basata sulla sessione. In particolare, si fornisce l'autorizzazione `s3express:CreateSession` al bucket di directory in una policy di bucket o in una policy basata sull'identità. Quindi, si effettua la chiamata API `CreateSession` sul bucket di directory per ottenere un token di sessione. Con il token di sessione nell'intestazione della richiesta, è possibile effettuare richieste API per questa operazione. Dopo la scadenza del token di sessione, si effettua un'altra chiamata API `CreateSession` per generare un nuovo token di sessione da utilizzare. La AWS CLI e AWS gli SDK creeranno e gestiranno la sessione, incluso l'aggiornamento automatico del token di sessione per evitare interruzioni del servizio alla scadenza di una sessione. Per ulteriori informazioni, consulta [CreateSession](#) nella Guida di riferimento delle API di Amazon S3. Per ulteriori informazioni sulle operazioni API degli endpoint di zona, consulta [Autorizzazione delle operazioni API dell'endpoint di zona con CreateSession](#).

Se non desideri sovrascrivere un oggetto esistente, è possibile aggiungere l'intestazione condizionale `If-None-Match` con il valore `'*'` nella richiesta `RenameObject`. Amazon S3 restituisce un errore `412 Precondition Failed` se il nome dell'oggetto esiste già. Per ulteriori informazioni, consulta [RenameObject](#) nella documentazione di riferimento delle API di Amazon S3.

`RenameObject` è un'operazione API dell'endpoint di zona (operazione a livello di oggetto o piano dati) che viene registrata nel log in AWS CloudTrail. Puoi utilizzarlo CloudTrail per raccogliere informazioni sull'`RenameObject` operazione eseguita sui tuoi oggetti nei bucket di directory. Per

ulteriori informazioni, vedere [Registrazione con AWS CloudTrail per bucket di directory](#) ed esempi di file di [CloudTrail registro per bucket di directory](#).

S3 Express One Zone è l'unica classe di archiviazione che supporta `RenameObject`, con un prezzo uguale a quello delle richieste `PUT`, `COPY`, `POST` e `LIST` (per 1.000 richieste) in S3 Express One Zone. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Ridenominazione di un oggetto

Per rinominare un oggetto nel tuo bucket di directory, puoi utilizzare la console Amazon S3, la AWS CLI, gli AWS SDK, l'API REST o Mountpoint for Amazon S3 (versione 1.19.0 o successiva).

Utilizzo della console S3

Come rinominare un oggetto in un bucket di directory

1. Accedi e apri la console Amazon S3 all'indirizzo. Console di gestione AWS <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli **Bucket**, quindi seleziona la scheda **Bucket di directory**. Passa al bucket di directory Amazon S3 contenente l'oggetto da rinominare.
3. Seleziona la casella di controllo dell'oggetto da rinominare.
4. Nel menu **Azioni**, scegli **Rinomina oggetto**.
5. Nella casella **Nuovo nome oggetto**, inserisci il nuovo nome dell'oggetto.

Note

Se specifichi lo stesso nome di un oggetto esistente, l'operazione ha esito negativo e Amazon S3 restituisce un errore `412 Precondition Failed`. La lunghezza del nome della chiave dell'oggetto non può superare 1.024 byte. I prefissi inclusi nel nome dell'oggetto vengono conteggiati ai fini della lunghezza totale.

6. Scegli **Rinomina l'oggetto**. Amazon S3 rinomina l'oggetto.

Utilizzo di AWS CLI

Gli esempi `rename-object` illustrano in che modo è possibile utilizzare l' AWS CLI per rinominare un oggetto. Per eseguire questi comandi, sostituiscili *user input placeholders* con le tue informazioni

L'esempio seguente mostra come rinominare un oggetto con un controllo condizionale sull'ETag dell'oggetto di origine.

```
aws s3api rename-object \  
  --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 \  
  --key new-file.txt \  
  --rename-source original-file.txt \  
  --source-if-match "\"a1b7c3d2e5f6\""
```

Questo comando funziona nel modo seguente:

- Rinomina un oggetto da *original-file.txt* a *new-file.txt* nel bucket di *amzn-s3-demo-bucket--usw2-az1--x-s3* directory.
- Esegue la ridenominazione solo se l'ETag dell'oggetto sorgente corrisponde a "». *a1b7c3d4e5f6*

Se l'ETag non corrisponde, l'operazione non riesce con un errore 412 `Precondition Failed`.

L'esempio seguente mostra come rinominare un oggetto con un controllo condizionale sul nuovo nome dell'oggetto specificato.

```
aws s3api rename-object \  
  --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 \  
  --key new-file.txt \  
  --rename-source amzn-s3-demo-bucket--usw2-az1--x-s3/original-file.txt \  
  --destination-if-none-match "\"e5f3g7h8i9j0\""
```

Questo comando funziona nel modo seguente:

- Rinomina un oggetto da *original-file.txt* a *new-file.txt* nel bucket di directory. *amzn-s3-demo-bucket--usw2-az1--x-s3*
- Esegue l'operazione di ridenominazione solo se l'oggetto esiste e l'ETag dell'oggetto non corrisponde a "». *e5f3g7h8i9j0*

Se esiste già un oggetto con il nuovo nome specificato e l'ETag corrispondente, l'operazione avrà esito negativo e verrà generato un errore 412 `Precondition Failed`.

Utilizzo di AWS SDK

SDK for Java

Puoi usare il AWS SDK per Java per rinominare i tuoi oggetti. Per utilizzare questi esempi, sostituiscili *user input placeholders* con le tue informazioni

L'esempio seguente dimostra come creare un `RenameObjectRequest` utilizzando l' AWS SDK per Java

```
String key = "key";
String newKey = "new-key";
String expectedETag = "e5f3g7h8i9j0";
RenameObjectRequest renameRequest = RenameObjectRequest.builder()
    .bucket(amzn-s3-demo-bucket--usw2-az1--x-s3)
    .key(newKey)
    .renameSource(key)
    .destinationIfMatch(e5f3g7h8i9j0)
    .build();
```

Il codice effettua le seguenti operazioni:

- Crea una richiesta per rinominare un oggetto da "" a key "new-key" nel bucket di directory. *amzn-s3-demo-bucket--usw2-az1--x-s3*
- Include una condizione secondo cui la ridenominazione avverrà solo se l'ETag dell'oggetto corrisponde a "». *e5f3g7h8i9j0*
- Se l'ETag non corrisponde o l'oggetto non esiste, l'operazione non riesce.

L'esempio seguente mostra come creare una condizione `RenameObjectRequest` con una non corrispondenza utilizzando l'SDK per Java. AWS

```
String key = "key";
String newKey = "new-key";
String noneMatchETag = "e5f3g7h8i9j0";
RenameObjectRequest renameRequest = RenameObjectRequest.builder()
    .bucket(amzn-s3-demo-bucket--usw2-az1--x-s3)
    .key(newKey)
    .renameSource(key)
    .destinationIfNoneMatch(noneMatchETag)
    .build();
```

Il codice effettua le seguenti operazioni:

- Crea una richiesta per rinominare un oggetto da "" a "*keynew-key*" nel bucket di directory. *amzn-s3-demo-bucket--usw2-az1--x-s3*
- Include una condizione `.destinationIfNoneMatch(noneMatchETag)` che garantisce che la ridenominazione avvenga solo se l'ETag dell'oggetto di destinazione non corrisponde a "». *e5f3g7h8i9j0*

L'operazione non riesce con un errore `412 Precondition Failed` se esiste un oggetto con il nuovo nome specificato e l'ETag specificato.

SDK for Python

È possibile utilizzare SDK per Python per rinominare gli oggetti. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

L'esempio seguente dimostra come rinominare un oggetto utilizzando l' AWS SDK per Python (Boto3).

```
def basic_rename(bucket, source_key, destination_key):
    try:
        s3.rename_object(
            Bucket=amzn-s3-demo-bucket--usw2-az1--x-s3,
            Key=destination_key,
            RenameSource=f"{source_key}"
        )
        print(f"Successfully renamed {source_key} to {destination_key}")
    except ClientError as e:
        print(f"Error renaming object: {e}")
```

Il codice effettua le seguenti operazioni:

- Rinomina un oggetto da a nel bucket di directory. *source_key destination_key amzn-s3-demo-bucket--usw2-az1--x-s3*
- Stampa un messaggio di esito positivo se la ridenominazione dell'oggetto è stata completata o stampa un messaggio di errore se non è riuscita.

L'esempio seguente dimostra come rinominare un oggetto con `DestinationIfNoneMatch` le condizioni `SourceIfMatch` and utilizzando l' AWS SDK per Python (Boto3).


```
def rename_with_conditions(bucket, source_key, destination_key, source_etag,
    dest_etag):
    try:
        s3.rename_object(
            Bucket=amzn-s3-demo-bucket--usw2-az1--x-s3,
            Key=destination_key,
            RenameSource=f"{amzn-s3-demo-bucket--usw2-az1--x-s3}/{source_key}",
            SourceIfMatch=source_ETag,
            DestinationIfNoneMatch=dest_ETag
        )
        print(f"Successfully renamed {source_key} to {destination_key} with
conditions")
    except ClientError as e:
        print(f"Error renaming object: {e}")
```

Il codice effettua le seguenti operazioni:

- Esegue un'operazione di ridenominazione condizionale e applica due condizioni, `SourceIfMatch` e `DestinationIfNoneMatch`. La combinazione di queste condizioni assicura che l'oggetto non sia stato modificato e che non esista già un oggetto con il nuovo nome specificato.
- Rinomina un oggetto da *source_key* a nel bucket di directory. *destination_key amzn-s3-demo-bucket--usw2-az1--x-s3*
- Stampa un messaggio di esito positivo se la ridenominazione dell'oggetto è stata completata o stampa un messaggio di errore se non è riuscita o se le condizioni non sono soddisfatte.

SDK for Rust

È possibile utilizzare SDK per Rust per rinominare gli oggetti. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

L'esempio seguente mostra come rinominare un oggetto nel bucket di directory *amzn-s3-demo-bucket--usw2-az1--x-s3* utilizzando SDK per Rust.

```
async fn basic_rename_example(client: &Client) -> Result<(), Box<dyn Error>> {
    let response = client
        .rename_object()
        .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3")
        .key("new-name.txt") // New name/path for the object
        .rename_source("old-name.txt") // Original object name/path
```

```
        .send()  
        .await?;  
    ok(()  
}
```

Il codice effettua le seguenti operazioni:

- Crea una richiesta per rinominare un oggetto da "" a *old-name.tx new-name.txt* "nel bucket di directory. *amzn-s3-demo-bucket--usw2-az1--x-s3*
- Restituisce un tipo `Result` per gestire potenziali errori.

Utilizzo della REST API

Per rinominare un oggetto è possibile inviare richieste REST. Per ulteriori informazioni, consulta [RenameObject](#) nella documentazione di riferimento delle API di Amazon S3.

Utilizzo di Mountpoint per Amazon S3

A partire dalla versione 1.19.0 o successiva, Mountpoint per Amazon S3 supporta la ridenominazione degli oggetti in S3 Express One Zone. Per ulteriori informazioni su Mountpoint, consulta [Operazioni con Mountpoint](#).

Caricamento di oggetti in un bucket di directory

Dopo aver creato un bucket di directory Amazon S3, è possibile caricarvi oggetti. Gli esempi seguenti mostrano come caricare un oggetto in un bucket di directory utilizzando la console S3 e gli SDK AWS . Per informazioni sulle operazioni di caricamento di oggetti in blocco con S3 Express One Zone, consulta [Gestione degli oggetti](#).

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Scegli il nome del bucket in cui caricare le cartelle o i file.
4. Nell'elenco Oggetti, scegli Carica.
5. Nella pagina di caricamento, esegui una delle seguenti operazioni:

- Trascina e rilascia i file e le cartelle nell'area di caricamento tratteggiata.
- Scegli Aggiungi file o Aggiungi cartella, scegli i file o le cartelle da caricare, quindi scegli Apri o Carica.

6. In Checksum, scegli la funzione Checksum da utilizzare.

(Facoltativo) Se si sta caricando un singolo oggetto di dimensioni inferiori a 16 MB, si può anche specificare un valore di checksum precalcolato. Quando si fornisce un valore precalcolato, Amazon S3 lo confronta con il valore calcolato utilizzando la funzione di checksum selezionata. Se i valori non corrispondono, il caricamento non viene avviato.

7. Le opzioni delle sezioni Autorizzazioni e Proprietà sono impostate automaticamente come predefinite e non possono essere modificate. Blocco dell'accesso pubblico è abilitato automaticamente; Controllo delle versioni S3 e S3 Object Lock non possono essere abilitati per i bucket della directory.

(Facoltativo) Se desideri aggiungere metadati in coppie chiave-valore agli oggetti, espandi la sezione Proprietà e scegli Aggiungi metadati nella sezione Metadati.

8. Per caricare i file e le cartelle elencati, scegli Carica.

Amazon S3 caricherà i tuoi oggetti e le tue cartelle. Al termine del caricamento viene visualizzato un messaggio di esito positivo nella pagina Carica: stato.

Utilizzo di AWS SDK

SDK for Java 2.x

Example

```
public static void putObject(S3Client s3Client, String bucketName, String objectKey,
    Path filePath) {
    //Using File Path to avoid loading the whole file into memory
    try {
        PutObjectRequest putObj = PutObjectRequest.builder()
            .bucket(bucketName)
            .key(objectKey)
            //.metadata(metadata)
            .build();
        s3Client.putObject(putObj, filePath);
        System.out.println("Successfully placed " + objectKey + " into bucket "
            + bucketName);
    }
```

```

    }

    catch (S3Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

SDK for Python

Example

```

import boto3
import botocore
from botocore.exceptions import ClientError

def put_object(s3_client, bucket_name, key_name, object_bytes):
    """
    Upload data to a directory bucket.
    :param s3_client: The boto3 S3 client
    :param bucket_name: The bucket that will contain the object
    :param key_name: The key of the object to be uploaded
    :param object_bytes: The data to upload
    """
    try:
        response = s3_client.put_object(Bucket=bucket_name, Key=key_name,
                                         Body=object_bytes)
        print(f"Upload object '{key_name}' to bucket '{bucket_name}'.")
        return response
    except ClientError:
        print(f"Couldn't upload object '{key_name}' to bucket '{bucket_name}'.")
        raise

def main():
    # Share the client session with functions and objects to benefit from S3 Express
    # One Zone auth key
    s3_client = boto3.client('s3')
    # Directory bucket name must end with --zone-id--x-s3
    resp = put_object(s3_client, 'doc-bucket-example--use1-az5--x-s3', 'sample.txt',
                      b'Hello, World!')
    print(resp)

```

```
if __name__ == "__main__":  
    main()
```

Utilizzo di AWS CLI

Il seguente esempio di comando `put-object` mostra come utilizzare AWS CLI per caricare un oggetto da Amazon S3. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key sampleinput/  
file001.bin --body bucket-seed/file001.bin
```

Per ulteriori informazioni, consulta [put-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Argomenti

- [Utilizzo dei caricamenti multiparte con i bucket di directory](#)

Utilizzo dei caricamenti multiparte con i bucket di directory

È possibile utilizzare il processo di caricamento multiparte per caricare un singolo oggetto come un insieme di parti. Ciascuna parte è una parte contigua dei dati dell'oggetto. È possibile caricare queste parti dell'oggetto in modo indipendente e in qualsiasi ordine. Se la trasmissione di una parte non riesce, è possibile ritrasmettere tale parte senza influire sulle altre. Una volta caricate tutte le parti dell'oggetto, Amazon S3 le assembla e crea l'oggetto. In generale, quando la dimensione dell'oggetto raggiunge i 100 MB, si consiglia di valutare la possibilità di eseguire caricamenti in più parti anziché caricare l'oggetto in una singola operazione.

Il caricamento in più parti comporta i vantaggi riportati di seguito.

- Throughput migliorato: puoi caricare le parti in parallelo per migliorare il throughput.
- Ripristino rapido da qualsiasi problema di rete - Le dimensioni ridotte dei pezzi riducono al minimo l'impatto del riavvio di un caricamento fallito a causa di un errore di rete.
- Messa in pausa e ripresa dei caricamenti dell'oggetto: puoi caricare le parti dell'oggetto nel corso del tempo. Dopo aver avviato un caricamento multiparte, non c'è una data di scadenza. È necessario completare o interrompere esplicitamente il caricamento multiparte.

- Avvio di un caricamento prima di conoscere la dimensione finale dell'oggetto: puoi caricare un oggetto mentre viene creato.

Si consiglia di utilizzare i caricamenti multiparte nei seguenti modi:

- Se si caricano oggetti di grandi dimensioni su una rete stabile ad alta larghezza di banda, utilizzare i caricamenti multiparte per massimizzare l'uso della larghezza di banda disponibile, caricando le parti dell'oggetto in parallelo per ottenere prestazioni multi-thread.
- Se si sta caricando su una rete discontinua, utilizzare i caricamenti multiparte per aumentare la resilienza agli errori di rete evitando il riavvio del caricamento. Quando si utilizza il caricamento multiparte, è necessario riprovare a caricare solo le parti che si interrompono durante il caricamento. Non è necessario riavviare il caricamento dell'oggetto dall'inizio.

Quando si utilizzano i caricamenti multiparte per caricare oggetti nella classe di storage Amazon S3 Express One Zone in bucket di directory, il processo di caricamento multiparte è simile al processo di caricamento multiparte per caricare oggetti in bucket per uso generico. Tuttavia, non vi sono alcune differenze importanti.

Per ulteriori informazioni sull'uso dei caricamenti multiparte per caricare oggetti su S3 Express One Zone, consulta i seguenti argomenti.

Argomenti

- [Il processo di caricamento multiparte](#)
- [Checksum con operazioni di caricamento in più parti](#)
- [Operazioni simultanee di caricamento in più parti](#)
- [Caricamenti multiparte e prezzi](#)
- [Operazioni e autorizzazioni dell'API per il caricamento multiparte](#)
- [Esempi](#)

Il processo di caricamento multiparte

Un caricamento multiparte è un processo in tre fasi:

- L'utente avvia il caricamento.
- Si caricano le parti dell'oggetto.

- Dopo aver caricato tutte le parti, si completa il caricamento multiparte.

Una volta ricevuta la richiesta di caricamento multiparte completa, Amazon S3 costruisce l'oggetto dalle parti caricate e l'utente può quindi accedere all'oggetto come a qualsiasi altro oggetto nel bucket.

Avvio del caricamento in più parti

Quando invii una richiesta di avvio di un caricamento in più parti, Amazon S3 restituisce una risposta con un ID di caricamento, che è un identificativo univoco per il caricamento in più parti. È necessario includere questo ID di caricamento ogni volta che si caricano o si elencano le parti oppure ogni volta che si completa o si interrompe un caricamento.

Caricamento delle parti

Quando si carica una parte, oltre all'ID di caricamento è necessario specificare il numero della parte. Quando si utilizza un caricamento multiparte con S3 Express One Zone, i numeri di parte multiparte devono essere numeri di parte consecutivi. Se si tenta di completare una richiesta di caricamento multiparte con numeri di parte non consecutivi, viene generato un errore HTTP 400 Bad Request (Invalid Part Order).

Un numero di parte identifica in modo univoco una parte e la sua posizione nell'oggetto che si sta caricando. Se si carica una nuova parte utilizzando lo stesso numero di parte di una parte caricata in precedenza, la parte caricata in precedenza viene sovrascritta.

Ogni volta che carichi una parte, Amazon S3 restituisce un'intestazione tag di entità (ETag) nella risposta corrispondente. Per ogni caricamento di parte è necessario registrare il numero della parte e il valore ETag. I valori ETag per tutti i caricamenti di parti di oggetti rimarranno gli stessi, ma a ogni parte verrà assegnato un numero di parte diverso. Occorre includere questi valori nella successiva richiesta di complemento del caricamento in più parti.

Amazon S3 esegue automaticamente la crittografia di tutti i nuovi oggetti caricati in un bucket S3. Quando si esegue un caricamento in più parti, se non si specificano le informazioni di crittografia nella richiesta, l'impostazione di crittografia delle parti caricate viene impostata sulla configurazione di crittografia predefinita del bucket di destinazione. La configurazione di crittografia predefinita di un bucket Amazon S3 è sempre abilitata ed è almeno impostata sulla crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Per i bucket di directory, è supportata la SSE-S3 crittografia lato server con chiavi (). AWS KMS SSE-KMS Per ulteriori informazioni, consulta [Protezione e crittografia dei dati](#).

Completamento del caricamento in più parti

Quando si completa un caricamento multiparte, Amazon S3 crea l'oggetto concatenando le parti in ordine crescente in base al numero di parte. Una volta completata la richiesta, le parti non esisteranno più.

La richiesta di caricamento completo di più parti deve includere l'ID di caricamento e un elenco di entrambi i numeri di parte e dei valori ETag corrispondenti. La risposta di Amazon S3 include un ETag che identifica in modo univoco i dati oggetto combinati. Questo ETag non è un hash MD5 dei dati dell'oggetto.

Elenchi dei caricamenti in più parti

È possibile elencare le parti di un caricamento in più parti specifico o tutti i caricamenti in più parti in corso. L'operazione di creazione dell'elenco delle parti restituisce informazioni sulle parti coinvolte in un caricamento in più parti specifico. Per ogni richiesta di elenco delle parti, Amazon S3 restituisce informazioni sulle parti per il caricamento in più parti specificato, fino a un massimo di 1000 parti. Se nel caricamento in più parti sono presenti più di 1000 parti, è necessario utilizzare la paginazione per recuperare tutte le parti.

L'elenco di parti restituite non include quelle che non hanno terminato il caricamento. L'operazione `list multipart uploads` (elenco dei caricamenti in più parti) consente di ottenere l'elenco dei caricamenti in più parti in corso.

Un caricamento in più parti in corso è un caricamento avviato, ma non ancora completato o annullato. Ogni richiesta restituisce al massimo 1.000 caricamenti in più parti. Se sono in corso più di 1.000 caricamenti in più parti, è necessario inviare richieste aggiuntive per recuperare i caricamenti rimanenti. Utilizza l'elenco restituito solo per la verifica. Non utilizzarlo per inviare la richiesta completa multipart upload (completamento del caricamento in più parti). Al contrario, mantieni il tuo elenco dei numeri delle parti specificato durante il caricamento delle parti e i valori ETag corrispondenti restituiti da Amazon S3.

Per ulteriori informazioni sugli elenchi di caricamento multiparte, consulta [ListParts](#) in Riferimento API di Amazon Simple Storage Service.

Checksum con operazioni di caricamento in più parti

Quando si carica un oggetto, è possibile specificare un algoritmo di checksum per verificare l'integrità dell'oggetto. MD5 non è supportato per i bucket di directory. È possibile specificare uno dei seguenti

algoritmi di controllo dell'integrità dei dati Secure Hash Algorithms (SHA) o Cyclic Redundancy Check (CRC):

- CRC32
- CRC32C
- SHA-1
- SHA-256

Puoi utilizzare l'API REST di Amazon S3 o gli AWS SDK per recuperare il valore di checksum per le singole parti utilizzando `GetObjectHeadObject`. Se desideri recuperare i valori di checksum per singole parti di caricamenti in più parti ancora in corso, puoi utilizzare `ListParts`.

 Important

Quando si utilizzano i precedenti algoritmi di checksum, i numeri di parte multipart devono utilizzare numeri di parte consecutivi. Se si tenta di completare una richiesta di caricamento multipart con numeri di parte non consecutivi, Amazon S3 genera un errore HTTP 400 Bad Request (Invalid Part Order).

Per ulteriori informazioni sul funzionamento dei checksum con gli oggetti di caricamento multipart, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Operazioni simultanee di caricamento in più parti

In un ambiente di sviluppo distribuito, l'applicazione può avviare diversi aggiornamenti sullo stesso oggetto nello stesso momento. Ad esempio, l'applicazione potrebbe avviare diversi caricamenti multipart utilizzando la stessa chiave oggetto. Per ciascuno di questi caricamenti, l'applicazione può quindi caricare le parti e inviare una richiesta di completamento del caricamento ad Amazon S3 per creare l'oggetto. Per S3 Express One Zone, l'ora di creazione dell'oggetto è la data di completamento del caricamento in più parti.

 Important

Il controllo delle versioni non è supportato per gli oggetti memorizzati nei bucket della directory.

Caricamenti multiparte e prezzi

Una volta avviato un caricamento in più parti, Amazon S3 mantiene tutte le parti finché il caricamento non viene completato o interrotto. Per tutta la durata del processo, all'utente vengono fatturati i costi per lo storage, la larghezza di banda e le richieste per questo tipo di caricamento e per le parti associate. Se si interrompe il caricamento multiparte, Amazon S3 elimina gli artefatti di caricamento e tutte le parti caricate e non vengono più addebitate. Non sono previsti costi di cancellazione anticipata per l'eliminazione di caricamenti multiparte incompleti, indipendentemente dalla classe di storage specificata. Per ulteriori informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Important

Se la richiesta completa di caricamento multiparte non viene inviata con successo, le parti dell'oggetto non vengono assemblate e non viene creato un oggetto. Ti viene addebitato tutto lo spazio di storage associato alle parti caricate. È importante completare il caricamento multiparte per creare l'oggetto o interrompere il caricamento multiparte per rimuovere le parti caricate.

Prima di eliminare un bucket di directory, è necessario completare o interrompere tutti i caricamenti multiparte in corso. I bucket di directory non supportano le configurazioni di S3 Lifecycle. Se necessario, è possibile elencare i caricamenti multiparte attivi, quindi interrompere i caricamenti e cancellare il bucket.

Operazioni e autorizzazioni dell'API per il caricamento multiparte

Per consentire l'accesso alle operazioni API di gestione degli oggetti su un bucket di directory, si concede l'autorizzazione `s3express:CreateSession` in una policy di bucket o in una policy basata sull'identità AWS Identity and Access Management (IAM).

Per eseguire le operazioni di caricamento in più parti, devi disporre delle autorizzazioni necessarie. È possibile utilizzare le policy dei bucket o le policy basate sull'identità IAM per concedere ai principali IAM le autorizzazioni per eseguire le operazioni. Nella tabella riportata di seguito sono elencate le autorizzazioni richieste per le varie operazioni di caricamento in più parti.

È possibile identificare l'iniziatore di un caricamento multiparte tramite l'elemento `Initiator`. Se l'iniziatore è un Account AWS, questo elemento fornisce le stesse informazioni dell'elemento `Owner`. Se è un utente IAM, questo elemento fornisce l'ARN e il nome visualizzato dell'utente.

Azione	Autorizzazioni richieste
Creazione di un caricamento in più parti	Per creare il caricamento multiparte, è necessario essere autorizzati a eseguire l'azione <code>s3express:CreateSession</code> sul bucket della directory.
Avvio di un caricamento multiparte	Per avviare il caricamento multiparte, è necessario essere autorizzati a eseguire l'azione <code>s3express:CreateSession</code> sul bucket della directory.
Caricamento di una parte	<p>Per caricare una parte, è necessario essere autorizzati a eseguire l'azione <code>s3express:CreateSession</code> sul bucket della directory.</p> <p>Affinché l'iniziatore possa caricare una parte, il proprietario del bucket deve consentire all'iniziatore di eseguire l'azione <code>s3express:CreateSession</code> sul bucket della directory.</p>
Caricamento di una parte (copia)	<p>Per caricare una parte, è necessario essere autorizzati a eseguire l'azione <code>s3express:CreateSession</code> sul bucket della directory.</p> <p>Perché l'iniziatore possa caricare una parte di un oggetto, il proprietario del bucket deve consentire all'iniziatore di eseguire l'operazione <code>s3express:CreateSession</code> sull'oggetto.</p>
Completamento del caricamento in più parti	<p>Per completare un caricamento multiparte, è necessario essere autorizzati a eseguire l'azione <code>s3express:CreateSession</code> sul bucket della directory.</p> <p>Affinché l'iniziatore completi un caricamento multiparte, il proprietario del bucket deve consentire all'iniziatore di eseguire l'azione <code>s3express:CreateSession</code> sull'oggetto.</p>
Interrompere un caricamento in più parti	<p>Per interrompere un caricamento multiparte, è necessario essere autorizzati a eseguire l'azione <code>s3express:CreateSession</code>.</p> <p>Affinché l'iniziatore possa interrompere un caricamento multiparte, è necessario che gli venga concesso l'accesso esplicito per eseguire l'azione <code>s3express:CreateSession</code>.</p>

Azione	Autorizzazioni richieste
Elenco di parti	Per elencare le parti in un caricamento multiparte, è necessario essere autorizzati a eseguire l'azione <code>s3express:CreateSession</code> sul bucket della directory.
Elenco di carichi in più parti in corso	Per elencare i carichi multiparte in corso su un bucket, è necessario essere autorizzati a eseguire l'azione <code>s3:ListBucketMultipartUploads</code> su quel bucket.

Supporto delle operazioni API per il caricamento multiparte

Le seguenti sezioni della Riferimento API di Amazon Simple Storage Service descrivono il funzionamento della REST API di Amazon S3 per il caricamento multiparte.

- [CreateMultipartUpload](#)
- [UploadPart](#)
- [UploadPartCopy](#)
- [CompleteMultipartUpload](#)
- [AbortMultipartUpload](#)
- [ListParts](#)
- [ListMultipartUploads](#)

Esempi

Per utilizzare un caricamento multiparte per caricare un oggetto su S3 Express One Zone in un bucket di directory, consulta gli esempi seguenti.

Argomenti

- [Creazione di un caricamento in più parti](#)
- [Caricamento delle parti di un caricamento multiparte](#)
- [Completamento di un caricamento in più parti](#)
- [Interruzione di un caricamento in più parti](#)
- [Creazione di un'operazione di copia di caricamento in più parti](#)

- [Elenco dei caricamenti multiparte in corso](#)
- [Elenco di parti di un caricamento multiparte](#)

Creazione di un caricamento in più parti

Note

Per i bucket di directory, quando si esegue un'operazione `CreateMultipartUpload` e un'operazione `UploadPartCopy`, la crittografia predefinita del bucket deve utilizzare la configurazione di crittografia desiderata e le intestazioni di richiesta fornite nella richiesta `CreateMultipartUpload` devono corrispondere alla configurazione di crittografia predefinita del bucket di destinazione.

Gli esempi seguenti mostrano come creare un caricamento multiparte.

Utilizzo di AWS SDK

SDK for Java 2.x

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 * that is used to track
 * all the upload parts
 *
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--use1-az4--x-s3'
 * @param key
 * @return
 */
private static String createMultipartUpload(S3Client s3, String bucketName, String
key) {

    CreateMultipartUploadRequest createMultipartUploadRequest =
CreateMultipartUploadRequest.builder()
        .bucket(bucketName)
        .key(key)
        .build();
```

```
String uploadId = null;

try {
    CreateMultipartUploadResponse response =
s3.createMultipartUpload(createMultipartUploadRequest);
    uploadId = response.uploadId();
}
catch (S3Exception e) {
    System.err.println(e.awsErrorDetails().errorMessage());
    System.exit(1);
}
return uploadId;
```

SDK for Python

Example

```
def create_multipart_upload(s3_client, bucket_name, key_name):
    """
    Create a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: The destination bucket for the multipart upload
    :param key_name: The key name for the object to be uploaded
    :return: The UploadId for the multipart upload if created successfully, else None
    """

    try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None
```

Utilizzo di AWS CLI

Questo esempio mostra come creare un upload multiparte su un bucket di directory utilizzando il metodo AWS CLI. Questo comando avvia un caricamento in più parti nel bucket di directory *bucket-base-name* -- *zone-id* --x-s3 per l'oggetto. *KEY_NAME* Per utilizzare il comando, sostituisci il file con le tue informazioni *user input placeholders*.

```
aws s3api create-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --  
key KEY_NAME
```

Per ulteriori informazioni, consulta [create-multipart-upload](#) in AWS Command Line Interface.

Caricamento delle parti di un caricamento multiparte

Gli esempi seguenti mostrano come caricare parti di un caricamento multiparte.

Utilizzo di AWS SDK

SDK for Java 2.x

L'esempio seguente mostra come suddividere un singolo oggetto in parti e quindi caricare tali parti in un bucket di directory utilizzando l'SDK per Java 2.x.

Example

```
/**  
 * This method creates part requests and uploads individual parts to S3 and then  
 * returns all the completed parts  
 *  
 * @param s3  
 * @param bucketName  
 * @param key  
 * @param uploadId  
 * @throws IOException  
 */  
private static ListCompletedPartmultipartUpload(S3Client s3, String bucketName,  
String key, String uploadId, String filePath) throws IOException {  
  
    int partNumber = 1;  
    ListCompletedPart completedParts = new ArrayList<>();  
    ByteBuffer bb = ByteBuffer.allocate(1024 * 1024 * 5); // 5 MB byte buffer  
  
    // read the local file, breakdown into chunks and process  
    try (RandomAccessFile file = new RandomAccessFile(filePath, "r")) {  
        long fileSize = file.length();  
        int position = 0;  
        while (position < fileSize) {  
            file.seek(position);  
            int read = file.getChannel().read(bb);
```

```

        bb.flip(); // Swap position and limit before reading from the
buffer.

        UploadPartRequest uploadPartRequest = UploadPartRequest.builder()
            .bucket(bucketName)
            .key(key)
            .uploadId(uploadId)
            .partNumber(partNumber)
            .build();

        UploadPartResponse partResponse = s3.uploadPart(
            uploadPartRequest,
            RequestBody.fromByteBuffer(bb));

        CompletedPart part = CompletedPart.builder()
            .partNumber(partNumber)
            .eTag(partResponse.eTag())
            .build();
        completedParts.add(part);

        bb.clear();
        position += read;
        partNumber++;
    }
}

catch (IOException e) {
    throw e;
}

return completedParts;
}

```

SDK for Python

L'esempio seguente mostra come suddividere un singolo oggetto in parti e quindi caricare tali parti in un bucket di directory utilizzando l'SDK per Python.

Example

```

def multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_size):
    """
    Break up a file into multiple parts and upload those parts to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload

```



```

:param key_name: Key name for object to be uploaded and for the local file
that's being uploaded
:param mpu_id: The UploadId returned from the create_multipart_upload call
:param part_size: The size parts that the object will be broken into, in bytes.
                  Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
last part of your multipart upload.
:return: part_list for the multipart upload if all parts are uploaded
successfully, else None
'''

part_list = []
try:
    with open(key_name, 'rb') as file:
        part_counter = 1
        while True:
            file_part = file.read(part_size)
            if not len(file_part):
                break
            upload_part = s3_client.upload_part(
                Bucket = bucket_name,
                Key = key_name,
                UploadId = mpu_id,
                Body = file_part,
                PartNumber = part_counter
            )
            part_list.append({'PartNumber': part_counter, 'ETag':
upload_part['ETag']})
            part_counter += 1
except ClientError as e:
    logging.error(e)
    return None
return part_list

```

Utilizzo di AWS CLI

Questo esempio mostra come suddividere un singolo oggetto in parti e quindi caricare tali parti in un bucket di directory, utilizzando il metodo AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```

aws s3api upload-part --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --part-number 1 --body LOCAL_FILE_NAME --upload-id
"AS_mgt9RaQE9GEaifATue15dAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAAAA0AAAAAAAAAAH2AfYAA

```

Per ulteriori informazioni, consulta [upload-part](#) in AWS Command Line Interface.

Completamento di un caricamento in più parti

Gli esempi seguenti mostrano come completare un caricamento multiparte.

Utilizzo di AWS SDK

SDK for Java 2.x

Gli esempi che seguono mostrano come completare un caricamento multiparte utilizzando l'SDK per Java 2.x.

Example

```
/**
 * This method completes the multipart upload request by collating all the upload
 * parts
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--usw2-az1--x-s3'
 * @param key
 * @param uploadId
 * @param uploadParts
 */
private static void completeMultipartUpload(S3Client s3, String bucketName, String
key, String uploadId, List<CompletedPart> uploadParts) {
    CompletedMultipartUpload completedMultipartUpload =
CompletedMultipartUpload.builder()
        .parts(uploadParts)
        .build();

    CompleteMultipartUploadRequest completeMultipartUploadRequest =
        CompleteMultipartUploadRequest.builder()
            .bucket(bucketName)
            .key(key)
            .uploadId(uploadId)
            .multipartUpload(completedMultipartUpload)
            .build();

    s3.completeMultipartUpload(completeMultipartUploadRequest);
}

public static void multipartUploadTest(S3Client s3, String bucketName, String
key, String localFilePath) {
```

```

        System.out.println("Starting multipart upload for: " + key);
        try {
            String uploadId = createMultipartUpload(s3, bucketName, key);
            System.out.println(uploadId);
            ListCompletedPart parts = multipartUpload(s3, bucketName, key, uploadId,
localFilePath);
            completeMultipartUpload(s3, bucketName, key, uploadId, parts);
            System.out.println("Multipart upload completed for: " + key);
        }

        catch (Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}

```

SDK for Python

Gli esempi che seguono mostrano come completare un caricamento multiparte utilizzando l'SDK per Python.

Example

```

def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    """
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: The destination bucket for the multipart upload
    :param key_name: The key name for the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: The list of uploaded part numbers with their associated ETags
    :return: True if the multipart upload was completed successfully, else False
    """

    try:
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
    
```

```

except ClientError as e:
    logging.error(e)
    return False
return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'OBJECT_NAME'
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, bucket_name, key_name)
    if mpu_id is not None:
        part_list = multipart_upload(s3_client, bucket_name, key_name, mpu_id,
part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id,
part_list):
                print (f'{key_name} successfully uploaded through a ultipart upload
to {bucket_name}')
            else:
                print (f'Could not upload {key_name} hrough a multipart upload to
{bucket_name}')

```

Utilizzo di AWS CLI

Questo esempio mostra come completare un caricamento multiparte per un bucket di directory utilizzando il comando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```

aws s3api complete-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
"AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAAAEAAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAAAA0AAAAAAAAAAAH2AfYAA
--multipart-upload file://parts.json

```

Questo esempio prende una struttura JSON che descrive le parti del caricamento multiparte che devono essere riassemblate nel file completo. In questo esempio, il prefisso `file://` è usato per caricare la struttura JSON da un file nella cartella locale chiamato `parts`.

parts.json:

```
parts.json
{
  "Parts": [
    {
      "ETag": "6b78c4a64dd641a58dac8d9258b88147",
      "PartNumber": 1
    }
  ]
}
```

Per ulteriori informazioni, consulta [complete-multipart-upload](#) in AWS Command Line Interface.

Interruzione di un caricamento in più parti

Gli esempi seguenti mostrano come interrompere un caricamento multiparte.

Utilizzo di AWS SDK

SDK for Java 2.x

L'esempio seguente mostra come interrompere un caricamento multiparte utilizzando l'SDK per Java 2.x.

Example

```
public static void abortMultiPartUploads( S3Client s3, String bucketName ) {

    try {
        ListMultipartUploadsRequest listMultipartUploadsRequest =
            ListMultipartUploadsRequest.builder()
                .bucket(bucketName)
                .build();

        ListMultipartUploadsResponse response =
            s3.listMultipartUploads(listMultipartUploadsRequest);
        ListMultipartUpload uploads = response.uploads();

        AbortMultipartUploadRequest abortMultipartUploadRequest;
        for (MultipartUpload upload: uploads) {
            abortMultipartUploadRequest = AbortMultipartUploadRequest.builder()
                .bucket(bucketName)
                .key(upload.key())
                .uploadId(upload.uploadId())
```

```

        .build();

        s3.abortMultipartUpload(abortMultipartUploadRequest);
    }

}

catch (S3Exception e) {
    System.err.println(e.getMessage());
    System.exit(1);
}
}

```

SDK for Python

L'esempio seguente mostra come interrompere un caricamento multiparte utilizzando l'SDK per Python.

Example

```

import logging
import boto3
from botocore.exceptions import ClientError

def abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
    """
    Aborts a partial multipart upload in a directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket where the multipart upload was initiated - for
    example, 'doc-example-bucket--usw2-az1--x-s3'
    :param key_name: Name of the object for which the multipart upload needs to be
    aborted
    :param upload_id: Multipart upload ID for the multipart upload to be aborted
    :return: True if the multipart upload was successfully aborted, False if not
    """
    try:
        s3_client.abort_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = upload_id
        )
    except ClientError as e:

```

```

        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
    upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    if abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
        print (f'Multipart upload for object {key_name} in {bucket_name} bucket has
been aborted')
    else:
        print (f'Unable to abort multipart upload for object {key_name} in
{bucket_name} bucket')

```

Utilizzo di AWS CLI

L'esempio seguente mostra come interrompere un caricamento multipart utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```

aws s3api abort-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
"AS_mgt9RaQE9GEaifATue15dAAAAAAAAAEMAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAA0AAAAAAAAAH2AfYAA
MAQAAAAB00xUFeA7LTbWWFS8WYwhrxDxTIDN-pdEEq_agIHqsbg"

```

Per ulteriori informazioni, consulta [abort-multipart-upload](#) in AWS Command Line Interface.

Creazione di un'operazione di copia di caricamento in più parti

Note

- Per crittografare le copie di nuove parti dell'oggetto in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita [dal cliente](#)). [Chiave gestita da AWS](#) (aws/s3) non è supportato. La SSE-KMS configurazione può supportare solo 1 chiave gestita [dal cliente per bucket di directory](#) per tutta la durata del bucket. Dopo aver specificato una chiave gestita dal cliente per SSE-KMS, non puoi

sovrascrivere la chiave gestita dal cliente per la configurazione del bucket. SSE-KMS Non è possibile specificare le impostazioni di crittografia sul lato server per le nuove copie delle parti dell'oggetto SSE-KMS nelle intestazioni della richiesta. [UploadPartCopy](#) Inoltre, le intestazioni della richiesta fornite nella richiesta `CreateMultipartUpload` devono corrispondere alla configurazione di crittografia predefinita del bucket di destinazione.

- Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket generici o tra bucket di directory, tramite. [UploadPartCopy](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia per un oggetto. KMS-encrypted

Gli esempi seguenti mostrano come copiare gli oggetti da un bucket a un altro utilizzando un caricamento multiparte.

Utilizzo di AWS SDK

SDK for Java 2.x

L'esempio seguente mostra come utilizzare un caricamento multiparte per copiare programmaticamente un oggetto da un bucket all'altro, utilizzando l'SDK per Java 2.x.

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 * that is used to track
 * all the upload parts.
 *
 * @param s3
 * @param bucketName
 * @param key
 * @return
 */
private static String createMultipartUpload(S3Client s3, String bucketName, String
key) {
    CreateMultipartUploadRequest createMultipartUploadRequest =
CreateMultipartUploadRequest.builder()
        .bucket(bucketName)
        .key(key)
        .build();
```



```
String uploadId = null;
try {
    CreateMultipartUploadResponse response =
s3.createMultipartUpload(createMultipartUploadRequest);
    uploadId = response.uploadId();
} catch (S3Exception e) {
    System.err.println(e.awsErrorDetails().errorMessage());
    System.exit(1);
}
return uploadId;
}

/**
 * Creates copy parts based on source object size and copies over individual parts
 *
 * @param s3
 * @param sourceBucket
 * @param sourceKey
 * @param destnBucket
 * @param destnKey
 * @param uploadId
 * @return
 * @throws IOException
 */
public static List<CompletedPart> multipartUploadCopy(S3Client s3, String
sourceBucket, String sourceKey, String destnBucket, String destnKey, String
uploadId) throws IOException {

    // Get the object size to track the end of the copy operation.
    HeadObjectRequest headObjectRequest = HeadObjectRequest
        .builder()
        .bucket(sourceBucket)
        .key(sourceKey)
        .build();
    HeadObjectResponse response = s3.headObject(headObjectRequest);
    Long objectSize = response.contentLength();

    System.out.println("Source Object size: " + objectSize);

    // Copy the object using 20 MB parts.
    long partSize = 20 * 1024 * 1024;
    long bytePosition = 0;
    int partNum = 1;
    List<CompletedPart> completedParts = new ArrayList<>();
```

```
while (bytePosition < objectSize) {
    // The last part might be smaller than partSize, so check to make sure
    // that lastByte isn't beyond the end of the object.
    long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

    System.out.println("part no: " + partNum + ", bytePosition: " +
bytePosition + ", lastByte: " + lastByte);

    // Copy this part.
    UploadPartCopyRequest req = UploadPartCopyRequest.builder()
        .uploadId(uploadId)
        .sourceBucket(sourceBucket)
        .sourceKey(sourceKey)
        .destinationBucket(destnBucket)
        .destinationKey(destnKey)
        .copySourceRange("bytes="+bytePosition+"-"+lastByte)
        .partNumber(partNum)
        .build();
    UploadPartCopyResponse res = s3.uploadPartCopy(req);
    CompletedPart part = CompletedPart.builder()
        .partNumber(partNum)
        .eTag(res.copyPartResult().eTag())
        .build();
    completedParts.add(part);
    partNum++;
    bytePosition += partSize;
}
return completedParts;
}

public static void multipartCopyUploadTest(S3Client s3, String srcBucket, String
srcKey, String destnBucket, String destnKey) {
    System.out.println("Starting multipart copy for: " + srcKey);
    try {
        String uploadId = createMultipartUpload(s3, destnBucket, destnKey);
        System.out.println(uploadId);
        List parts = multipartUploadCopy(s3, srcBucket,
srcKey, destnBucket, destnKey, uploadId);
        completeMultipartUpload(s3, destnBucket, destnKey, uploadId, parts);
        System.out.println("Multipart copy completed for: " + srcKey);
    } catch (Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

```
}  
}
```

SDK for Python

L'esempio seguente mostra come utilizzare un caricamento multiparte per copiare programmaticamente un oggetto da un bucket a un altro, utilizzando l'SDK per Python.

Example

```
import logging  
import boto3  
from botocore.exceptions import ClientError  
  
def head_object(s3_client, bucket_name, key_name):  
    """  
    Returns metadata for an object in a directory bucket  
  
    :param s3_client: boto3 S3 client  
    :param bucket_name: Bucket that contains the object to query for metadata  
    :param key_name: Key name to query for metadata  
    :return: Metadata for the specified object if successful, else None  
    """  
  
    try:  
        response = s3_client.head_object(  
            Bucket = bucket_name,  
            Key = key_name  
        )  
        return response  
    except ClientError as e:  
        logging.error(e)  
        return None  
  
def create_multipart_upload(s3_client, bucket_name, key_name):  
    """  
    Create a multipart upload to a directory bucket  
  
    :param s3_client: boto3 S3 client  
    :param bucket_name: Destination bucket for the multipart upload  
    :param key_name: Key name of the object to be uploaded  
    :return: UploadId for the multipart upload if created successfully, else None  
    """
```

```

    try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None

```

```

def multipart_copy_upload(s3_client, source_bucket_name, key_name,
target_bucket_name, mpu_id, part_size):
    '''

```

Copy an object in a directory bucket to another bucket in multiple parts of a specified size

```

:param s3_client: boto3 S3 client
:param source_bucket_name: Bucket where the source object exists
:param key_name: Key name of the object to be copied
:param target_bucket_name: Destination bucket for copied object
:param mpu_id: The UploadId returned from the create_multipart_upload call
:param part_size: The size parts that the object will be broken into, in bytes.
                    Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
last part of your multipart upload.
:return: part_list for the multipart copy if all parts are copied successfully,
else None
'''

```

```

part_list = []
copy_source = {
    'Bucket': source_bucket_name,
    'Key': key_name
}
try:
    part_counter = 1
    object_size = head_object(s3_client, source_bucket_name, key_name)
    if object_size is not None:
        object_size = object_size['ContentLength']
        while (part_counter - 1) * part_size < object_size:
            bytes_start = (part_counter - 1) * part_size
            bytes_end = (part_counter * part_size) - 1
            upload_copy_part = s3_client.upload_part_copy (
                Bucket = target_bucket_name,
                CopySource = copy_source,
                CopySourceRange = f'bytes={bytes_start}-{bytes_end}',
                Key = key_name,

```

```

        PartNumber = part_counter,
        UploadId = mpu_id
    )
    part_list.append({'PartNumber': part_counter, 'ETag':
upload_copy_part['CopyPartResult']['ETag']})
    part_counter += 1
except ClientError as e:
    logging.error(e)
    return None
return part_list

def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    """
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: List of uploaded part numbers with associated ETags
    :return: True if the multipart upload was completed successfully, else False
    """

    try:
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    source_bucket_name = 'SOURCE_BUCKET_NAME'
    target_bucket_name = 'TARGET_BUCKET_NAME'
    key_name = 'KEY_NAME'
    part_size = 10 * MB

```

```
s3_client = boto3.client('s3', region_name = region)
mpu_id = create_multipart_upload(s3_client, target_bucket_name, key_name)
if mpu_id is not None:
    part_list = multipart_copy_upload(s3_client, source_bucket_name, key_name,
target_bucket_name, mpu_id, part_size)
    if part_list is not None:
        if complete_multipart_upload(s3_client, target_bucket_name, key_name,
mpu_id, part_list):
            print (f'{key_name} successfully copied through multipart copy from
{source_bucket_name} to {target_bucket_name}')
        else:
            print (f'Could not copy {key_name} through multipart copy from
{source_bucket_name} to {target_bucket_name}')
```

Utilizzo di AWS CLI

L'esempio seguente mostra come utilizzare un caricamento multiparte per copiare programmaticamente un oggetto da un bucket a un bucket della directory, utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3api upload-part-copy --bucket bucket-base-name--zone-id--x-s3 --
key TARGET_KEY_NAME --copy-source SOURCE_BUCKET_NAME/SOURCE_KEY_NAME --part-number 1 --
upload-id
"AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAAAA0AAAAAAAAAAAH2AfYAA"
```

Per ulteriori informazioni, consulta [upload-part-copy](#) in AWS Command Line Interface.

Elenco dei caricamenti multiparte in corso

Per elencare i caricamenti multiparte in corso in un bucket di directory, puoi utilizzare gli AWS SDK o il. AWS CLI

Utilizzo di AWS SDK

SDK for Java 2.x

Gli esempi seguenti mostrano come elencare i caricamenti multiparte in corso (incompleti) utilizzando l'SDK per Java 2.x.

Example

```
public static void listMultiPartUploads( S3Client s3, String bucketName) {
```

```

    try {
        ListMultipartUploadsRequest listMultipartUploadsRequest =
ListMultipartUploadsRequest.builder()
            .bucket(bucketName)
            .build();

        ListMultipartUploadsResponse response =
s3.listMultipartUploads(listMultipartUploadsRequest);
        List MultipartUpload uploads = response.uploads();
        for (MultipartUpload upload: uploads) {
            System.out.println("Upload in progress: Key = \"" + upload.key() +
"\", id = " + upload.uploadId());
        }
    }
    catch (S3Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

SDK for Python

Gli esempi seguenti mostrano come elencare i caricamenti multiparte in corso (incompleti) utilizzando l'SDK per Python.

Example

```

import logging
import boto3
from botocore.exceptions import ClientError

def list_multipart_uploads(s3_client, bucket_name):
    """
    List any incomplete multipart uploads in a directory bucket in e specified gion

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to check for incomplete multipart uploads
    :return: List of incomplete multipart uploads if there are any, None if not
    """

    try:
        response = s3_client.list_multipart_uploads(Bucket = bucket_name)
        if 'Uploads' in response.keys():

```

```

        return response['Uploads']
    else:
        return None
except ClientError as e:
    logging.error(e)

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
    multipart_uploads = list_multipart_uploads(s3_client, bucket_name)
    if multipart_uploads is not None:
        print (f'There are {len(multipart_uploads)} ncomplete multipart uploads for
{bucket_name}')
    else:
        print (f'There are no incomplete multipart uploads for {bucket_name}')

```

Utilizzo di AWS CLI

Gli esempi seguenti mostrano come elencare i caricamenti multiparte in corso (incompleti) utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file con le tue informazioni *user input placeholders*.

```
aws s3api list-multipart-uploads --bucket bucket-base-name--zone-id--x-s3
```

Per ulteriori informazioni, consulta [list-multiparte-uploads](#) in AWS Command Line Interface.

Elenco di parti di un caricamento multiparte

Gli esempi seguenti mostrano come elencare le parti di un caricamento multiparte in un bucket di directory.

Utilizzo di AWS SDK

SDK for Java 2.x

Gli esempi seguenti mostrano come elencare le parti di un caricamento multipartito in un bucket di directory utilizzando l'SDK per Java 2.x.

```
public static void listMultiPartUploadsParts( S3Client s3, String bucketName, String
objKey, String uploadID) {
```



```

    try {
        ListPartsRequest listPartsRequest = ListPartsRequest.builder()
            .bucket(bucketName)
            .uploadId(uploadID)
            .key(objKey)
            .build();

        ListPartsResponse response = s3.listParts(listPartsRequest);
        ListPart parts = response.parts();
        for (Part part: parts) {
            System.out.println("Upload in progress: Part number = \"\" +
part.partNumber() + "\", etag = \"\" + part.eTag());
        }

    }

    catch (S3Exception e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }

}

```

SDK for Python

Gli esempi seguenti mostrano come elencare le parti di un caricamento multipartito in un bucket di directory utilizzando SDK per Python.

```

import logging
import boto3
from botocore.exceptions import ClientError

def list_parts(s3_client, bucket_name, key_name, upload_id):
    """
    Lists the parts that have been uploaded for a specific multipart upload to a
    directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that multipart uploads parts have been uploaded to
    :param key_name: Name of the object that has parts uploaded
    :param upload_id: Multipart upload ID that the parts are associated with
    """

```

```

    :return: List of parts associated with the specified multipart upload, None if
    there are no parts
    '''
    parts_list = []
    next_part_marker = ''
    continuation_flag = True
    try:
        while continuation_flag:
            if next_part_marker == '':
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id
                )
            else:
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id,
                    NextPartMarker = next_part_marker
                )
            if 'Parts' in response:
                for part in response['Parts']:
                    parts_list.append(part)
                if response['IsTruncated']:
                    next_part_marker = response['NextPartNumberMarker']
            else:
                continuation_flag = False
        else:
            continuation_flag = False
    return parts_list
except ClientError as e:
    logging.error(e)
    return None

if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
    upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    parts_list = list_parts(s3_client, bucket_name, key_name, upload_id)
    if parts_list is not None:
        print (f'{key_name} has {len(parts_list)} parts uploaded to {bucket_name}')

```

```
else:
    print (f'There are no multipart uploads with that upload ID for
{bucket_name} bucket')
```

Utilizzo di AWS CLI

Gli esempi seguenti mostrano come elencare le parti di un caricamento multiparte in un bucket di directory utilizzando AWS CLI. Per utilizzare il comando, sostituisci il *user input placeholders* con le tue informazioni.

```
aws s3api list-parts --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME --upload-
id
"AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAAAA0AAAAAAAAAAH2AfYAA"
```

Per ulteriori informazioni, consulta [list-parts](#) in AWS Command Line Interface.

Copia di oggetti da o verso un bucket di directory

L'operazione copy crea una copia di un oggetto già archiviato in Amazon S3. Puoi copiare oggetti tra bucket di directory e bucket per uso generico. Inoltre, puoi copiare oggetti all'interno di un bucket e tra bucket dello stesso tipo, ad esempio, da un bucket di directory all'altro.

Note

La copia di oggetti tra diversi Regioni AWS non è supportata quando il bucket di origine o di destinazione si trova in una AWS zona locale. I bucket di origine e di destinazione devono avere lo stesso Regione AWS padre. I bucket di origine e di destinazione possono essere di tipo diverso (zona di disponibilità o zona locale).

È possibile creare una copia di un oggetto fino a 5 GB in una singola operazione atomica. Tuttavia, per copiare un oggetto di dimensioni superiori a 5 GB, è necessario utilizzare le operazioni API di caricamento multiparte. Per ulteriori informazioni, consulta [Utilizzo dei caricamenti multiparte con i bucket di directory](#).

Permissions

Per copiare oggetti, è necessario disporre delle seguenti autorizzazioni:

- Per copiare oggetti da un bucket di directory a un altro, è necessario disporre dell'autorizzazione `s3express:CreateSession`.
- Per copiare gli oggetti dai bucket di directory ai bucket per uso generico, è necessario disporre dell'autorizzazione `s3express:CreateSession` e dell'autorizzazione `s3:PutObject` per scrivere la copia dell'oggetto nel bucket di destinazione.
- Per copiare oggetti da bucket per uso generico a bucket di directory, è necessario disporre dei permessi `s3express:CreateSession` e `s3:GetObject` per leggere l'oggetto di origine che si sta copiando.

Per ulteriori informazioni, consulta [CopyObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Encryption (Crittografia)

Amazon S3 esegue automaticamente la crittografia di tutti i nuovi oggetti caricati in un bucket S3. La configurazione di crittografia predefinita di un bucket S3 è sempre abilitata ed è almeno impostata sulla crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3

Per i bucket di directory, è supportata SSE-S3 la crittografia lato server con AWS Key Management Service chiavi ().AWS KMS SSE-KMS Quando il bucket di destinazione è un bucket di directory, si consiglia di utilizzare la configurazione di crittografia desiderata come crittografia predefinita per il bucket di destinazione e di non sostituire la crittografia predefinita del bucket. I nuovi oggetti vengono quindi crittografati automaticamente con le impostazioni di crittografia desiderate. Inoltre, le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket per uso generico o tra bucket di directory, tramite. [CopyObject](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia per un oggetto. KMS-encrypted Per ulteriori informazioni sui comportamenti di crittografia che sovrascrivono nei bucket di directory, consulta [Specificare la crittografia lato server con per il caricamento di nuovi oggetti. AWS KMS](#)

Per i bucket generici, è possibile utilizzare SSE-S3 (impostazione predefinita) la crittografia lato server con () chiavi AWS Key Management Service (AWS KMS), la crittografia lato server a doppio livello con chiavi (SSE-KMS) o la crittografia lato server con AWS KMS chiavi fornite dal cliente (). DSSE-KMS SSE-C

Se si effettua una richiesta di copia che specifica l'uso DSSE-KMS o SSE-C per un bucket di directory (bucket di origine o di destinazione), la risposta restituisce un errore.

Tag

I bucket di directory non supportano i tag. Se si copia un oggetto con tag da un bucket per uso generico a un bucket di directory, si riceve una risposta HTTP 501 (Not Implemented). Per ulteriori informazioni, consulta [CopyObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

ETag

I tag entità (ETag) per S3 Express One Zone sono stringhe alfanumeriche casuali e non sono checksum MD5. Per garantire l'integrità degli oggetti, utilizza checksum aggiuntivi.

Checksum aggiuntivi

S3 Express One Zone offre la possibilità di scegliere l'algoritmo di checksum utilizzato per convalidare i dati durante il caricamento o il download. È possibile selezionare uno dei seguenti algoritmi di controllo dell'integrità dei dati Secure Hash Algorithms (SHA) o Cyclic Redundancy Check (CRC): CRC32, CRC32C e SHA-1 SHA-256 MD5-based i checksum non sono supportati con la classe di storage S3 Express One Zone.

Per ulteriori informazioni, consulta [Best practice per il checksum S3 aggiuntivo](#).

Funzionalità supportate

Per ulteriori informazioni sulle caratteristiche di Amazon S3 supportate da S3 Express One Zone, consulta [Differenze per i bucket di directory](#).

Utilizzo della console S3 (copia in un bucket di directory)

Note

Le restrizioni e le limitazioni quando si copia un oggetto in un bucket di directory con la console sono le seguenti:

- L'azione Copy si applica a tutti gli oggetti all'interno delle cartelle (prefissi) specificate. Gli oggetti aggiunti a queste cartelle mentre l'azione è in corso potrebbero essere interessati.
- Gli oggetti crittografati con chiavi di crittografia fornite dal cliente (SSE-C) non possono essere copiati utilizzando la console S3. Per copiare oggetti crittografati con SSE-C, utilizza l'AWS SDK o l'AWS CLI API REST di Amazon S3.
- Gli oggetti copiati non manterranno le impostazioni di Object Lock dagli oggetti originali.

- Se il bucket da cui si stanno copiando gli oggetti utilizza l'impostazione del proprietario del bucket per la proprietà degli oggetti S3, le ACL degli oggetti non verranno copiate nella destinazione specificata.
- Se desideri copiare oggetti in un bucket che utilizza l'impostazione imposta dal proprietario del bucket per S3 Object Ownership, assicurati che anche il bucket di origine utilizzi l'impostazione imposta dal proprietario del bucket o rimuovi qualsiasi oggetto che ACL concede ad altri account e gruppi. AWS
- Gli oggetti copiati da un bucket per uso generico a un bucket di directory non manterranno i tag degli oggetti, le ACL o i valori ETag. I valori di checksum possono essere copiati, ma non sono equivalenti a un ETag. Il valore del checksum può cambiare rispetto a quando è stato aggiunto.
- Tutti gli oggetti copiati in un bucket della directory saranno con il proprietario del bucket impostato per la proprietà degli oggetti S3.

Per copiare un oggetto da un bucket per uso generico o da un bucket di directory a un bucket di directory

1. Accedi e apri la console Amazon S3 all'indirizzo. Console di gestione AWS <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione di sinistra, specifica il tipo di bucket da cui copiare gli oggetti:
 - Per copiare da un bucket per uso generico, scegli la scheda Bucket per uso generico.
 - Per copiare da un bucket di directory, scegli la scheda Bucket di directory.
3. Scegli il bucket per uso generico o il bucket della directory che contiene gli oggetti da copiare.
4. Scegli la scheda Objects (Oggetti). Nella pagina Oggetti, seleziona la casella di controllo a sinistra dei nomi degli oggetti da copiare.
5. Nel menu Actions (Operazioni) scegliere Copy (Copia).

Viene visualizzata la pagina Copia.

6. In Destinazione, scegli Directory bucket per il tipo di destinazione. Per specificare il percorso di destinazione, scegli Sfoglia S3, navigare fino alla destinazione e scegli il pulsante di opzione a sinistra della destinazione. Scegliere Choose destination (Scegli destinazione).

In alternativa, immettere il percorso di destinazione.

7. In Impostazioni di copia aggiuntive, scegli se eseguire Copia impostazioni dell'origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni dell'origine, scegli Non specificare le impostazioni. Scegli Specifica impostazioni per specificare le impostazioni di crittografia lato server, checksum e metadati.
8. Scegli Copia. Amazon S3 copia gli oggetti nella destinazione.

Utilizzo della console S3 (copia in un bucket per uso generico)

Note

Le restrizioni e le limitazioni quando si copia un oggetto in un bucket per uso generico con la console sono le seguenti:

- L'azione Copy si applica a tutti gli oggetti all'interno delle cartelle (prefissi) specificate. Gli oggetti aggiunti a queste cartelle mentre l'azione è in corso potrebbero essere interessati.
- Gli oggetti crittografati con le chiavi di crittografia fornite dal cliente (SSE-C) non possono essere copiati utilizzando la console S3. Per copiare oggetti crittografati con SSE-C, utilizza l' AWS SDK o l' AWS CLI API REST di Amazon S3.
- Gli oggetti copiati non manterranno le impostazioni di Object Lock dagli oggetti originali.
- Se il bucket da cui si stanno copiando gli oggetti utilizza l'impostazione del proprietario del bucket per la proprietà degli oggetti S3, le ACL degli oggetti non verranno copiate nella destinazione specificata.
- Se desideri copiare oggetti in un bucket che utilizza l'impostazione imposta dal proprietario del bucket per S3 Object Ownership, assicurati che anche il bucket di origine utilizzi l'impostazione imposta dal proprietario del bucket o rimuovi qualsiasi oggetto che ACL concede ad altri account e gruppi. AWS

Per copiare un oggetto da un bucket di directory in un bucket per uso generico

1. Accedi e apri la console Amazon S3 all'indirizzo. Console di gestione AWS <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Scegli la scheda Bucket di directory.
4. Scegli il bucket della directory che contiene gli oggetti da copiare.

5. Scegli la scheda Objects (Oggetti). Nella pagina Oggetti, seleziona la casella di controllo a sinistra dei nomi degli oggetti da copiare.
6. Nel menu Actions (Operazioni) scegliere Copy (Copia).
7. Alla voce Destinazione, scegli il Bucket per uso generico per il tipo di destinazione. Per specificare il percorso di destinazione, scegli Sfoglia S3, naviga fino alla destinazione e scegli il pulsante di opzione a sinistra della destinazione. Scegliere Choose destination (Scegli destinazione).

In alternativa, immettere il percorso di destinazione.

8. In Impostazioni di copia aggiuntive, scegli se eseguire Copia impostazioni dell'origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni dell'origine, scegli Non specificare le impostazioni. Scegli Specifica le impostazioni per specificare le impostazioni per la classe di storage, le ACL, i tag degli oggetti, i metadati, la crittografia lato server e i checksum aggiuntivi.
9. Scegli Copia. Amazon S3 copia gli oggetti nella destinazione.

Utilizzo di AWS SDK

SDK for Java 2.x

Example

```
public static void copyBucketObject (S3Client s3, String sourceBucket, String
objectKey, String targetBucket) {
    CopyObjectRequest copyReq = CopyObjectRequest.builder()
        .sourceBucket(sourceBucket)
        .sourceKey(objectKey)
        .destinationBucket(targetBucket)
        .destinationKey(objectKey)
        .build();
    String temp = "";

    try {
        CopyObjectResponse copyRes = s3.copyObject(copyReq);
        System.out.println("Successfully copied " + objectKey + " from bucket " +
sourceBucket + " into bucket "+targetBucket);
    }
}
```



```
        catch (S3Exception e) {  
            System.err.println(e.awsErrorDetails().errorMessage());  
            System.exit(1);  
        }  
    }
```

Utilizzo di AWS CLI

Il seguente comando di `copy-object` esempio mostra come è possibile utilizzare il AWS CLI per copiare un oggetto da un bucket a un altro bucket. È possibile copiare gli oggetti tra i tipi di bucket. Per eseguire questo comando, sostituisci i segnaposto inseriti dall'utente con le tue informazioni.

```
aws s3api copy-object --copy-source SOURCE_BUCKET/SOURCE_KEY_NAME --key TARGET_KEY_NAME  
--bucket TARGET_BUCKET_NAME
```

Per ulteriori informazioni, consulta [copy-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Eliminazione di oggetti da un bucket di directory

Puoi eliminare oggetti da un bucket di directory Amazon S3 utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) o gli SDK. AWS Per ulteriori informazioni, consulta [Operazioni con i bucket di directory](#) e [S3 Express One Zone](#).

Warning

- L'eliminazione di un oggetto non può essere annullata.
- Questa azione elimina tutti gli oggetti specificati. Quando si eliminano le cartelle, attendere che l'azione di eliminazione finisca prima di aggiungere nuovi oggetti alla cartella. In caso contrario, potrebbero essere eliminati anche nuovi oggetti.

Note

Quando si eliminano programmaticamente più oggetti da un bucket della directory, si noti quanto segue:

- Le chiavi degli oggetti nelle richieste `DeleteObjects` devono contenere almeno un carattere diverso dallo spazio. Le stringhe con tutti i caratteri di spazio bianco non sono supportate.
- Le chiavi degli oggetti nelle richieste di `DeleteObjects` non possono contenere caratteri di controllo Unicode, ad eccezione di newline (`\n`), tab (`\t`) e carriage return (`\r`).

Utilizzo della console S3

Per eliminare oggetti

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Scegli il bucket della directory che contiene gli oggetti da eliminare.
4. Scegli la scheda Objects (Oggetti). Nell'elenco Oggetti, seleziona la casella di controllo a sinistra dell'oggetto o degli oggetti che si desidera eliminare.
5. Scegliere Elimina.
6. Nella pagina Elimina oggetti inserisci **permanently delete** nella casella di testo.
7. Scegliere Delete objects (Elimina oggetti).

Utilizzo di AWS SDK

SDK for Java 2.x

Example

L'esempio seguente elimina gli oggetti di un bucket di directory usando AWS SDK for Java 2.x.

```
static void deleteObject(S3Client s3Client, String bucketName, String objectKey) {  
  
    try {  
  
        DeleteObjectRequest del = DeleteObjectRequest.builder()  
            .bucket(bucketName)
```

```

        .key(objectKey)
        .build();

    s3Client.deleteObject(del);

    System.out.println("Object " + objectKey + " has been deleted");

} catch (S3Exception e) {
    System.err.println(e.awsErrorDetails().errorMessage());
    System.exit(1);
}

}

```

SDK for Python

Example

L'esempio seguente elimina gli oggetti di un bucket di directory usando AWS SDK per Python (Boto3).

```

import logging
import boto3
from botocore.exceptions import ClientError

def delete_objects(s3_client, bucket_name, objects):
    """
    Delete a list of objects in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains objects to be deleted; for example,
    'doc-example-bucket--usw2-az1--x-s3'
    :param objects: List of dictionaries that specify the key names to delete
    :return: Response output, else False
    """

    try:
        response = s3_client.delete_objects(
            Bucket = bucket_name,
            Delete = {
                'Objects': objects
            }

```

```
    )
    return response
except ClientError as e:
    logging.error(e)
    return False

if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    objects = [
        {
            'Key': '0.txt'
        },
        {
            'Key': '1.txt'
        },
        {
            'Key': '2.txt'
        },
        {
            'Key': '3.txt'
        },
        {
            'Key': '4.txt'
        }
    ]

    s3_client = boto3.client('s3', region_name = region)
    results = delete_objects(s3_client, bucket_name, objects)
    if results is not None:
        if 'Deleted' in results:
            print (f'Deleted {len(results["Deleted"])} objects from {bucket_name}')
        if 'Errors' in results:
            print (f'Failed to delete {len(results["Errors"])} objects from
{bucket_name}')
```

Utilizzo di AWS CLI

Il seguente esempio di comando `delete-object` mostra come si può usare il comando AWS CLI per eliminare un oggetto da un bucket della directory. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api delete-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

Per ulteriori informazioni, consulta [delete-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Il seguente esempio di comando `delete-objects` mostra come utilizzare la AWS CLI per eliminare un oggetto da un bucket di directory. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

Il file `delete.json` è il seguente:

```
{
  "Objects": [
    {
      "Key": "0.txt"
    },
    {
      "Key": "1.txt"
    },
    {
      "Key": "2.txt"
    },
    {
      "Key": "3.txt"
    }
  ]
}
```

Il comando di esempio `delete-objects` è il seguente:

```
aws s3api delete-objects --bucket bucket-base-name--zone-id--x-s3 --delete
file:///delete.json
```

Per ulteriori informazioni, consulta [delete-objects](#) nella documentazione di riferimento dei comandi della AWS CLI .

Download di un oggetto da un bucket di directory

I seguenti esempi di codice mostrano come leggere (scaricare) i dati da un oggetto in un bucket della directory Amazon S3 utilizzando l'operazione API `GetObject`.

Utilizzo di AWS SDK

SDK for Java 2.x

Example

Il seguente esempio di codice mostra come leggere i dati da un oggetto in un bucket di directory, usando AWS SDK for Java 2.x.

```
public static void getObject(S3Client s3Client, String bucketName, String objectKey)
{
    try {
        GetObjectRequest objectRequest = GetObjectRequest
            .builder()
            .key(objectKey)
            .bucket(bucketName)
            .build();

        ResponseBytes GetObjectResponse objectBytes =
s3Client.getObjectAsBytes(objectRequest);
        byte[] data = objectBytes.asByteArray();

        //Print object contents to console
        String s = new String(data, StandardCharsets.UTF_8);
        System.out.println(s);
    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

Il seguente esempio di codice mostra come leggere i dati da un oggetto in un bucket di directory, usando AWS SDK per Python (Boto3).

```
import boto3
from botocore.exceptions import ClientError
from botocore.response import StreamingBody

def get_object(s3_client: boto3.client, bucket_name: str, key_name: str) ->
    StreamingBody:
    """
    Gets the object.
    :param s3_client:
    :param bucket_name: The bucket that contains the object.
    :param key_name: The key of the object to be downloaded.
    :return: The object data in bytes.
    """
    try:
        response = s3_client.get_object(Bucket=bucket_name, Key=key_name)
        body = response['Body'].read()
        print(f"Got object '{key_name}' from bucket '{bucket_name}'.")
    except ClientError:
        print(f"Couldn't get object '{key_name}' from bucket '{bucket_name}'.")
        raise
    else:
        return body

def main():
    s3_client = boto3.client('s3')
    resp = get_object(s3_client, 'doc-example-bucket--use1-az4--x-s3', 'sample.txt')
    print(resp)

if __name__ == "__main__":
    main()
```

Utilizzo di AWS CLI

L'esempio `get-object` seguente mostra come utilizzare la AWS CLI per scaricare un oggetto da Amazon S3. Questo comando ottiene l'oggetto *KEY_NAME* dal bucket della directory *bucket-base-*

name --*zone-id*--x-s3. L'oggetto verrà scaricato in un file denominato *LOCAL_FILE_NAME*. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api get-object --bucket bucket-base-name--zone-id--x-s3 --  
key KEY_NAME LOCAL_FILE_NAME
```

Per ulteriori informazioni, consulta [get-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Generazione di URL prefirmati per condividere oggetti da bucket di directory

I seguenti esempi di codice mostrano come generare URL prefirmati per condividere oggetti da un bucket di directory Amazon S3.

Utilizzo di AWS CLI

Il seguente esempio di comando mostra come utilizzare la AWS CLI per generare un URL prefirmato per un oggetto su Amazon S3. Questo comando genera un URL prefirmato per un oggetto *KEY_NAME* dal bucket di directory *bucket-base-name--zone-id--x-s3*. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3 presign s3://bucket-base-name--zone-id--x-s3/KEY_NAME --expires-in 7200
```

Per ulteriori informazioni, consulta [presign](#) nella documentazione di riferimento dei comandi della AWS CLI .

Recupero dei metadati degli oggetti dai bucket della directory

I seguenti esempi di AWS SDK e AWS CLI mostrano come utilizzare l'operazione `HeadObject` and `GetObjectAttributes` API per recuperare i metadati da un oggetto in un bucket di directory Amazon S3 senza restituire l'oggetto stesso.

Utilizzo di AWS SDK

SDK for Java 2.x

Example


```
public static void headObject(S3Client s3Client, String bucketName, String
objectKey) {
    try {
        HeadObjectRequest headObjectRequest = HeadObjectRequest
            .builder()
            .bucket(bucketName)
            .key(objectKey)
            .build();
        HeadObjectResponse response = s3Client.headObject(headObjectRequest);
        System.out.format("Amazon S3 object: \"%s\" found in bucket: \"%s\" with
ETag: \"%s\"", objectKey, bucketName, response.eTag());
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
    }
}
```

Utilizzo di AWS CLI

Il seguente comando di `head-object` esempio mostra come è possibile utilizzare per recuperare i metadati da un oggetto. AWS CLI Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api head-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

Per ulteriori informazioni, consulta [head-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Il comando di `get-object-attributes` esempio seguente mostra come è possibile utilizzare il AWS CLI per recuperare i metadati da un oggetto. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api get-object-attributes --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
--object-attributes "StorageClass" "ETag" "ObjectSize"
```

Per ulteriori informazioni, consulta [get-object-attributes](#) nella documentazione di riferimento dei comandi della AWS CLI .

Elenco degli oggetti di un bucket di directory

I seguenti esempi di codice mostrano come elencare gli oggetti di un bucket di directory Amazon S3 utilizzando l'operazione API `ListObjectsV2`.

Utilizzo di AWS CLI

Il seguente esempio di comando `list-objects-v2` mostra come utilizzare la AWS CLI per elencare gli oggetti da Amazon S3. Questo comando elenca gli oggetti del bucket di directory `bucket-base-name--zone-id--x-s3`. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api list-objects-v2 --bucket bucket-base-name--zone-id--x-s3
```

Per ulteriori informazioni, consulta [list-objects-v2](#) nella documentazione di riferimento dei comandi della AWS CLI .

Sicurezza per i bucket di directory

La sicurezza del cloud AWS è la massima priorità. Come AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza. La sicurezza è una responsabilità condivisa tra voi. AWS Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura in esecuzione Servizi AWS in Cloud AWS. AWS ti fornisce anche servizi che puoi utilizzare in sicurezza. Third-party i revisori testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito del. [AWS Compliance Programs](#)

Per conoscere i programmi di conformità, consulta [Servizi AWS in Scope by Compliance Program](#).

- Sicurezza nel cloud: la tua responsabilità è determinata da Servizio AWS ciò che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione vi aiuterà a capire come applicare il modello di responsabilità condivisa quando si utilizzano i bucket di directory. I seguenti argomenti illustrano come configurare i bucket della directory per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che possono aiutarti a monitorare e proteggere i tuoi oggetti nei bucket di directory.

Protezione e crittografia dei dati

Per ulteriori informazioni su come configurare la crittografia per i bucket di directory, consulta i seguenti argomenti.

Argomenti

- [Server-side crittografia](#)
- [Impostazione e monitoraggio della crittografia predefinita per i bucket di directory](#)
- [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket di directory](#)
- [Crittografia dei dati in transito](#)
- [Eliminazione dei dati](#)

Server-side crittografia

La crittografia è configurata per impostazione predefinita per tutti i bucket di directory e tutti i nuovi oggetti caricati nei bucket di directory vengono crittografati automaticamente quando sono inattivi. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket di directory. Se desideri specificare un tipo di crittografia diverso, puoi utilizzare la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS), impostando la configurazione di crittografia predefinita del bucket. Per ulteriori informazioni sui bucket SSE-KMS in directory, vedere. [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket di directory](#)

Si consiglia di utilizzare la configurazione di crittografia predefinita del bucket e di non sovrascrivere la crittografia predefinita del bucket nelle richieste `CreateSession` o nelle richieste di oggetti `PUT`. I nuovi oggetti vengono quindi crittografati automaticamente con le impostazioni di crittografia desiderate. Per ulteriori informazioni sui comportamenti di crittografia che sovrascrivono nei bucket di directory, vedi [Specificare la crittografia lato server con per il caricamento di nuovi oggetti. AWS KMS](#)

SSE-KMS con bucket di directory si differenzia dai bucket generici per i seguenti SSE-KMS aspetti.

- La SSE-KMS configurazione può supportare solo 1 chiave gestita [dal cliente per bucket di directory](#) per tutta la durata del bucket. [Chiave gestita da AWS](#) (aws/s3) non è supportato. Inoltre, dopo aver specificato una chiave gestita dal cliente per SSE-KMS, non è possibile sovrascrivere la chiave gestita dal cliente per la configurazione del bucket. SSE-KMS

Puoi identificare la chiave gestita dal cliente che hai specificato per la SSE-KMS configurazione del bucket nel modo seguente:

- Si effettua una richiesta di operazione `API HeadObject` per trovare il valore di `x-amz-server-side-encryption-aws-kms-key-id` nella risposta.

Per utilizzare una nuova chiave gestita dal cliente per i propri dati, si consiglia di copiare gli oggetti esistenti in un nuovo bucket della directory con una nuova chiave gestita dal cliente.

- Per le operazioni API [sugli endpoint zionali \(a livello di oggetto\)](#), ad eccezione di [CopyObject](#) e [UploadPartCopy](#), si autenticano e autorizzano le richieste con una bassa latenza. [CreateSession](#) Si consiglia di utilizzare la configurazione di crittografia predefinita del bucket e di non sovrascrivere la crittografia predefinita del bucket nelle richieste `CreateSession` o nelle richieste di oggetti `PUT`. I nuovi oggetti vengono quindi crittografati automaticamente con le impostazioni di crittografia desiderate. Per crittografare i nuovi oggetti in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> Quindi, quando viene creata una sessione per le operazioni dell'API Zonal Endpoint, i nuovi oggetti vengono automaticamente crittografati e decrittografati con SSE-KMS le chiavi S3 Bucket durante la sessione. Per ulteriori informazioni sui comportamenti di crittografia che sovrascrivono nei bucket di directory, vedi [Specificare la crittografia lato server con per il caricamento di nuovi oggetti. AWS KMS](#)

Nelle chiamate API degli endpoint zionali (eccetto [CopyObject](#) e [UploadPartCopy](#)), non puoi sovrascrivere i valori delle impostazioni di crittografia (`x-amz-server-side-encryption`, e) della richiesta. `x-amz-server-side-encryption-aws-kms-key-id` `x-amz-server-side-encryption-context` `x-amz-server-side-encryption-bucket-key-enabled` `CreateSession` Non è necessario specificare esplicitamente i valori delle impostazioni di crittografia nelle chiamate API dell'endpoint di zona; Amazon S3 utilizzerà i valori delle impostazioni di crittografia dalla richiesta `CreateSession` per proteggere i nuovi oggetti nel bucket della directory.

Note

Quando utilizzi gli SDK AWS CLI o gli AWS SDK, `forCreateSession`, il token di sessione si aggiorna automaticamente per evitare interruzioni del servizio alla scadenza di una sessione. Gli AWS CLI o gli AWS SDK utilizzano la configurazione di crittografia predefinita del bucket per la richiesta. `CreateSession` Non è supportato l'annullamento dei valori delle impostazioni di crittografia nella richiesta `CreateSession`. Inoltre, nelle chiamate API degli endpoint zionali (eccetto [CopyObject](#) e [UploadPartCopy](#)), non è supportato sovrascrivere i valori delle impostazioni di crittografia della richiesta. `CreateSession`

- Per [CopyObject](#) crittografare le copie di nuovi oggetti in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> Quindi, quando si specificano le impostazioni di crittografia sul lato server per le copie di nuovi oggetti con SSE-KMS, è necessario assicurarsi che la chiave di crittografia sia la stessa chiave gestita dal cliente specificata per la configurazione di crittografia predefinita del bucket di directory. Per [UploadPartCopy](#) crittografare le copie di nuove parti di oggetti in un bucket di directory con SSE-KMS, devi specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> Non è possibile specificare le impostazioni di crittografia sul lato server per le nuove copie delle parti dell'oggetto nelle intestazioni della richiesta. SSE-KMS [UploadPartCopy](#) Inoltre, le impostazioni di crittografia fornite nella [CreateMultipartUpload](#) richiesta devono corrispondere alla configurazione di crittografia predefinita del bucket di destinazione.
- Le S3 Bucket Keys sono sempre abilitate per le operazioni GET e PUT in un bucket di directory e non possono essere disabilitate. Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket generici o tra bucket di directory, tramite [CopyObject](#) [UploadPartCopy](#), [l'Copyoperazione in Batch Operations o i job.](#) [import](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia di un oggetto. KMS-encrypted
- Quando si specifica una [chiave gestita dal cliente AWS KMS](#) per la crittografia nel bucket della directory, utilizzare solo l'ID chiave o l'ARN chiave. Il formato alias della chiave KMS non è supportato.

I bucket di directory non supportano la crittografia lato server a doppio livello con chiavi AWS Key Management Service (AWS KMS) () o la crittografia lato server con chiavi di crittografia fornite dal cliente (DSSE-KMS). SSE-C

Impostazione e monitoraggio della crittografia predefinita per i bucket di directory

La crittografia dei bucket Amazon S3 è abilitata per impostazione predefinita e i nuovi oggetti vengono crittografati automaticamente utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Questa crittografia si applica a tutti i nuovi oggetti nei bucket Amazon S3 e non comporta costi aggiuntivi.

Se hai bisogno di un maggiore controllo sulle tue chiavi di crittografia, ad esempio gestendo la rotazione delle chiavi e la concessione delle policy di accesso, puoi scegliere di utilizzare la crittografia lato server con () keys (). AWS Key Management Service AWS KMS SSE-KMS

Note

- Si consiglia di utilizzare la configurazione di crittografia predefinita del bucket e di non sovrascrivere la crittografia predefinita del bucket nelle richieste `CreateSession` o nelle richieste di oggetti `PUT`. I nuovi oggetti vengono quindi crittografati automaticamente con le impostazioni di crittografia desiderate. Per ulteriori informazioni sui comportamenti di crittografia che sovrascrivono nei bucket di directory, consulta [Specificare la crittografia lato server con per il caricamento di nuovi oggetti. AWS KMS](#)
- Per crittografare i nuovi oggetti in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). Quindi, quando viene creata una sessione per le operazioni dell'API Zonal Endpoint, i nuovi oggetti vengono automaticamente crittografati e decrittografati con SSE-KMS le chiavi S3 Bucket durante la sessione.
- Quando si imposta la crittografia dei bucket predefinita su SSE-KMS, le chiavi S3 Bucket sono sempre abilitate e le `PUT` operazioni si trovano in un bucket di directory `GET` e non possono essere disabilitate. Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket generici o tra bucket di directory [CopyObject](#), [UploadPartCopy](#) tramite l'operazione in Batch Operations o i job. [Copy import](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia di un oggetto. KMS-encrypted Per ulteriori informazioni su come S3 Bucket Keys riduce i costi delle AWS KMS richieste, consulta. [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#)
- Quando si specifica una [chiave gestita dal cliente AWS KMS](#) per la crittografia nel bucket della directory, utilizzare solo l'ID chiave o l'ARN chiave. Il formato alias della chiave KMS non è supportato.
- Dual-layer la crittografia lato server con AWS KMS chiavi (DSSE-KMS) e la crittografia lato server con chiavi fornite dal cliente (SSE-C) non sono supportate per la crittografia predefinita nei bucket di directory.

Per ulteriori informazioni sulla configurazione della crittografia predefinita, consulta [Configurazione della crittografia predefinita](#).

Per ulteriori informazioni sulle autorizzazioni richieste per la crittografia predefinita, consulta [PutBucketEncryption](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Puoi configurare la crittografia predefinita di Amazon S3 per un bucket S3 utilizzando la console Amazon S3, gli AWS SDK, l'API REST di Amazon S3 e (). AWS Command Line Interface AWS CLI

Utilizzo della console S3

Per configurare la crittografia predefinita per un bucket Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il nome del bucket desiderato.
4. Scegliere la scheda Properties (Proprietà).
5. Nelle impostazioni di Server-side crittografia, i bucket di directory utilizzano Server-side la crittografia con chiavi gestite da Amazon S3 (). SSE-S3
6. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Questi esempi mostrano come configurare la crittografia predefinita utilizzando SSE-S3 o utilizzando una chiave SSE-KMS bucket S3.

Per ulteriori informazioni sulla crittografia predefinita, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#). Per ulteriori informazioni sull'utilizzo di per configurare la AWS CLI crittografia predefinita, vedere [put-bucket-encryption](#).

Example— Crittografia predefinita con SSE-S3

In questo esempio viene configurata la crittografia predefinita dei bucket con le chiavi gestite da Amazon S3. Per utilizzare il comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-encryption-configuration '{
  "Rules": [
    {
      "ApplyServerSideEncryptionByDefault": {
        "SSEAlgorithm": "AES256"
      }
    }
  ]
}'
```

Example— Crittografia predefinita con SSE-KMS l'utilizzo di una chiave S3 Bucket

Questo esempio configura la crittografia bucket predefinita SSE-KMS utilizzando una chiave bucket S3. Per utilizzare il comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-encryption-configuration '{
  "Rules": [
    {
      "ApplyServerSideEncryptionByDefault": {
        "SSEAlgorithm": "aws:kms",
        "KMSEMasterKeyID": "KMS-Key-ARN"
      },
      "BucketKeyEnabled": true
    }
  ]
}'
```

Utilizzo della REST API

Utilizza l'`PutBucketEncryption` operazione REST API per impostare la crittografia predefinita con un tipo di crittografia lato server da utilizzare:, o. SSE-S3 SSE-KMS

Per ulteriori informazioni, consulta [PutBucketEncryption](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

Quando utilizzi AWS gli SDK, puoi richiedere ad Amazon S3 di AWS KMS keys utilizzarlo per la crittografia lato server. I seguenti esempi di AWS SDK per Java e .NET configurano la configurazione

di crittografia predefinita per un bucket di directory con SSE-KMS una chiave bucket S3. Per informazioni su altri SDK, consulta Codice e librerie [di](#) esempio nel Developer Center. AWS

Important

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetrica. Per ulteriori informazioni sulle chiavi, consulta [Chiavi KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Java

Con AWS SDK for Java 2.x, puoi richiedere ad Amazon S3 di utilizzare un AWS KMS key `applyServerSideEncryptionByDefault` metodo per specificare la configurazione di crittografia predefinita del tuo bucket di directory con cui crittografare i dati. SSE-KMS Si crea una chiave KMS di crittografia simmetrica e la si specifica nella richiesta.

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.PutBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.ServerSideEncryption;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionByDefault;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionConfiguration;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionRule;

public class Main {
    public static void main(String[] args) {
        S3Client s3 = S3Client.create();
        String bucketName = "bucket-base-name--zoneid--x-s3";
        String kmsKeyId = "your-kms-customer-managed-key-id";

        // AWS managed KMS keys aren't supported. Only customer-managed keys are
        // supported.
        ServerSideEncryptionByDefault serverSideEncryptionByDefault =
        ServerSideEncryptionByDefault.builder()
            .sseAlgorithm(ServerSideEncryption.AWS_KMS)
            .kmsMasterKeyId(kmsKeyId)
            .build();

        // The bucketKeyEnabled field is enforced to be true.
        ServerSideEncryptionRule rule = ServerSideEncryptionRule.builder()
```

```
        .bucketKeyEnabled(true)
        .applyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
        .build();

    ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
    ServerSideEncryptionConfiguration.builder()
        .rules(rule)
        .build();

    PutBucketEncryptionRequest putRequest = PutBucketEncryptionRequest.builder()
        .bucket(bucketName)

        .serverSideEncryptionConfiguration(serverSideEncryptionConfiguration)
        .build();

    s3.putBucketEncryption(putRequest);
    }
}
```

Per ulteriori informazioni sulla creazione di chiavi gestite dal cliente, consulta [Programming the AWS KMS API](#) nella AWS Key Management Service Developer Guide.

Per esempi di codice di utilizzo per il caricamento di un oggetto, consulta gli argomenti elencati di seguito. Per usare questi esempi dovrai aggiornare gli esempi di codice e fornire informazioni sulla crittografia come mostrato nel frammento di codice precedente.

- Per il caricamento di un oggetto in un'unica operazione, consulta [Caricamento di oggetti in un bucket di directory](#).
- Per le operazioni API di caricamento multiparte, consulta [Utilizzo dei caricamenti multiparte con i bucket di directory](#).

.NET

Con AWS SDK per .NET, puoi richiedere ad Amazon S3 di utilizzare un AWS KMS key utilizzando la `ServerSideEncryptionByDefault` proprietà per specificare la configurazione di crittografia predefinita del tuo bucket di directory con cui crittografare i dati. SSE-KMS Si crea una chiave di crittografia simmetrica gestita dal cliente e la si specifica nella richiesta.

```

    // Set the bucket server side encryption to use AWSKMS with a customer-managed
    key id.
    // bucketName: Name of the directory bucket. "bucket-base-name--zonsid--x-s3"
    // kmsKeyId: The Id of the customer managed KMS Key. "your-kms-customer-managed-
    key-id"
    // Returns True if successful.
    public static async Task<bool> SetBucketServerSideEncryption(string bucketName,
    string kmsKeyId)
    {
        var serverSideEncryptionByDefault = new ServerSideEncryptionConfiguration
        {
            ServerSideEncryptionRules = new List<ServerSideEncryptionRule>
            {
                new ServerSideEncryptionRule
                {
                    ServerSideEncryptionByDefault = new
    ServerSideEncryptionByDefault
                    {
                        ServerSideEncryptionAlgorithm =
    ServerSideEncryptionMethod.AWSKMS,
                        ServerSideEncryptionKeyManagementServiceKeyId = kmsKeyId
                    }
                }
            }
        };
        try
        {
            var encryptionResponse = await _s3Client.PutBucketEncryptionAsync(new
    PutBucketEncryptionRequest
            {
                BucketName = bucketName,
                ServerSideEncryptionConfiguration = serverSideEncryptionByDefault,
            });

            return encryptionResponse.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine(ex.ErrorCode == "AccessDenied"
                ? $"This account does not have permission to set encryption on
    {bucketName}, please try again."

```

```
        : $"Unable to set bucket encryption for bucket {bucketName},  
{ex.Message}");  
    }  
    return false;  
}
```

Per ulteriori informazioni sulla creazione di chiavi gestite dal cliente, consulta [Programming the AWS KMS API](#) nella AWS Key Management Service Developer Guide.

Per esempi di codice di utilizzo per il caricamento di un oggetto, consulta gli argomenti elencati di seguito. Per usare questi esempi dovrai aggiornare gli esempi di codice e fornire informazioni sulla crittografia come mostrato nel frammento di codice precedente.

- Per il caricamento di un oggetto in un'unica operazione, consulta [Caricamento di oggetti in un bucket di directory](#).
- Per le operazioni API di caricamento multiparte, consulta [Utilizzo dei caricamenti multiparte con i bucket di directory](#).

Monitoraggio della crittografia predefinita per i bucket di directory con AWS CloudTrail

È possibile tenere traccia delle richieste di configurazione della crittografia predefinita per i bucket di directory Amazon S3 utilizzando gli eventi AWS CloudTrail . I seguenti nomi di eventi API vengono utilizzati nei CloudTrail log:

- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

Note

- EventBridge non è supportato nei bucket di directory.
- Dual-layer la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (DSSE-KMS) o la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C) non sono supportate nei bucket di directory.

Per ulteriori informazioni sul monitoraggio della crittografia predefinita con AWS CloudTrail, consulta [Monitoraggio della crittografia predefinita con AWS CloudTrail e Amazon EventBridge](#).

Utilizzo della crittografia lato server con AWS KMS keys (SSE-KMS) nei bucket di directory

I controlli di sicurezza in ingresso AWS KMS possono aiutarti a soddisfare i requisiti di conformità relativi alla crittografia. Puoi scegliere di configurare i bucket di directory per utilizzare la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS) e utilizzare queste chiavi KMS per proteggere i tuoi dati nei bucket di directory Amazon S3. Per ulteriori informazioni su, consulta. SSE-KMS [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#)

Permissions

Per caricare o scaricare un oggetto crittografato con un indirizzo da o AWS KMS key verso Amazon S3, sono necessarie `kms:GenerateDataKey` le `kms:Decrypt` autorizzazioni necessarie sulla chiave. Per ulteriori informazioni, consulta l'argomento relativo all'[autorizzazione concessa agli utenti delle chiavi di utilizzare una chiave KMS per le operazioni di crittografia](#) nella Guida per gli sviluppatori di AWS Key Management Service . Per informazioni sulle AWS KMS autorizzazioni necessarie per i caricamenti in più parti, consulta. [Autorizzazioni e API per il caricamento in più parti](#)

Per ulteriori informazioni sulle chiavi KMS per, consulta. SSE-KMS [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#)

Argomenti

- [AWS KMS keys](#)
- [Utilizzo SSE-KMS per operazioni su più account](#)
- [Chiavi bucket Amazon S3](#)
- [Richiedendo SSE-KMS](#)
- [Contesto di crittografia](#)
- [Invio di richieste per AWS KMS oggetti crittografati](#)
- [Verifica della SSE-KMS crittografia nei bucket di directory](#)
- [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\) per il caricamento di nuovi oggetti nei bucket di directory](#)

AWS KMS keys

La tua SSE-KMS configurazione può supportare solo 1 chiave gestita [dal cliente](#) per bucket di directory per tutta la durata del bucket. [Chiave gestita da AWS](#) (aws/s3) non è supportato. Inoltre, dopo aver specificato una chiave gestita dal cliente per SSE-KMS, non è possibile sovrascrivere la chiave gestita dal cliente per la configurazione del bucket. SSE-KMS

Puoi identificare la chiave gestita dal cliente che hai specificato per la SSE-KMS configurazione del bucket nel modo seguente:

- Si effettua una richiesta di operazione API HeadObject per trovare il valore di x-amz-server-side-encryption-aws-kms-key-id nella risposta.

Per utilizzare una nuova chiave gestita dal cliente per i propri dati, si consiglia di copiare gli oggetti esistenti in un nuovo bucket della directory con una nuova chiave gestita dal cliente.

Quando si specifica una [chiave gestita dal cliente AWS KMS](#) per la crittografia nel bucket della directory, utilizzare solo l'ID chiave o l'ARN chiave. Il formato alias della chiave KMS non è supportato.

Per ulteriori informazioni sulle chiavi KMS per SSE-KMS, vedere [AWS KMS keys](#).

Utilizzo SSE-KMS per operazioni su più account

Quando si utilizza la crittografia per le operazioni tra account nei bucket della directory, tieni presente quanto segue:

- Se desideri garantire l'accesso multi-account agli oggetti S3, configura una policy di una chiave gestita dal cliente per consentire l'accesso da un altro account.
- Per specificare una chiave gestita dal cliente, è necessario utilizzare un ARN di chiave KMS completamente qualificato.

Chiavi bucket Amazon S3

Le S3 Bucket Keys sono sempre abilitate per le operazioni GET e PUT in un bucket di directory e non possono essere disabilitate. Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket generici o tra bucket di directory [CopyObject](#) [UploadPartCopy](#), tramite [l'Copyoperazione in Batch Operations o i job. import](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia di un oggetto. KMS-encrypted

Per le operazioni API [sugli endpoint zionali \(a livello di oggetto\)](#), eccetto [CopyObject](#) e [UploadPartCopy](#), si autenticano e autorizzano le richieste con una bassa latenza. [CreateSession](#) Si consiglia di utilizzare la configurazione di crittografia predefinita del bucket e di non sovrascrivere la crittografia predefinita del bucket nelle richieste `CreateSession` o nelle richieste di oggetti PUT. I nuovi oggetti vengono quindi crittografati automaticamente con le impostazioni di crittografia desiderate. Per crittografare i nuovi oggetti in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> Quindi, quando viene creata una sessione per le operazioni dell'API Zonal Endpoint, i nuovi oggetti vengono automaticamente crittografati e decrittografati con SSE-KMS le chiavi S3 Bucket durante la sessione. Per ulteriori informazioni sui comportamenti di crittografia che sovrascrivono nei bucket di directory, vedi [Specificare la crittografia lato server con per il caricamento di nuovi oggetti. AWS KMS](#)

Le chiavi S3 Bucket vengono utilizzate per un periodo di tempo limitato all'interno di Amazon S3, riducendo ulteriormente la necessità per Amazon S3 di effettuare richieste per completare le operazioni di crittografia. AWS KMS Per ulteriori informazioni sull'uso delle chiavi S3 Bucket, consulta [Chiavi bucket Amazon S3](#) e [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

Richiedendo SSE-KMS

Per richiedere SSE-KMS tutti gli oggetti in un particolare bucket di directory, puoi utilizzare una bucket policy. Ad esempio, quando utilizzi l'operazione `CreateSession` API per concedere l'autorizzazione a caricare un nuovo oggetto (`PutObject`, `CreateMultipartUpload`) `CopyObject`, la seguente policy del bucket nega l'autorizzazione di caricamento dell'oggetto (`s3express:CreateSession`) a tutti se la `CreateSession` richiesta non include un'`x-amz-server-side-encryption-aws-kms-key-id` intestazione che richieda. SSE-KMS

JSON

```
{
  "Version": "2012-10-17",
  "Id": "UploadObjectPolicy",
  "Statement": [{
    "Sid": "DenyObjectsThatAreNotSSEKMS",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3express:CreateSession",
```

```

    "Resource": "arn:aws:s3express:us-east-1:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3",
    "Condition": {
      "Null": {
        "s3express:x-amz-server-side-encryption-aws-kms-key-id": "true"
      }
    }
  ]
}

```

Per richiedere l'uso di un particolare AWS KMS key per crittografare gli oggetti in un bucket, puoi utilizzare la chiave condizionale. `s3express:x-amz-server-side-encryption-aws-kms-key-id` Per specificare la chiave KMS, devi utilizzare una chiave Amazon Resource Name (ARN) nel formato indicato. `arn:aws:kms:region:acct-id:key/key-id` AWS Identity and Access Management non convalida se la stringa per esiste. `s3express:x-amz-server-side-encryption-aws-kms-key-id` L'ID AWS KMS chiave utilizzato da Amazon S3 per la crittografia degli oggetti deve corrispondere all'ID della AWS KMS chiave nella policy, altrimenti Amazon S3 respinge la richiesta.

Per ulteriori informazioni su come SSE-KMS utilizzarlo per il caricamento di nuovi oggetti, consulta [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\) per il caricamento di nuovi oggetti nei bucket di directory](#)

Per un elenco completo delle chiavi di condizione specifiche per i bucket di directory, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).

Contesto di crittografia

Per i bucket di directory, un contesto di crittografia è un insieme di coppie chiave-valore che contiene informazioni contestuali sui dati. Non è supportato un valore aggiuntivo del contesto di crittografia. Per ulteriori informazioni sul contesto di crittografia, consulta [Contesto di crittografia](#).

Per impostazione predefinita, se utilizzi SSE-KMS un bucket di directory, Amazon S3 utilizza il bucket Amazon Resource Name (ARN) come coppia di contesti di crittografia:

```
arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3
```


Assicurati che le tue policy o policy AWS KMS chiave IAM utilizzino il bucket ARN come contesto di crittografia.

Facoltativamente, puoi fornire una coppia di contesti di crittografia esplicita utilizzando l'`x-amz-server-side-encryption-context` intestazione in una richiesta API Zonal Endpoint, ad esempio. [CreateSession](#) Il valore di questa intestazione è una Base64-encoded stringa di un JSON UTF-8 codificato, che contiene il contesto di crittografia come coppie chiave-valore. Per i bucket di directory, il contesto di crittografia deve corrispondere al contesto di crittografia predefinito: il nome della risorsa Amazon (ARN) del bucket. Inoltre, poiché il contesto di crittografia non è criptato, assicurarsi che non contenga informazioni sensibili.

È possibile utilizzare il contesto di crittografia per identificare e categorizzare le operazioni di crittografia. Puoi anche utilizzare il valore ARN del contesto di crittografia predefinito per tenere traccia delle richieste pertinenti AWS CloudTrail visualizzando quale bucket di directory ARN è stato utilizzato con quale chiave di crittografia.

Nel `requestParameters` campo di un file di CloudTrail log, se si utilizza SSE-KMS in un bucket di directory, il valore del contesto di crittografia è l'ARN del bucket.

```
"encryptionContext": {  
  "aws:s3express:arn": "arn:aws:s3::arn:aws:s3express:region:account-  
id:bucket/bucket-base-name--zone-id--x-s3"  
}
```

Inoltre, per la crittografia degli oggetti SSE-KMS in un bucket di directory, AWS KMS CloudTrail gli eventi registrano l'ARN del bucket anziché l'ARN dell'oggetto.

Invio di richieste per AWS KMS oggetti crittografati

È possibile accedere ai bucket di directory solo tramite HTTPS (TLS). Inoltre, i bucket di directory firmano le richieste utilizzando AWS Signature Version 4 (Sigv4). Per ulteriori informazioni sull'invio di richieste di oggetti AWS KMS crittografati, vedere. [Invio di richieste per AWS KMS oggetti crittografati](#)

Se l'oggetto utilizza SSE-KMS, non inviare intestazioni di richiesta di crittografia per GET richieste e HEAD richieste. In caso contrario, riceverai un errore HTTP 400 Bad Request (HTTP 400 - Richiesta non valida).

Verifica della SSE-KMS crittografia nei bucket di directory

Per verificare l'utilizzo delle AWS KMS chiavi per i dati SSE-KMS crittografati, puoi utilizzare AWS CloudTrail i log. Puoi ottenere informazioni dettagliate sulle tue operazioni [crittografiche](#), ad esempio

[GenerateDataKey](#) e [Decrypt](#). CloudTrail supporta numerosi valori di [attributo](#) per filtrare la ricerca, tra cui nome dell'evento, nome utente e origine dell'evento.

Argomenti

- [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\) per il caricamento di nuovi oggetti nei bucket di directory](#)

Specificare la crittografia lato server con AWS KMS (SSE-KMS) per il caricamento di nuovi oggetti nei bucket di directory

Per i bucket di directory, per crittografare i dati con la crittografia lato server, puoi utilizzare la crittografia lato server con chiavi gestite Amazon S3 (`sse-s3`) (impostazione predefinita) o la crittografia lato server con chiavi (SSE-S3) (`sse-kms`). AWS Key Management Service AWS KMS SSE-KMS Si consiglia di utilizzare la configurazione di crittografia predefinita del bucket e di non sovrascrivere la crittografia predefinita del bucket nelle richieste `CreateSession` o nelle richieste di oggetti `PUT`. I nuovi oggetti vengono quindi crittografati automaticamente con le impostazioni di crittografia desiderate. Per ulteriori informazioni sui comportamenti di crittografia che sovrascrivono nei bucket di directory, consulta [Specificare la crittografia lato server con per il caricamento di nuovi oggetti](#). [AWS KMS](#)

Tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita e tutti i nuovi oggetti caricati in un bucket S3 vengono crittografati automaticamente quando sono inattivi. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket in Amazon S3. Se desideri specificare un tipo di crittografia diverso per un bucket di directory, puoi utilizzare la crittografia lato server con AWS Key Management Service (`sse-kms`). AWS KMS SSE-KMS Per crittografare i nuovi oggetti in un bucket di directory con SSE-KMS, devi specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> Chiave gestita da AWS (aws/s3) non è supportato. La SSE-KMS configurazione può supportare solo 1 chiave gestita [dal cliente per bucket di directory](#) per tutta la durata del bucket. Dopo aver specificato una chiave gestita dal cliente per SSE-KMS, non puoi sovrascrivere la chiave gestita dal cliente per la configurazione del bucket. SSE-KMS Quindi, quando si specificano le impostazioni di crittografia lato server per i nuovi oggetti con SSE-KMS, è necessario assicurarsi che la chiave di crittografia sia la stessa chiave gestita dal cliente specificata per la configurazione di crittografia predefinita del bucket di directory. Per utilizzare una nuova chiave gestita dal cliente per i propri dati, si consiglia di copiare gli oggetti esistenti in un nuovo bucket della directory con una nuova chiave gestita dal cliente.

È possibile applicare la crittografia quando stai caricando un nuovo oggetto o copiando un oggetto esistente. Se si modifica la crittografia di un oggetto, viene creato un nuovo oggetto per sostituire quello precedente.

È possibile specificare SSE-KMS utilizzando le operazioni dell'API REST, AWS gli SDK e (). AWS Command Line Interface AWS CLI

Note

- Per i bucket di directory, i comportamenti di esclusione della crittografia sono i seguenti:
 - Quando utilizzi l'[CreateSession](#) API REST per autenticare e autorizzare le richieste dell'API Zonal endpoint tranne [CopyObject](#) e [UploadPartCopy](#), puoi sovrascrivere le impostazioni di crittografia su SSE-S3 o su SSE-KMS solo se hai specificato la crittografia predefinita del bucket con in precedenza. SSE-KMS
 - Quando si utilizza [CreateSession](#) con AWS CLI o con gli AWS SDK per autenticare e autorizzare le richieste dell'API Zonal Endpoint eccetto [CopyObject](#) e [UploadPartCopy](#), non è possibile sovrascrivere affatto le impostazioni di crittografia.
 - Quando effettui [CopyObject](#) richieste, puoi sovrascrivere le impostazioni di crittografia su SSE-S3 o su SSE-KMS solo se in precedenza hai specificato la crittografia predefinita del bucket. SSE-KMS Quando effettui [UploadPartCopy](#) richieste, non puoi sovrascrivere le impostazioni di crittografia.
- Puoi utilizzare Multi-region AWS KMS keys in Amazon S3. Tuttavia, Amazon S3 attualmente tratta le chiavi multiregionali come se fossero chiavi monoregionali e non utilizza le caratteristiche multiregionali della chiave. Per ulteriori informazioni, consulta [Utilizzo delle chiavi multi-regione](#) nella Guida per gli sviluppatori di AWS Key Management Service .
- Se si desidera utilizzare una chiave KMS di proprietà di un altro account, è necessario avere l'autorizzazione a utilizzarla. Per ulteriori informazioni sulle autorizzazioni tra account per le chiavi KMS, vedi [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Utilizzo della REST API

Note

Per ogni bucket di directory è supportata una sola [chiave gestita dal cliente](#) per tutta la durata del bucket. [Chiave gestita da AWS](#) (aws/s3) non è supportato. Dopo aver specificato SSE-KMS come configurazione di crittografia predefinita del bucket una chiave gestita dal cliente, non è possibile modificare la chiave gestita dal cliente per la configurazione del bucket. SSE-KMS

Per le operazioni API [sugli endpoint zionali \(a livello di oggetto\)](#), ad eccezione di [CopyObject](#) and [UploadPartCopy](#), si autenticano e autorizzano le richieste con una bassa latenza. [CreateSession](#) Si consiglia di utilizzare la crittografia predefinita del bucket con le configurazioni di crittografia desiderate e di non sovrascrivere la crittografia predefinita del bucket nelle richieste `CreateSession` o nelle richieste di oggetti PUT. I nuovi oggetti vengono quindi crittografati automaticamente con le impostazioni di crittografia desiderate. Per crittografare i nuovi oggetti in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> Quindi, quando viene creata una sessione per le operazioni dell'API Zonal Endpoint, i nuovi oggetti vengono automaticamente crittografati e decrittografati con SSE-KMS le chiavi S3 Bucket durante la sessione. Per ulteriori informazioni sui comportamenti di crittografia che sovrascrivono nei bucket di directory, vedi [Specificare la crittografia lato server con per il caricamento di nuovi oggetti. AWS KMS](#)

Nelle chiamate all'API degli endpoint zionali (eccetto [CopyObject](#) e [UploadPartCopy](#)) che utilizzano l'API REST, non è possibile sovrascrivere i valori delle impostazioni di crittografia (`x-amz-server-side-encryption,, e`) della richiesta. `x-amz-server-side-encryption-aws-kms-key-id` `x-amz-server-side-encryption-context` `x-amz-server-side-encryption-bucket-key-enabled` `CreateSession` Non è necessario specificare esplicitamente i valori delle impostazioni di crittografia nelle chiamate API dell'endpoint di zona; Amazon S3 utilizzerà i valori delle impostazioni di crittografia dalla richiesta `CreateSession` per proteggere i nuovi oggetti nel bucket della directory.

Note

Quando utilizzi AWS CLI o gli AWS SDK, `forCreateSession`, il token di sessione si aggiorna automaticamente per evitare interruzioni del servizio alla scadenza di una sessione.

Gli AWS CLI o gli AWS SDK utilizzano la configurazione di crittografia predefinita del bucket per la richiesta. `CreateSession` Non è supportato l'annullamento dei valori delle impostazioni di crittografia nella richiesta `CreateSession`. Inoltre, nelle chiamate API degli endpoint zonali (eccetto [CopyObject](#) e [UploadPartCopy](#)), non è supportato sovrascrivere i valori delle impostazioni di crittografia della richiesta. `CreateSession`

Per [CopyObject](#) crittografare le copie di nuovi oggetti in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> Quindi, quando si specificano le impostazioni di crittografia sul lato server per le copie di nuovi oggetti con SSE-KMS, è necessario assicurarsi che la chiave di crittografia sia la stessa chiave gestita dal cliente specificata per la configurazione di crittografia predefinita del bucket di directory. Per [UploadPartCopy](#) crittografare le copie di nuove parti di oggetti in un bucket di directory con SSE-KMS, devi specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> Non è possibile specificare le impostazioni di crittografia sul lato server per le nuove copie delle parti dell'oggetto nelle intestazioni della richiesta. SSE-KMS [UploadPartCopy](#) Inoltre, le impostazioni di crittografia fornite nella [CreateMultipartUpload](#) richiesta devono corrispondere alla configurazione di crittografia predefinita del bucket di destinazione.

Argomenti

- [Operazioni API REST di Amazon S3 che supportano SSE-KMS](#)
- [Contesto di crittografia \(x-amz-server-side-encryption-context\)](#)
- [AWS KMS ID della chiave \(x-amz-server-side-encryption-aws-kms-key-id\)](#)
- [Chiavi bucket S3 \(x-amz-server-side-encryption-aws-bucket-key-enabled\)](#)

Operazioni API REST di Amazon S3 che supportano SSE-KMS

Le seguenti operazioni REST API a livello di oggetto nei bucket di directory accettano le intestazioni di richiesta `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id` e `x-amz-server-side-encryption-context`.

- [CreateSession](#)— Quando utilizzi le operazioni API Zonal Endpoint (a livello di oggetto) (eccetto `CopyObject` and `UploadPartCopy`), puoi specificare queste intestazioni di richiesta.

- [PutObject](#): quando carichi i dati utilizzando l'operazione API PUT, è possibile specificare queste intestazioni di richiesta.
- [CopyObject](#) - Quando si copia un oggetto, si ha un oggetto di origine e un oggetto di destinazione. Quando si trasmettono le SSE-KMS intestazioni con l'CopyObject operazione, queste vengono applicate solo all'oggetto di destinazione.
- [CreateMultipartUpload](#) - Quando si caricano oggetti di grandi dimensioni utilizzando l'operazione API di caricamento multipart, è possibile specificare queste intestazioni. Queste intestazioni vengono specificate nella richiesta CreateMultipartUpload.

Le intestazioni di risposta delle seguenti operazioni REST API restituiscono l'intestazione `x-amz-server-side-encryption` quando un oggetto viene memorizzato utilizzando la crittografia lato server.

- [CreateSession](#)
- [PutObject](#)
- [CopyObject](#)
- [POST Object](#)
- [CreateMultipartUpload](#)
- [UploadPart](#)
- [UploadPartCopy](#)
- [CompleteMultipartUpload](#)
- [GetObject](#)
- [HeadObject](#)

 Important

- Tutte le richieste di GET e PUT per un oggetto protetto da AWS KMS falliscono se non si effettuano queste richieste utilizzando il Transport Layer Security (TLS) o la Signature Version 4.
- Se il tuo oggetto utilizza SSE-KMS, non inviare intestazioni di richiesta di crittografia per GET richieste e HEAD richieste, altrimenti riceverai un errore HTTP 400 BadRequest.

Contesto di crittografia (x-amz-server-side-encryption-context)

Se si specifica `x-amz-server-side-encryption:aws:kms`, l'API di Amazon S3 consente di fornire facoltativamente un contesto di crittografia esplicito con l'intestazione `x-amz-server-side-encryption-context`. Per i bucket di directory, un contesto di crittografia è un insieme di coppie chiave-valore che contengono informazioni contestuali sui dati. Il valore deve corrispondere al contesto di crittografia predefinito: il nome della risorsa Amazon (ARN) per il bucket. Non è supportato un valore aggiuntivo del contesto di crittografia.

Per informazioni sul contesto di crittografia nei bucket di directory, consulta [Contesto di crittografia](#). Per informazioni generali sul contesto di crittografia, consulta [Concetti di AWS Key Management Service : Contesto di crittografia](#) nella Guida per gli sviluppatori di AWS Key Management Service .

AWS KMS ID della chiave (x-amz-server-side-encryption-aws-kms-key-id)

Puoi utilizzare l'intestazione `x-amz-server-side-encryption-aws-kms-key-id` per specificare l'ID della chiave gestita dal cliente utilizzata per proteggere i dati.

La tua SSE-KMS configurazione può supportare solo 1 chiave gestita dal cliente per bucket di directory per tutta la durata del bucket. <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk> [Chiave gestita da AWS](#) (aws/s3) non è supportato. Inoltre, dopo aver specificato una chiave gestita dal cliente per SSE-KMS, non è possibile sovrascrivere la chiave gestita dal cliente per la configurazione del bucket. SSE-KMS

Puoi identificare la chiave gestita dal cliente che hai specificato per la SSE-KMS configurazione del bucket nel modo seguente:

- Si effettua una richiesta di operazione API `HeadObject` per trovare il valore di `x-amz-server-side-encryption-aws-kms-key-id` nella risposta.

Per utilizzare una nuova chiave gestita dal cliente per i propri dati, si consiglia di copiare gli oggetti esistenti in un nuovo bucket della directory con una nuova chiave gestita dal cliente.

Per informazioni sul contesto di crittografia nei bucket di directory, consulta [AWS KMS keys](#).

Chiavi bucket S3 (x-amz-server-side-encryption-aws-bucket-key-enabled)

Le S3 Bucket Keys sono sempre abilitate per le operazioni GET e PUT in un bucket di directory e non possono essere disabilitate. Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a

bucket generici o tra bucket di directory, tramite, l'operazione in Batch Operations o i job. [CopyObject](#) [UploadPartCopy](#) [Copy import](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia di un oggetto. KMS-encrypted Per informazioni sulle chiavi dei bucket S3 nei bucket di directory, consulta [Contesto di crittografia](#).

Utilizzo di AWS CLI

Note

Quando si utilizza AWS CLI, `forCreateSession`, il token di sessione si aggiorna automaticamente per evitare interruzioni del servizio alla scadenza di una sessione. Non è supportato sovrascrivere i valori delle impostazioni di crittografia per la richiesta `CreateSession`. Inoltre, nelle chiamate all'API Zonal Endpoint (eccetto [CopyObject](#) e [UploadPartCopy](#)), non è supportato sovrascrivere i valori delle impostazioni di crittografia della richiesta. `CreateSession`

Per crittografare i nuovi oggetti in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). Quindi, quando viene creata una sessione per le operazioni dell'API Zonal Endpoint, i nuovi oggetti vengono automaticamente crittografati e decrittografati con SSE-KMS le chiavi S3 Bucket durante la sessione.

Per utilizzare i seguenti AWS CLI comandi di esempio, sostituiscili con le tue informazioni. *user input placeholders*

Quando si carica un nuovo oggetto o si copia un oggetto esistente, è possibile specificare l'uso della crittografia lato server con AWS KMS chiavi per crittografare i dati. A tale scopo, utilizzate il `put-bucket-encryption` comando per impostare la configurazione di crittografia predefinita del bucket di directory come (). SSE-KMS `aws:kms` In particolare, aggiungi l'intestazione `--server-side-encryption aws:kms` alla richiesta. Usa `--ssekms-key-id example-key-id` per aggiungere la AWS KMS chiave gestita [dal cliente](#) che hai creato. Se lo specifichi `--server-side-encryption aws:kms`, devi fornire un ID AWS KMS chiave della chiave gestita dal cliente. I bucket di directory non utilizzano una chiave AWS gestita. Per un comando di esempio, consulta [Utilizzo di AWS CLI](#).

Quindi, quando si carica un nuovo oggetto con il seguente comando, Amazon S3 utilizza le impostazioni del bucket per la crittografia predefinita per crittografare l'oggetto in modo predefinito.


```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key example-object-key  
--body filepath
```

Non è necessario aggiungere esplicitamente `--bucket-key-enabled` nei comandi delle operazioni API dell'endpoint di zona. Le S3 Bucket Keys sono sempre abilitate per le operazioni GET e PUT in un bucket di directory e non possono essere disabilitate. Le chiavi S3 Bucket non sono supportate quando si copiano oggetti SSE-KMS crittografati da bucket generici a bucket di directory, da bucket di directory a bucket generici o tra bucket di directory [CopyObject](#) [UploadPartCopy](#), tramite [l'Copyoperazione in Batch Operations o i job.](#) [import](#) In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta di copia di un oggetto. KMS-encrypted

Puoi copiare un oggetto da un bucket di origine (ad esempio un bucket generico) a un nuovo bucket (ad esempio, un bucket di directory) e utilizzare la SSE-KMS crittografia per gli oggetti di destinazione. A tale scopo, utilizzate il `put-bucket-encryption` comando per impostare la configurazione di crittografia predefinita del bucket di destinazione (ad esempio, un bucket di directory) come `()`. SSE-KMS `aws:kms` Per un comando di esempio, consulta [Utilizzo di AWS CLI](#). Quindi, quando si copia un oggetto con il seguente comando, Amazon S3 utilizza le impostazioni del bucket per la crittografia predefinita per crittografare l'oggetto per impostazione predefinita.

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket/example-object-key --  
bucket bucket-base-name--zone-id--x-s3 --key example-object-key
```

Utilizzo di AWS SDK

Quando usi AWS gli SDK, puoi richiedere ad Amazon S3 di AWS KMS keys utilizzarlo per la crittografia lato server. Gli esempi seguenti mostrano come utilizzarli SSE-KMS con gli AWS SDK per Java e .NET. Per informazioni su altri SDK, vedi Codice e librerie [di](#) esempio nel AWS Developer Center.

Note

Quando utilizzi gli AWS SDK, `perCreateSession`, il token di sessione si aggiorna automaticamente per evitare interruzioni del servizio alla scadenza di una sessione. Non è supportato sovrascrivere i valori delle impostazioni di crittografia per la richiesta `CreateSession`. Inoltre, nelle chiamate API Zonal Endpoint (eccetto [CopyObject](#) e [UploadPartCopy](#)), non è supportato sovrascrivere i valori delle impostazioni di crittografia della richiesta. `CreateSession`

Per crittografare i nuovi oggetti in un bucket di directory con SSE-KMS, è necessario specificare SSE-KMS come configurazione di crittografia predefinita del bucket di directory una chiave KMS (in particolare, una chiave gestita dal cliente). Quindi, quando viene creata una sessione per le operazioni dell'API Zonal Endpoint, i nuovi oggetti vengono automaticamente crittografati e decrittografati con SSE-KMS le chiavi S3 Bucket durante la sessione.

Per ulteriori informazioni sull'utilizzo degli AWS SDK per impostare la configurazione di crittografia predefinita di un bucket di directory, vedere. SSE-KMS [Utilizzo di AWS SDK](#)

Important

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetrica. Per ulteriori informazioni sulle chiavi, consulta [Chiavi KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni sulla creazione di chiavi gestite dal cliente, consulta [Programming the API nella AWS KMS Developer Guide.](#) AWS Key Management Service

Crittografia dei dati in transito

I bucket della directory utilizzano gli endpoint API regionali e di zona. A seconda dell'operazione API Amazon S3 utilizzata, è necessario un endpoint regionale o zonale. È possibile accedere agli endpoint zonali e regionali tramite un endpoint del cloud privato virtuale (VPC) del gateway. L'utilizzo di endpoint gateway non comporta costi supplementari. Per ulteriori informazioni sugli endpoint API regionali e zonali, consulta [Collegamento in rete per i bucket di directory.](#)

Eliminazione dei dati

Puoi eliminare uno o più oggetti direttamente dai tuoi bucket di directory utilizzando la console Amazon S3, gli AWS SDK, AWS Command Line Interface (AWS CLI) o l'API REST di Amazon S3. Tutti gli oggetti nel bucket di directory sono soggetti a costi di archiviazione, pertanto è necessario eliminare gli oggetti non più necessari.

L'eliminazione di un oggetto archiviato in un bucket di directory elimina in modo ricorsivo anche tutte le directory padre, se queste non contengono oggetti diversi dall'oggetto che viene eliminato.

 Note

Multi-factor l'eliminazione dell'autenticazione (MFA) e il controllo delle versioni S3 non sono supportati per S3 Express One Zone.

Autenticazione e autorizzazione delle richieste

Per impostazione predefinita, i bucket di directory sono privati e l'accesso è possibile solo dagli utenti a cui è concesso esplicitamente l'accesso. Il limite di controllo degli accessi per i bucket di directory è impostato solo a livello di bucket. Al contrario, il limite di controllo degli accessi per i bucket per uso generico può essere impostato a livello di bucket, prefisso o tag dell'oggetto. Questa differenza significa che i bucket di directory sono l'unica risorsa che puoi includere nelle policy dei bucket o nelle policy di identità IAM per l'accesso a S3 Express One Zone.

Amazon S3 Express One Zone supporta sia l'autorizzazione AWS Identity and Access Management (AWS IAM) che l'autorizzazione basata sulla sessione:

- Per utilizzare le operazioni API endpoint regionali (operazioni a livello di bucket, o piano di controllo (control-plane)) con S3 Express One Zone, si utilizza il modello di autorizzazione IAM, che non prevede la gestione delle sessioni. Le autorizzazioni sono concesse per le singole azioni. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).
- Per utilizzare le operazioni API endpoint di zona (operazioni a livello di oggetto o di piano dati), ad eccezione di CopyObject e HeadBucket, si utilizza l'operazione API CreateSession per creare e gestire sessioni ottimizzate per l'autorizzazione a bassa latenza delle richieste di dati. Per recuperare e utilizzare un token di sessione, è necessario consentire l'azione `s3express:CreateSession` per il bucket della directory in una policy basata sull'identità o in una policy di bucket. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#). Se accedi a S3 Express One Zone nella console Amazon S3, tramite AWS Command Line Interface (AWS CLI) o utilizzando gli AWS SDK, S3 Express One Zone crea una sessione per tuo conto.

Con l'operazione API CreateSession, si autenticano e autorizzano le richieste attraverso un nuovo meccanismo basato sulla sessione. Puoi utilizzare CreateSession per richiedere credenziali temporanee che forniscono un accesso a bassa latenza al bucket. Queste credenziali temporanee sono definite per un bucket di directory specifico.

Per utilizzarlo `CreateSession`, ti consigliamo di utilizzare la versione più recente degli AWS SDK o di utilizzare (). AWS Command Line Interface AWS CLI Gli AWS SDK supportati AWS CLI gestiscono l'avvio, l'aggiornamento e la chiusura della sessione per conto dell'utente.

Utilizza i token di sessione solo con operazioni (a livello di oggetto) zonali (fatta eccezione per `CopyObject` e `HeadBucket`) per distribuire la latenza associata all'autorizzazione su un determinato numero di richieste in una sessione. Per operazioni API degli endpoint regionali (operazioni a livello di bucket), viene utilizzata l'autorizzazione IAM, che non prevede la gestione di una sessione. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#) e [Autorizzazione delle operazioni API dell'endpoint di zona con `CreateSession`](#).

Come vengono autenticate e autorizzate le operazioni API

La tabella seguente elenca le informazioni di autenticazione e autorizzazione per le operazioni API del bucket della directory. Per ogni operazione API, la tabella mostra il nome dell'operazione API, l'azione della policy IAM, il tipo di endpoint (regionale o di zona) e il meccanismo di autorizzazione (IAM o basato sulla sessione). Questa tabella indica anche se è supportato l'accesso multi-account. L'accesso alle azioni a livello di bucket può essere concesso solo nelle policy basate sull'identità IAM (utente o ruolo) e non nelle policy dei bucket.

"Hello, World!"	Tipo di endpoint	Azione IAM	Cross-account accesso
<code>CreateBucket</code>	Regionale	<code>s3express:CreateBucket</code>	No
<code>DeleteBucket</code>	Regionale	<code>s3express>DeleteBucket</code>	No
<code>DeleteBucketInventoryConfiguration</code>	Regionale	<code>s3express:PutInventoryConfiguration</code>	No
<code>DeleteBucketPolicy</code>	Regionale	<code>s3express>DeleteBucketPolicy</code>	No
<code>GetBucketInventoryConfiguration</code>	Regionale	<code>s3express:GetInventoryConfiguration</code>	No

"Hello, World!"	Tipo di endpoint	Azione IAM	Cross-account accesso
GetBucketPolicy	Regionale	s3express:GetBucketPolicy	No
ListBucketInventoryConfigurations	Regionale	s3express:GetInventoryConfiguration	No
ListDirectoryBuckets	Regionale	s3express:ListAllMyDirectoryBuckets	No
PutBucketInventoryConfiguration	Regionale	s3express:PutInventoryConfiguration	No
PutBucketPolicy	Regionale	s3express:PutBucketPolicy	No
CreateSession	Zonale	s3express:CreateSession	Sì
CopyObject	Zonale	s3express:CreateSession	Sì
DeleteObject	Zonale	s3express:CreateSession	Sì
DeleteObjects	Zonale	s3express:CreateSession	Sì
HeadObject	Zonale	s3express:CreateSession	Sì
PutObject	Zonale	s3express:CreateSession	Sì
RenameObject	Zonale	s3express:CreateSession	No
GetObjectAttributes	Zonale	s3express:CreateSession	Sì
ListObjectsV2	Zonale	s3express:CreateSession	Sì

"Hello, World!"	Tipo di endpoint	Azione IAM	Cross-account accesso
HeadBucket	Zonale	s3express:CreateSession	Sì
CreateMultiPartUpload	Zonale	s3express:CreateSession	Sì
UploadPart	Zonale	s3express:CreateSession	Sì
UploadPartCopy	Zonale	s3express:CreateSession	Sì
CompleteMultiPartUpload	Zonale	s3express:CreateSession	Sì
AbortMultiPartUpload	Zonale	s3express:CreateSession	Sì
ListParts	Zonale	s3express:CreateSession	Sì
ListMultiPartUploads	Zonale	s3express:CreateSession	Sì
ListAccessPointsForDirectoryBuckets	Zonale	s3express:ListAccessPointsForDirectoryBuckets	Sì
GetAccessPointScope	Zonale	s3express:GetAccessPointScope	Sì
PutAccessPointScope	Zonale	s3express:PutAccessPointScope	Sì
DeleteAccessPointScope	Zonale	s3express>DeleteAccessPointScope	Sì

Argomenti

- [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#)
- [Autorizzazione delle operazioni API dell'endpoint di zona con CreateSession](#)

Autorizzazione delle operazioni API dell'endpoint regionale con IAM

AWS Identity and Access Management (IAM) è una soluzione Servizio AWS che aiuta gli amministratori a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (accesso effettuato) e autorizzato (dotato di autorizzazioni) a utilizzare le risorse Amazon S3 nelle operazioni di bucket di directory e S3 Express One Zone. Puoi utilizzare IAM senza alcun costo aggiuntivo.

Per impostazione predefinita, gli utenti non hanno i permessi per i bucket di directory. Per concedere le autorizzazioni di accesso per i bucket di directory, puoi utilizzare IAM per creare utenti, gruppi o ruoli e collegare le autorizzazioni a tali identità. Per ulteriori informazioni su IAM, consulta [Best Practice per la sicurezza in IAM](#) nella Guida per l'utente di IAM.

Per fornire l'accesso, puoi aggiungere autorizzazioni a utenti, gruppi o ruoli tramite i mezzi seguenti:

- Utenti e gruppi in Centro identità AWS IAM: crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di Centro identità AWS IAM .
- Utenti gestiti in IAM tramite un provider di identità: crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Creazione di un ruolo per un provider di identità di terze parti \(federazione\)](#) nella Guida per l'utente di IAM.
- Ruoli e utenti IAM: crea un ruolo che l'utente è in grado di assumere. Segui le istruzioni in [Creazione di un ruolo per delegare le autorizzazioni a un utente IAM](#) nella Guida per l'utente di IAM.

Per ulteriori informazioni su IAM per S3 Express One Zone, consulta i seguenti argomenti.

Argomenti

- [Principali](#)
- [Resources](#)
- [Azioni per i bucket della directory](#)
- [Policy IAM basate sull'identità per i bucket di directory](#)

- [Esempi di policy di bucket per i bucket di directory](#)
- [AWS politiche gestite per Amazon S3 Express One Zone](#)

Principali

Quando si crea una policy basata sulle risorse per concedere l'accesso ai bucket, è necessario utilizzare l'elemento `Principal` per specificare la persona o l'applicazione che può effettuare una richiesta per un'azione o un'operazione su tale risorsa. Per le policy dei bucket di directory, puoi utilizzare i seguenti principali:

- Un AWS account
- Un utente IAM
- Un ruolo IAM:
- Un utente federato

Per ulteriori informazioni, consulta la sezione [Principal](#) nella Guida per l'utente di IAM.

Resources

Gli Amazon Resource Names (ARN) per i bucket di directory contengono lo spazio dei nomi s3express, la Regione AWS, l'ID dell'AWS account e il nome del bucket di directory, che include l'ID di zona AWS (una zona di disponibilità o un ID di zona locale).

Per accedere ed eseguire azioni sul bucket di directory, è necessario utilizzare il seguente formato ARN:

```
arn:aws:s3express:region:account-id:bucket/base-bucket-name--zone-id--x-s3
```

Per accedere ed eseguire azioni sul punto di accesso di un bucket di directory, è necessario utilizzare il seguente formato ARN:

```
arn:aws::s3express:region:account-id:accesspoint/accesspoint-basename--zone-id--xa-s3
```

Per ulteriori informazioni sugli ARN, consulta [Amazon Resource Names \(ARNs\)](#) nella Guida per l'utente di IAM. Per ulteriori informazioni sulle risorse, consulta [Elementi delle policy JSON IAM: Resource](#) nella Guida per l'utente di IAM.

Azioni per i bucket della directory

In una policy IAM basata sull'identità o una policy basata sulle risorse, vengono definite quali azioni S3 sono consentite o negate. Le azioni corrispondono a specifiche operazioni API. Per fornire le autorizzazioni con i bucket di directory, è necessario utilizzare il namespace S3 Express One Zone, denominato `s3express`.

Quando si fornisce l'autorizzazione `s3express:CreateSession`, l'operazione API `CreateSession` recupera un token di sessione temporaneo per le operazioni API (a livello di oggetto) degli endpoint di zona. Il token di sessione restituisce le credenziali utilizzate per tutte le altre operazioni API degli endpoint di zona. Di conseguenza, non è necessario fornire le autorizzazioni di accesso alle operazioni API di zona utilizzando le policy IAM. `CreateSession` abilita l'accesso a tutte le operazioni a livello di oggetto. Per l'elenco delle operazioni e delle autorizzazioni delle API zonali, consulta [Autenticazione e autorizzazione delle richieste](#).

Per ulteriori informazioni sulle operazioni API `CreateSession`, consulta [CreateSession](#) nella Documentazione di riferimento delle API Amazon Simple Storage Service.

Puoi specificare le seguenti operazioni nell'elemento `Action` di un'istruzione di policy IAM. Utilizza le policy per concedere le autorizzazioni per eseguire un'operazione in AWS. Quando si utilizza un'azione in una policy, in genere si consente o si nega l'accesso all'operazione API con lo stesso nome. Tuttavia, in alcuni casi, una singola azione controlla l'accesso a più operazioni API. L'accesso alle azioni a livello di bucket può essere concesso solo nelle policy basate sulle identità IAM (utente o ruolo) e non nelle policy dei bucket.

Per ulteriori informazioni su come configurare le policy dei punti di accesso, consulta [Configurazione delle policy IAM per l'utilizzo dei punti di accesso per i bucket di directory](#).

Per ulteriori informazioni, consulta [Operazioni, risorse e chiavi di condizione per Amazon S3 Express](#).

Policy IAM basate sull'identità per i bucket di directory

Prima di poter creare i bucket di directory, è necessario concedere le autorizzazioni necessarie al ruolo o agli utenti di AWS Identity and Access Management (IAM). Questa policy di esempio consente l'accesso all'operazione API `CreateSession` (per l'utilizzo con le operazioni API [a livello di oggetto] degli endpoint zonali) e a tutte le operazioni API (a livello di bucket) degli endpoint regionali. Questa policy consente l'operazione API `CreateSession` per l'utilizzo con tutti i bucket di directory, ma le operazioni API degli endpoint regionali sono consentite solo per l'utilizzo con il bucket di directory specificato. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

Note

Come best practice, concedi solo le autorizzazioni necessarie per eseguire un'attività (privilegio minimo). Rimuovi da questa policy tutte le azioni che non sono necessarie per il tuo caso d'uso. Per un elenco completo delle azioni di S3 Express One Zone, vedi [Azioni, risorse e chiavi di condizione per S3 Express One Zone](#) nel Service Authorization Reference.

Example— Identity-based politica per l'accesso al bucket di directory

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRegionalEndpointAPIs",
      "Effect": "Allow",
      "Action": [
        "s3express:CreateBucket",
        "s3express:DeleteBucket",
        "s3express:DeleteBucketPolicy",
        "s3express:GetBucketPolicy",
        "s3express:PutBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:PutEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:PutLifecycleConfiguration",
        "s3express:GetInventoryConfiguration",
        "s3express:PutInventoryConfiguration",
        "s3express:GetMetricsConfiguration",
        "s3express:PutMetricsConfiguration"
      ],
      "Resource": "arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3"
    },
    {
      "Sid": "AllowListAndCreateSession",
      "Effect": "Allow",
      "Action": [
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:CreateSession"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    }
  ]
}
```

Questa politica contiene due affermazioni:

- La prima dichiarazione concede le autorizzazioni per le operazioni API regionali di endpoint (a livello di bucket) su un bucket di directory specifico. Puoi rimuovere le azioni che non ti servono per il tuo caso d'uso.
- La seconda dichiarazione concede le autorizzazioni per `ListAllMyDirectoryBuckets` e `CreateSession`. Queste azioni non supportano le autorizzazioni a livello di risorsa, quindi lo sono. `Resource "*" L'CreateSession` autorizzazione abilita tutte le operazioni API degli endpoint zionali (a livello di oggetto), ad esempio, `PutObject`, `GetObject`, `DeleteObject`.

Esempi di policy di bucket per i bucket di directory

Questa sezione fornisce esempi di policy dei bucket di directory. Per usare queste policy, sostituisci *user input placeholders* con le tue informazioni.

Il seguente esempio di politica del bucket consente **111122223333** a Account AWS ID di utilizzare l'operazione `CreateSession` API per il bucket di directory specificato. Quando non viene specificata alcuna modalità di sessione, la sessione verrà creata con il privilegio massimo consentito (tentando `ReadWrite` prima, poi `ReadOnly` se non consentito). Questa policy concede l'accesso alle operazioni API (a livello di oggetto) degli endpoint zionali.

Example— Politica del bucket per consentire le chiamate `CreateSession`

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteAccess",
      "Effect": "Allow",
      "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3",
      "Principal": {
        "AWS": [
```

```

        "arn:aws:iam::111122223333:root"
      ]
    },
    "Action": [
      "s3express:CreateSession"
    ]
  }
]
}

```

Example– Policy del bucket per consentire chiamate CreateSession con una sessione ReadOnly

Il seguente esempio di politica del bucket consente **111122223333** a Account AWS ID di utilizzare l'operazione CreateSession API. Questa policy utilizza la chiave di condizione `s3express:SessionMode` con il valore `ReadOnly` per impostare una sessione di sola lettura.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnlyAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3express:CreateSession",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3express:SessionMode": "ReadOnly"
        }
      }
    }
  ]
}

```

Example– Policy del bucket per consentire accesso multi-account per chiamate CreateSession

Il seguente criterio di bucket di esempio consente **111122223333** a Account AWS ID di utilizzare l'operazione CreateSession API per il bucket di directory specificato di proprietà di ID. Account AWS **444455556666**

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccount",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "s3express:CreateSession"
      ],
      "Resource": "arn:aws:s3express:us-west-2:444455556666:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3"
    }
  ]
}
```

AWS politiche gestite per Amazon S3 Express One Zone

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. Le policy gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una policy AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui la policy è associata. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AmazonS3ExpressFullAccess

È possibile allegare la policy AmazonS3ExpressFullAccess alle identità IAM. Questa policy garantisce l'accesso completo ai bucket e alle operazioni di directory di Amazon S3 Express One Zone. Consente tutte le azioni con il prefisso del s3express servizio su tutte le risorse.

Questa policy è destinata agli utenti o ai ruoli che necessitano di un accesso illimitato ai bucket di directory. Questa politica copre solo le operazioni di Amazon S3 Express One Zone. Per le operazioni standard di Amazon S3, sono necessarie politiche aggiuntive.

Per visualizzare le autorizzazioni per questa policy, consulta [AmazonS3ExpressFullAccess](#) il AWS Managed Policy Reference.

AWS politica gestita: AmazonS3ExpressReadOnlyAccess

È possibile allegare la policy AmazonS3ExpressReadOnlyAccess alle identità IAM. Questa policy concede autorizzazioni che consentono ReadOnly l'accesso ai bucket di directory Amazon S3 Express One Zone.

Note

L'CreateSessionazione supporta la chiave di SessionMode condizione che può essere impostata su o. ReadOnly ReadWrite Questa politica utilizza SessionMode per una ReadOnly sessione.

Per visualizzare le autorizzazioni per questo criterio, consulta [AmazonS3ExpressReadOnlyAccess](#) il AWS Managed Policy Reference.

Amazon S3 Express One Zone si aggiorna a AWS policy gestite

Visualizza i dettagli sugli aggiornamenti delle policy AWS gestite per Amazon S3 Express One Zone da quando questo servizio ha iniziato a tracciare queste modifiche.

Modifica	Descrizione	Data
È stato aggiunto Amazon S3 Express One Zone. AmazonS3ExpressFullAccess	Amazon S3 Express One Zone ha aggiunto una nuova policy AWS gestita denominata AmazonS3ExpressFullAccess. Questa policy concede autorizzazioni che consentono l'accesso completo ai bucket e alle operazioni di directory di Amazon S3 Express One Zone.	3 aprile 2026
È stato aggiunto Amazon S3 Express One Zone. AmazonS3ExpressReadOnlyAccess	Amazon S3 Express One Zone ha aggiunto una nuova policy AWS gestita denominata AmazonS3ExpressReadOnlyAccess. Questa policy concede autorizzazioni che consentono l'accesso in sola lettura ai bucket di directory Amazon S3 Express One Zone.	3 aprile 2026
Amazon S3 Express One Zone ha iniziato a tracciare le modifiche.	Amazon S3 Express One Zone ha iniziato a tracciare le modifiche relative alle politiche AWS gestite.	3 aprile 2026

Autorizzazione delle operazioni API dell'endpoint di zona con **CreateSession**

Per utilizzare le operazioni API endpoint di zona (a livello di oggetto o di piano dati), ad eccezione di `CopyObject` e `HeadBucket`, si utilizza l'operazione API `CreateSession` per creare e gestire sessioni ottimizzate per l'autorizzazione a bassa latenza delle richieste di dati. Per recuperare e utilizzare un token di sessione, è necessario consentire l'azione `s3express:CreateSession`

per il bucket della directory in una policy basata sull'identità o in una policy di bucket. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#). Se accedi a S3 Express One Zone nella console Amazon S3, tramite AWS Command Line Interface (AWS CLI) o utilizzando gli AWS SDK, S3 Express One Zone crea una sessione per tuo conto. Tuttavia, non puoi modificare il `SessionMode` parametro quando usi gli o SDK. AWS CLI AWS

Se si utilizza la REST API Amazon S3, è possibile quindi utilizzare l'operazione API `CreateSession` per ottenere credenziali di sicurezza temporanee che includono un ID della chiave di accesso, una chiave di accesso segreta, un token di sessione e una data di scadenza. Le credenziali temporanee forniscono le stesse autorizzazioni delle credenziali di sicurezza a lungo termine, come le credenziali degli utenti IAM, ma le credenziali di sicurezza temporanee devono includere un token di sessione.

Modalità sessione

Modalità sessione definisce l'ambito della sessione. Se la modalità di sessione non è specificata nella richiesta `CreateSession` API, l' `CreateSession` azione tenterà di creare la sessione con il privilegio massimo consentito, tentando `ReadWrite` prima e poi ricorrendo `ReadOnly` solo se non `ReadWrite` è consentito dalle policy. Nella tua policy del bucket, puoi specificare la chiave di `s3express:SessionMode` condizione per controllare in modo esplicito chi può creare una sessione or. `ReadWrite` `ReadOnly` Per ulteriori informazioni sulle sessioni `ReadWrite` o `ReadOnly`, consulta il parametro `x-amz-create-session-mode` per [CreateSession](#) nella Documentazione di riferimento delle API Amazon S3. Per ulteriori informazioni sulla policy di bucket da creare, consulta [Esempi di policy di bucket per i bucket di directory](#).

Token di sessione

Quando effettui una chiamata utilizzando le credenziali di sicurezza temporanee, la chiamata deve includere un token di sessione. Il token di sessione viene restituito insieme alle credenziali temporanee. L'ambito di un token di sessione viene definito dal bucket di directory e il token di sessione viene utilizzato per verificare che le credenziali di sicurezza siano valide e non siano scadute. Per proteggere le sessioni, le credenziali di sicurezza temporanee scadono dopo 5 minuti.

CopyObject e HeadBucket

L'ambito delle credenziali di sicurezza temporanee viene definito da un bucket di directory specifico e le credenziali vengono abilitate automaticamente per tutte le chiamate API operative zionali (a livello di oggetto) verso un bucket di directory specifico. A differenza di altre operazioni API degli endpoint zionali, `CopyObject` e `HeadBucket` non utilizzano l'autenticazione `CreateSession`. Tutte le richieste `CopyObject` e `HeadBucket` devono essere autenticate e

firmate utilizzando credenziali IAM. Tuttavia, CopyObject e HeadBucket sono ancora autorizzate da `s3express:CreateSession`, come altre operazioni API degli endpoint zonali.

Per ulteriori informazioni, consulta [CreateSession](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Best practice di sicurezza per i bucket di directory

Quando si lavora con i bucket di directory, occorre tenere conto di una serie di caratteristiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per il tuo ambiente, considerale come consigli utili più che prescrizioni.

Impostazioni predefinite di Blocco dell'accesso pubblico e Proprietà dell'oggetto

I bucket di directory supportano Blocco dell'accesso pubblico S3 e Proprietà dell'oggetto S3. Queste funzionalità S3 vengono utilizzate per la verifica e la gestione dell'accesso ai bucket e agli oggetti.

Per impostazione predefinita, tutte impostazioni Blocco dell'accesso pubblico per i nuovi bucket sono abilitate. Inoltre, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato, il che significa che le liste di controllo degli accessi (ACL) sono disabilitate. Queste impostazioni non possono essere modificate. Per ulteriori informazioni su queste funzionalità, consulta [the section called “Blocco dell'accesso pubblico”](#) e [the section called “Controllo della proprietà degli oggetti”](#).

Note

Non è possibile concedere l'accesso agli oggetti archiviati nei bucket di directory, ma solo ai bucket di directory. Il modello di autorizzazione per S3 Express One Zone è diverso dal modello di autorizzazione per Amazon S3. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint di zona con CreateSession](#).

Autenticazione e autorizzazione

I meccanismi di autenticazione e autorizzazione per i bucket della directory sono diversi, a seconda che si facciano richieste alle operazioni API endpoint di zona o alle operazioni API endpoint regionali. Le operazioni API zonali sono operazioni a livello di oggetto (piano dati). Le operazioni API regionali sono operazioni a livello di bucket (piano di controllo (control-plane)).

L'autenticazione e l'autorizzazione delle richieste alle operazioni API dell'endpoint di zona avvengono tramite un nuovo meccanismo basato sulla sessione , ottimizzato per fornire la latenza più bassa. Con l'autenticazione basata sulla sessione, gli AWS SDK utilizzano l'operazione `CreateSession` API per richiedere credenziali temporanee che forniscono un accesso a bassa latenza al bucket di directory. Queste credenziali temporanee sono definite per un bucket di directory specifico e scadono dopo 5 minuti. È possibile utilizzare queste credenziali temporanee per firmare chiamate API (a livello di oggetto) zonali. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint di zona con `CreateSession`](#).

Firma delle richieste con le credenziali per la gestione dei bucket di directory

Utilizzi le tue credenziali per firmare le richieste API Zonal Endpoint (a livello di oggetto) con Signature Version 4, con AWS come nome del servizio. `s3express` Quando si firmano le richieste, viene utilizzata la chiave segreta restituita da `CreateSession` e viene fornito anche il token di sessione con `x-amzn-s3session-token` header. Per ulteriori informazioni, consulta [CreateSession](#).

Gli [SDK AWS supportati](#) gestiscono le credenziali e la firma per conto dell'utente. Ti consigliamo di utilizzare gli AWS SDK per aggiornare le credenziali e firmare le richieste per te.

Richieste di firma con credenziali IAM

Tutte le chiamate API (a livello di bucket) regionali devono essere autenticate e firmate da credenziali AWS Identity and Access Management (IAM) anziché da credenziali di sessione temporanee. Le credenziali IAM sono costituite dall'ID chiave di accesso e dalla chiave di accesso segreta per le identità IAM. Tutte le richieste `CopyObject` e `HeadBucket` devono essere autenticate e firmate utilizzando credenziali IAM.

Per ottenere la latenza più bassa per le chiamate alle operazioni di zona (a livello di oggetto), si consiglia di utilizzare le credenziali ottenute dalla chiamata a `CreateSession` per firmare le richieste, ad eccezione delle richieste a `CopyObject` e `HeadBucket`.

Utilizzo AWS CloudTrail

AWS CloudTrail fornisce un registro delle azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS in Amazon S3. Puoi utilizzare le informazioni raccolte da CloudTrail per determinare quanto segue:

- La richiesta effettuata ad Amazon S3

- L'indirizzo IP dal quale è stata effettuata la richiesta
- L'utente che ha effettuato la richiesta
- L'ora in cui è stata effettuata la richiesta
- Dettagli aggiuntivi relativi alla richiesta

Quando si configura il proprio Account AWS, gli eventi di CloudTrail gestione sono abilitati per impostazione predefinita. Le seguenti operazioni API regionali per gli endpoint (operazioni API a livello di bucket o piano di controllo) vengono registrate. CloudTrail

- [CreateBucket](#)
- [DeleteBucket](#)
- [DeleteBucketPolicy](#)
- [PutBucketPolicy](#)
- [GetBucketPolicy](#)
- [ListDirectoryBuckets](#)
- [ListMultipartUploads](#)
- [PutBucketEncryption](#)
- [GetBucketEncryption](#)
- [DeleteBucketEncryption](#)

 Note

`ListMultipartUploads` è un'operazione API dell'endpoint di zona. Tuttavia, viene registrato come evento di gestione. CloudTrail Per ulteriori informazioni, consulta [ListMultipartUploads](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Per impostazione predefinita, i CloudTrail percorsi non registrano gli eventi di dati, ma puoi configurare i percorsi per registrare gli eventi di dati per i bucket di directory specificati o per registrare gli eventi di dati per tutti i bucket di directory del tuo account. AWS Vengono registrate le seguenti operazioni API degli endpoint zonali (operazioni API a livello di oggetto o piano dati). CloudTrail

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CreateSession](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [DeleteObject](#)
- [DeleteObjects](#)
- [GetObject](#)
- [GetObjectAttributes](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListObjectsV2](#)
- [ListParts](#)
- [PutObject](#)
- [UploadPart](#)
- [UploadPartCopy](#)

Per ulteriori informazioni sull'utilizzo AWS CloudTrail con i bucket di directory, vedere [Registrazione con i bucket di directory. AWS CloudTrail](#)

Implementa il monitoraggio utilizzando AWS Strumenti di monitoraggio

Il monitoraggio è una parte importante per mantenere l'affidabilità, la sicurezza, la disponibilità e le prestazioni di Amazon S3 e delle tue AWS soluzioni. AWS fornisce diversi strumenti e servizi per aiutarti a monitorare Amazon S3 e gli altri. Servizi AWS Ad esempio, puoi monitorare le CloudWatch metriche di Amazon per Amazon S3, in particolare le metriche di storage `BucketSizeBytes` e `NumberOfObjects`.

Gli oggetti memorizzati nei bucket di directory non si rifletteranno nelle metriche di archiviazione `BucketSizeBytes` e `NumberOfObjects` per Amazon S3. Tuttavia, le metriche di archiviazione `BucketSizeBytes` e `NumberOfObjects` sono supportate per i bucket di directory. Per visualizzare le metriche desiderate, è possibile differenziare le classi di storage di Amazon S3 specificando una dimensione `StorageType`. Per ulteriori informazioni, consulta [Metriche di monitoraggio con Amazon CloudWatch](#).

Per ulteriori informazioni, consulta [Metriche di monitoraggio con Amazon CloudWatch](#) e [Registrazione e monitoraggio in Amazon S3](#).

Gestione dell'accesso ai set di dati condivisi in bucket di directory con punti di accesso

I punti di accesso Amazon S3 semplificano la gestione dell'accesso ai dati su larga scala per set di dati condivisi in Amazon S3. I punti di accesso sono nomi host univoci creati per applicare autorizzazioni e controlli di rete distinti per tutte le richieste effettuate tramite un punto di accesso. Puoi creare centinaia di punti di accesso per bucket, ognuno con un nome distinto e autorizzazioni personalizzate per ogni applicazione. Ogni punto di accesso funziona in combinazione con la policy di bucket associata al bucket sottostante.

Nei bucket di directory, il nome di un punto di accesso è costituito da un nome di base fornito, seguito dall'ID di zona (zona di AWS disponibilità o zona locale) della posizione del bucket di directory e quindi. --xa-s3 Ad esempio, *accesspointname--zoneID--xa-s3*. Dopo aver creato un punto di accesso, non è possibile modificare il nome o l'ID di zona.

Con i punti di accesso per i bucket di directory, è possibile utilizzare l'ambito del punto di accesso per limitare l'accesso a prefissi od operazioni API specifici. È possibile specificare qualsiasi numero di prefissi, ma la lunghezza totale dei caratteri di tutti i prefissi deve essere inferiore a 256 byte.

È possibile configurare qualsiasi punto di accesso per accettare le richieste solo da un cloud privato virtuale (VPC). Ciò limita l'accesso ai dati di Amazon S3 a una rete privata.

Gli argomenti di questa sezione illustrano come utilizzare i punti di accesso per i bucket di directory. Per informazioni sui bucket di directory, consulta [Operazioni con i bucket di directory](#).

Argomenti

- [Punti di accesso per i bucket di directory: regole di denominazione, restrizioni e limitazioni](#)
- [Riferimento ai punti di accesso per bucket di directory](#)
- [Operazioni sugli oggetti per i punti di accesso di bucket di directory](#)
- [Configurazione delle policy IAM per l'utilizzo dei punti di accesso per i bucket di directory](#)
- [Monitoraggio e registrazione dei log dei punti di accesso per i bucket di directory](#)
- [Creazione di punti di accesso per bucket di directory](#)
- [Gestione dei punti di accesso per bucket di directory](#)

- [Utilizzo di tag con Punti di accesso S3 per bucket di directory](#)

Punti di accesso per i bucket di directory: regole di denominazione, restrizioni e limitazioni

Gli Access Point semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in Amazon S3. I seguenti argomenti forniscono informazioni sulle regole di denominazione dei punti di accesso con restrizioni e limitazioni.

Argomenti

- [Regole di denominazione per i punti di accesso di bucket di directory](#)
- [Restrizioni e limitazioni per i punti di accesso di bucket di directory](#)

Regole di denominazione per i punti di accesso di bucket di directory

Il punto di accesso deve essere creato nella stessa zona in cui si trova il bucket. Il nome di un punto di accesso deve essere univoco all'interno della zona.

I nomi dei punti di accesso devono DNS-compliant e devono soddisfare le seguenti condizioni:

- Devono iniziare con un numero o una lettera minuscola
- Il nome di base fornito dall'utente essere composto da un numero di caratteri compreso tra 3 e 50.
- Non possono iniziare o terminare con un trattino (-).
- Non possono contenere caratteri di sottolineatura (_), lettere maiuscole, spazi o punti (.).
- Devono terminare con il suffisso **zoneid--xa--s3**.

Restrizioni e limitazioni per i punti di accesso di bucket di directory

I punti di accesso di bucket di directory presentano le seguenti restrizioni e limitazioni:

- Ogni punto di accesso è associato a un solo bucket di directory. Dopo aver creato un punto di accesso, non è possibile associarlo a un bucket diverso. Tuttavia, è possibile eliminare un punto di accesso e quindi crearne un altro con lo stesso nome associato a un bucket diverso.
- Dopo aver creato un access point, non è possibile modificarne la configurazione del cloud privato virtuale (VPC).
- Le policy access point sono limitate a una dimensione di 20 KB.

- I prefissi dell'ambito del punto di accesso sono limitati a 256 byte in totale.
- È possibile creare un massimo di 10.000 punti di accesso per Account AWS persona Regione AWS. Se hai bisogno di più di 10.000 punti di accesso per un singolo account in una singola Regione, puoi richiedere un aumento della quota di servizio. Per ulteriori informazioni su Service Quotas e la richiesta di un aumento, consultare [AWS Service Quotas](#) in Riferimenti generali di AWS.
- Puoi utilizzare gli access point solo per eseguire le operazioni sugli oggetti. Non puoi utilizzare i punti di accesso per eseguire operazioni sui bucket Amazon S3, ad esempio la modifica o l'eliminazione di bucket. Per l'elenco completo delle operazioni supportate, consulta [Operazioni sugli oggetti per i punti di accesso di bucket di directory](#).
- È possibile fare riferimento ai punti di accesso per nome, alias del punto di accesso o URI virtual-hosted-style. Non è possibile indirizzare i punti di accesso tramite ARN. Per ulteriori informazioni, consulta [Riferimento ai punti di accesso per bucket di directory](#).
- Le operazioni API che controllano la funzionalità del punto di accesso (ad esempio PutAccessPointPolicy e GetAccessPointPolicy) devono specificare l' AWS account proprietario del punto di accesso.
- È necessario utilizzare AWS la versione 4 di Signature quando si effettuano richieste a un punto di accesso utilizzando l'API REST. Per ulteriori informazioni sull'autenticazione delle richieste, consulta [Authenticating Requests \(AWS Signature Version 4\)](#) nel Amazon Simple Storage Service API Reference.
- I punti di accesso supportano solo le richieste tramite HTTPS. Amazon S3 risponderà automaticamente con un reindirizzamento HTTP per qualsiasi richiesta effettuata tramite HTTP, per aggiornare la richiesta a HTTPS.
- Gli access point non supportano l'accesso anonimo.
- Se crei un punto di accesso per un bucket di proprietà di un altro account (un punto di accesso multi-account), il punto di accesso multi-account non fornisce l'accesso ai dati finché il proprietario del bucket non ti concede l'autorizzazione ad accedere al bucket. Il proprietario del bucket mantiene sempre il massimo controllo sui dati e deve aggiornare la policy di bucket per autorizzare le richieste provenienti dal punto di accesso multi-account. Per un esempio di policy di bucket, consulta [Configurazione delle policy IAM per l'utilizzo dei punti di accesso per i bucket di directory](#).

Riferimento ai punti di accesso per bucket di directory

Dopo aver creato un punto di accesso, è possibile utilizzarlo come endpoint per eseguire operazioni sugli oggetti. Per i punti di accesso di bucket di directory, l'alias del punto di accesso è uguale al

nome del punto di accesso. È possibile utilizzare il nome del punto di accesso anziché il nome del bucket per tutte le operazioni sui dati. Per l'elenco delle operazioni supportate, consulta [Operazioni sugli oggetti per i punti di accesso di bucket di directory](#).

Riferimento ai punti di accesso tramite URI virtual-hosted-style

Gli access point supportano solo l'indirizzamento in stile hosting virtuale. I punti di accesso utilizzano lo stesso formato degli endpoint del bucket di directory. Per ulteriori informazioni, consulta [Endpoint regionali e di zona per i bucket di directory](#).

I punti di accesso S3 non supportano l'accesso tramite HTTP. I punti di accesso supportano solo l'accesso sicuro tramite HTTPS.

Operazioni sugli oggetti per i punti di accesso di bucket di directory

I punti di accesso consentono di accedere a un oggetto utilizzando le seguenti operazioni sui dati S3.

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [CreateSession](#)
- [DeleteObject](#)
- [DeleteObjects](#)
- [GetObject](#)
- [GetObjectAttributes](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListMultipartUploads](#)
- [ListObjectsV2](#)
- [ListParts](#)
- [PutObject](#)
- [UploadPart](#)

- [UploadPartCopy](#)

Configurazione delle policy IAM per l'utilizzo dei punti di accesso per i bucket di directory

Gli access point supportano politiche relative alle risorse AWS Identity and Access Management (IAM) che consentono di controllare l'uso dell'access point per risorsa, utente o altre condizioni. Affinché un'applicazione o un utente possa accedere agli oggetti tramite un punto di accesso, sia il punto di accesso che la policy di bucket sottostante devono consentire la richiesta.

Important

L'aggiunta di un punto di accesso a un bucket di directory non modifica il comportamento del bucket quando si accede al bucket direttamente tramite il nome del bucket. Tutte le operazioni esistenti inerenti il bucket continueranno a funzionare come prima. Le limitazioni incluse in una policy di punto di accesso si applicano solo alle richieste effettuate tramite quel punto di accesso.

Quando utilizzi le policy relative alle risorse IAM, assicurati di risolvere gli avvisi di sicurezza, gli errori, gli avvisi generali e i suggerimenti AWS Identity and Access Management Access Analyzer prima di salvare la policy. IAM Access Analyzer esegue controlli sulle policy per convalidare le policy rispetto alla [grammatica delle policy](#) IAM e alle [best practice](#). Questi controlli generano risultati e forniscono suggerimenti per aiutarti a creare policy funzionali e conformi alle best practice per la sicurezza.

Per ulteriori informazioni sulla convalida delle policy tramite IAM Access Analyzer, consulta [Convalida delle policy di IAM Access Analyzer](#) nella Guida per l'utente di IAM. Per visualizzare un elenco delle avvertenze, degli errori e dei suggerimenti restituiti da IAM Access Analyzer, consulta il [Riferimento al controllo delle policy di IAM Access Analyzer](#).

Esempi di policy dei punti di accesso per bucket di directory

Le seguenti policy dei punti di accesso mostrano come controllare le richieste per un bucket di directory. Le policy dei punti di accesso richiedono gli ARN dei bucket o gli ARN dei punti di accesso. Gli alias dei punti di accesso non sono supportati nelle policy. Di seguito è riportato un esempio di ARN di punto di accesso:

```
arn:aws:s3express:region:account-id:accesspoint/myaccesspoint--zoneID--xa-s3
```

È possibile visualizzare l'ARN del punto di accesso nei dettagli per un punto di accesso. Per ulteriori informazioni, consulta [Visualizzazione dei dettagli dei punti di accesso per bucket di directory](#).

Note

Le autorizzazioni concesse in una policy del punto di accesso sono valide solo se anche il bucket sottostante consente lo stesso accesso. Puoi farlo in due modi:

1. (Consigliato) Delega il controllo degli accessi dal bucket al punto di accesso come descritto in [Delegazione del controllo di accesso agli access point](#).
2. Aggiungere le stesse autorizzazioni contenute nella policy del punto di accesso alla policy del bucket sottostante.

Example 1. Policy di controllo del servizio per limitare i punti di accesso alle origini della rete VPC

La seguente policy di controllo del servizio richiede la creazione di tutti i nuovi punti di accesso con un'origine di rete di tipo cloud privato virtuale (VPC). Con questa policy, gli utenti dell'organizzazione non possono creare nuovi punti di accesso accessibili da Internet.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "s3express:CreateAccessPoint",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3express:AccessPointNetworkOrigin": "VPC"
        }
      }
    }
  ]
}
```

}

Example 2. Policy di punto di accesso per limitare l'accesso dei bucket ai punti di accesso con origine dalla rete VPC

La seguente politica sui punti di accesso limita tutti gli accessi al bucket *amzn-s3-demo-bucket--zoneID--x-s3* a un punto di accesso con origine di rete VPC.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSessionFromNonVPC",
      "Principal": "*",
      "Action": "s3express:CreateSession",
      "Effect": "Deny",
      "Resource": "arn:aws:s3express:us-east-1:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3"
    }
  ]
}
```

Chiavi di condizione

I punti di accesso per i bucket di directory dispongono di chiavi di condizione che è possibile utilizzare nelle policy IAM per controllare l'accesso alle risorse. Le seguenti chiavi di condizione rappresentano solo una parte di una policy IAM. Per esempi completi di policy, consulta [Esempi di policy dei punti di accesso per bucket di directory](#), [Delegazione del controllo di accesso agli access point](#) e [Concessione delle autorizzazioni per i punti di accesso multi-account](#).

s3express:DataAccessPointArn

Questo esempio mostra come filtrare l'accesso in base al nome della risorsa Amazon (ARN) di un punto di accesso e corrisponde a tutti i punti di accesso per Account AWS *111122223333* una regione: *region*

```
"Condition" : {
```

```
"StringLike": {
  "s3express:DataAccessPointArn":
    "arn:aws:s3express:region:111122223333:accesspoint/*"
}
```

s3express:DataAccessPointAccount

Questo esempio mostra un operatore stringa che è possibile utilizzare per la corrispondenza dell'ID account del proprietario di un punto di accesso. L'esempio seguente restituisce tutti i punti di accesso di proprietà dell' Account AWS *111122223333*.

```
"Condition" : {
  "StringEquals": {
    "s3express:DataAccessPointAccount": "111122223333"
  }
}
```

s3express:AccessPointNetworkOrigin

Questo esempio mostra un operatore stringa che è possibile utilizzare per la corrispondenza dell'origine di rete, Internet o VPC. L'esempio seguente esegue la corrispondenza solo degli access point con un'origine VPC.

```
"Condition" : {
  "StringEquals": {
    "s3express:AccessPointNetworkOrigin": "VPC"
  }
}
```

s3express:Permissions

È possibile utilizzare `s3express:Permissions` per limitare l'accesso a specifiche operazioni API nell'ambito del punto di accesso. Sono supportate le seguenti operazioni API:

- PutObject
- GetObject
- DeleteObject
- ListBucket (richiesto per ListObjectsV2)
- GetObjectAttributes

- AbortMultipartUpload
- ListBucketMultipartUploads
- ListMultipartUploadParts

Note

Quando si utilizzano le chiavi di condizione multivalore, è consigliabile utilizzare `ForAllValues` con le istruzioni `Allow` e `ForAnyValue` con le istruzioni `Deny`. Per ulteriori informazioni, consulta [Chiavi di contesto multivalore](#) nella Guida per l'utente IAM.

Per ulteriori informazioni sull'uso delle chiavi di condizione con Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni necessarie alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Delegazione del controllo di accesso agli access point

È possibile delegare il controllo dell'accesso dalla policy di bucket alla policy del punto di accesso. La policy di bucket di esempio seguente consente l'accesso completo a tutti i punti di accesso dell'account del proprietario del bucket. Dopo aver applicato la policy, l'accesso a questo bucket viene controllato dalla policy del punto di accesso. Si consiglia di configurare i bucket in questo modo per tutti i casi d'uso che non richiedono l'accesso diretto al bucket.

Example policy di bucket che delega il controllo degli accessi ai punti di accesso

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect": "Allow",
      "Principal" : { "AWS": "*" },
      "Action" : "*",
      "Resource" : [ "Bucket ARN",
      "Condition": {
        "StringEquals" : { "s3express:DataAccessPointAccount" : "Bucket owner's account ID" }
      }
    }
  ]
}
```

```
}
```

Concessione delle autorizzazioni per i punti di accesso multi-account

Per creare un punto di accesso a un bucket di proprietà di un altro account, devi prima creare il punto di accesso specificando il nome del bucket e l'ID del proprietario dell'account. Il proprietario del bucket deve quindi aggiornare la policy di bucket per autorizzare le richieste dal punto di accesso. La creazione di un punto di accesso è simile alla creazione di un DNS CNAME in quanto il punto di accesso non fornisce l'accesso al contenuto del bucket. Tutti gli accessi ai bucket sono controllati dalla policy di bucket. La policy di bucket di esempio consente di eseguire richieste GET e LIST sul bucket da un punto di accesso di proprietà di un Account AWS attendibile.

Sostituisci *Bucket ARN* con l'ARN del bucket.

Example della politica del bucket che delega le autorizzazioni a un altro Account AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCreateSessionForDirectoryBucket",
      "Effect": "Allow",
      "Principal": { "AWS": "*" },
      "Action": "s3express:CreateSession",
      "Resource": [ "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3" ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "s3express:Permissions": [
            "GetObject",
            "ListBucket"
          ]
        }
      }
    }
  ]
}
```

Monitoraggio e registrazione dei log dei punti di accesso per i bucket di directory

Puoi registrare le richieste effettuate tramite i punti di accesso e le richieste effettuate alle API che gestiscono i punti di accesso, ad esempio `CreateAccessPoint` utilizzando `GetAccessPointPolicy`, AWS CloudTrail CloudTrail le voci di registro per le richieste effettuate tramite i punti di accesso includono l'ARN del punto di accesso (che include il nome del punto di accesso) nella `resources` sezione del registro.

Si prenda come esempio la seguente configurazione:

- Un bucket denominato `amzn-s3-demo-bucket--zone-id--x-s3` nella Regione `region` che contiene un oggetto denominato `my-image.jpg`.
- Un punto di accesso denominato `my-bucket-ap--zoneID--xa-s3` associato a `amzn-s3-demo-bucket--zone-id--x-s3`
- Un Account AWS ID di 123456789012

L'esempio seguente mostra la `resources` sezione di una voce di CloudTrail registro relativa alla configurazione precedente:

```
"resources": [  
  {"type": "AWS::S3Express::Object",  
    "ARN": "arn:aws:s3express-region:123456789012:bucket/amzn-s3-demo-bucket--zone-id--x-s3/my-image.jpg",  
  },  
  {"accountId": "c",  
    "type": "AWS::S3Express::DirectoryBucket",  
    "ARN": "arn:aws:s3express-region:123456789012:bucket/amzn-s3-demo-bucket--zone-id--x-s3",  
  },  
  {"accountId": "123456789012",  
    "type": "AWS::S3::AccessPoint",  
    "ARN": "arn:aws:s3express-region:123456789012:accesspoint/my-bucket-ap--zoneID--xa-s3",  
  }  
]
```

Per ulteriori informazioni AWS CloudTrail, vedere [What is AWS CloudTrail?](#) nella Guida AWS CloudTrail per l'utente.

Creazione di punti di accesso per bucket di directory

Come i bucket di directory, i punti di accesso possono essere creati in zone di disponibilità o zone locali dedicate. Il punto di accesso deve essere creato nella stessa zona del bucket di directory ad esso associato.

Un punto di accesso è associato esattamente a solo un bucket di directory Amazon S3. Se desideri utilizzare un bucket di directory nel tuo Account AWS, devi prima creare un bucket di directory. Per ulteriori informazioni sulla creazione di bucket di directory, consulta [Creazione di bucket di directory in una zona di disponibilità](#) o [Creazione di un bucket di directory in una zona locale](#).

Puoi anche creare un punto di accesso multi-account associato a un bucket in un altro Account AWS, purché tu conosca il nome del bucket e l'ID dell'account del proprietario del bucket. Tuttavia, la creazione di punti di accesso multi-account non consente l'accesso ai dati nel bucket finché non vengono concesse le autorizzazioni dal proprietario del bucket. Il proprietario del bucket deve concedere all'account del proprietario del punto di accesso (il tuo account) l'accesso al bucket tramite la policy di bucket. Per ulteriori informazioni, consulta [Concessione delle autorizzazioni per i punti di accesso multi-account](#).

Puoi creare un punto di accesso per qualsiasi bucket di directory con Console di gestione AWS, AWS CLI, REST API o SDK. AWS Ogni punto di accesso è associato a un singolo bucket di directory ed è possibile creare centinaia di punti di accesso per ogni bucket. Quando si crea un punto di accesso, si sceglie il nome del punto di accesso e il bucket di directory a cui associarlo. Il nome del punto di accesso è composto da un nome di base fornito dall'utente e da un suffisso che contiene l'ID della zona della posizione del bucket, seguito da `--xa-s3`. Ad esempio, *myaccesspoint-zoneID--xa-s3*. È possibile limitare l'accesso al punto di accesso anche tramite un cloud privato virtuale (VPC). Quindi, è possibile iniziare immediatamente a leggere e scrivere dati tramite il punto di accesso tramite il nome, proprio come si fa con il nome di un bucket di directory.

È possibile utilizzare l'ambito del punto di accesso per limitare l'accesso al bucket di directory tramite il punto di accesso a prefissi od operazioni API specifici. Se non si aggiunge un ambito al punto di accesso, tutti i prefissi nel bucket di directory e tutte le operazioni API possono essere eseguiti sugli oggetti nel bucket quando si accede tramite il punto di accesso. Dopo aver creato il punto di accesso, puoi aggiungere, modificare o eliminare l'ambito utilizzando gli AWS CLI AWS SDK o l'API REST. Per ulteriori informazioni, consulta [Gestione dell'ambito dei punti di accesso per bucket di directory](#).

Dopo aver creato il punto di accesso, è possibile configurare la policy delle risorse IAM del punto di accesso. Per ulteriori informazioni, consulta [Visualizzazione, modifica o eliminazione delle policy dei punti di accesso](#).

Utilizzo della console S3

Note

È possibile creare un punto di accesso per un bucket di directory dalla schermata del bucket di directory. In questo modo viene fornito il nome del bucket di directory e non è necessario scegliere un bucket durante la creazione del punto di accesso. Per ulteriori informazioni, consulta [Elencare i bucket di directory](#).

Come creare un punto di accesso per bucket di directory

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui si desidera creare un punto di accesso. Il punto di accesso deve essere creato nella stessa Regione del bucket associato.
3. Nel riquadro di navigazione a sinistra, scegli Punti di accesso per bucket di directory.
4. Nella pagina Punto di accesso, scegli Crea punto di accesso.
5. Puoi creare un punto di accesso per un bucket di directory nel tuo account o in un altro account. Per creare un punto di accesso per un bucket di directory in un altro account:

Note

Se utilizzi un bucket in un altro Account AWS, il proprietario del bucket deve aggiornare la policy del bucket per autorizzare le richieste dal punto di accesso. Per un esempio di policy di bucket, consulta [Concessione delle autorizzazioni per i punti di accesso multi-account](#).

- a. Nel campo Bucket di directory, scegli Specifica un bucket in un altro account.
- b. Nel campo ID dell'account del proprietario del bucket, inserisci l' Account AWS ID proprietario del bucket.

- c. Nel campo Nome bucket, inserisci il nome del bucket, incluso il nome di base e l'ID della zona. Ad esempio, **bucket-base-name--zone-id--x-s3**.
 6. Per creare un punto di accesso per un bucket di directory nel tuo account:
 - a. Nel campo Bucket di directory, seleziona Scegli un bucket in questo account.
 - b. Nel campo Nome bucket, inserisci il nome del bucket, incluso il nome di base e l'ID della zona. Ad esempio, **bucket-base-name--zone-id--x-s3**. Per scegliere il bucket da un elenco, seleziona Sfoglia S3 e scegli il bucket di directory.
 7. In Nome del punto di accesso, inserisci il nome di base del punto di accesso nel campo Nome di base. Vengono visualizzati l'ID della zona e il nome completo del punto di accesso. Per ulteriori informazioni sulla denominazione dei punti di accesso, consulta [Regole di denominazione per i punti di accesso di bucket di directory](#).
 8. In Origine della rete, scegli tra cloud privato virtuale (VPC) o Internet. Se scegli cloud privato virtuale (VPC), nel campo ID del VPC immetti l'ID del VPC che desideri utilizzare con il punto di accesso.
 9. (Facoltativo) In Ambito del punto di accesso, per applicare un ambito a questo punto di accesso, scegli Limita l'ambito di questo punto di accesso utilizzando prefissi o autorizzazioni.
 - a. Per limitare l'accesso ai prefissi nel bucket di directory, inserisci uno o più prefissi nel campo Prefissi. Per aggiungere un altro prefisso, scegli Aggiungi prefisso. Per rimuovere un prefisso, scegli Rimuovi.
-  **Note**

L'ambito di un punto di accesso ha un limite di caratteri totali pari a 512 caratteri per tutti i prefissi. Puoi vedere il numero di caratteri rimanenti in Aggiungi prefisso.
- b. In Autorizzazioni, scegli una o più operazioni API consentite dal punto di accesso. Per rimuovere un'operazione sui dati, scegli la X accanto al nome dell'operazione sui dati.
 10. Per non applicare un ambito al punto di accesso e consentire l'accesso a tutti i prefissi nel bucket di directory e a tutte le operazioni API tramite il punto di accesso, in Ambito del punto di accesso, scegli Applica l'accesso all'intero bucket.
 11. Scegli Crea punto di accesso per bucket di directory. Il nome del punto di accesso e altre informazioni vengono visualizzati nell'elenco Punti di accesso per bucket di directory.

Utilizzo di AWS CLI

Il comando di esempio seguente crea un punto di accesso denominato *example-ap* per il bucket *amzn-s3-demo-bucket--zone-id--x-s3* nell'account *111122223333*.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3
```

Per limitare l'accesso al punto di accesso tramite un VPC, includi il parametro `--vpc` e l'ID del VPC.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --vpc vpc-id
```

Quando crei un punto di accesso per un bucket multi-account, includi il parametro `--bucket-account-id`. Il comando di esempio seguente crea un punto di accesso nel Account AWS *111122223333*, per il bucket *amzn-s3-demo-bucket--zone-id--x-s3*, di proprietà di Account AWS *444455556666*.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --bucket-account-id 444455556666
```

Per ulteriori informazioni ed esempi, vedere [create-access-point](#) nel Command Reference. AWS CLI

Utilizzo della REST API

Il seguente comando di esempio crea un punto di accesso denominato come *example-ap* il bucket *amzn-s3-demo-bucket--zone-id--x-s3* nell'account *111122223333* e l'accesso è limitato tramite il VPC (opzionale). *vpc-id*

```
PUT /v20180820/accesspoint/example-ap--zoneID--xa-s3 HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointRequest>
  <Bucket>amzn-s3-demo-bucket--zone-id--x-s3</Bucket>
  <BucketAccountId>111122223333</BucketAccountId>
  <VpcConfiguration>
    <VpcId>vpc-id</VpcId>
```

```
</VpcConfiguration>
</CreateAccessPointRequest>
```

Risposta:

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointResult>
  <AccessPointArn>
    "arn:aws:s3express:region:111122223333:accesspoint/example-ap--zoneID--xa-s3"
  </AccessPointArn>
  <Alias>example-ap--zoneID--xa-s3</Alias>
</CreateAccessPointResult>
```

Utilizzo di AWS SDK

È possibile utilizzare gli AWS SDK per creare un punto di accesso. Per ulteriori informazioni, consulta [l'elenco degli SDK supportati](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

Gestione dei punti di accesso per bucket di directory

Questa sezione spiega come gestire i punti di accesso per i bucket di directory utilizzando l' AWS Command Line Interface API REST di Amazon S3 o SDK. AWS

Argomenti

- [Elenco dei punti di accesso per bucket di directory](#)
- [Visualizzazione dei dettagli dei punti di accesso per bucket di directory](#)
- [Visualizzazione, modifica o eliminazione delle policy dei punti di accesso](#)
- [Gestione dell'ambito dei punti di accesso per bucket di directory](#)
- [Eliminazione del punto di accesso per bucket di directory](#)

Elenco dei punti di accesso per bucket di directory

Questa sezione spiega come elencare i punti di accesso per un bucket di directory utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI), API REST o SDK. AWS

Utilizzo della console S3

Per elencare i punti di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione a sinistra della console scegli Punti di accesso per bucket di directory.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegli il nome del punto di accesso da gestire.

Utilizzo di AWS CLI

Il seguente comando di `list-access-points-for-directory-buckets` esempio mostra come è possibile utilizzare il AWS CLI per elencare i punti di accesso di proprietà di un AWS account e associati a un bucket di directory.

Il comando seguente elenca i punti di Account AWS `111122223333` accesso collegati al `amzn-s3-demo-bucket--zone-id--x-s3` bucket.

```
aws s3control list-access-points-for-directory-buckets --account-id 111122223333 --  
directory-bucket amzn-s3-demo-bucket--zone-id--x-s3
```

Per ulteriori informazioni ed esempi, vedere [list-access-points-for-directory-buckets nel Command Reference](#). AWS CLI

Utilizzo della REST API

L'esempio seguente mostra come è possibile utilizzare la REST API per elencare i punti di accesso.

```
GET /v20180820/directoryaccesspoint?directoryBucket=amzn-s3-demo-bucket--zone-id--x-s3  
&maxResults=maxResults HTTP/1.1  
Host: s3express-control.region.amazonaws.com  
x-amz-account-id: 111122223333
```

Example risposta di **ListAccessPointsForDirectoryBuckets**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListDirectoryAccessPointsResult>
  <AccessPointList>
    <AccessPoint>
      <AccessPointArn>arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3</AccessPointArn>
      <Alias>example-access-point--zoneID--xa-s3</Alias>
      <Bucket>amzn-s3-demo-bucket--zone-id--x-s3</Bucket>
      <BucketAccountId>111122223333</BucketAccountId>
      <Name>example-access-point--zoneID--xa-s3</Name>
      <NetworkOrigin>VPC</NetworkOrigin>
      <VpcConfiguration>
        <VpcId>VPC-1</VpcId>
      </VpcConfiguration>
    </AccessPoint>
  </AccessPointList>
</ListDirectoryAccessPointsResult>
```

Utilizzo di AWS SDK

Puoi utilizzare AWS gli SDK per elencare i tuoi punti di accesso. Per ulteriori informazioni, consulta [l'elenco degli SDK supportati](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

Visualizzazione dei dettagli dei punti di accesso per bucket di directory

Questa sezione spiega come visualizzare i dettagli del punto di accesso per i bucket di directory utilizzando Console di gestione AWS, AWS CLI, AWS SDK o API REST.

Utilizzo della console S3

Visualizza i dettagli di un punto di accesso per bucket di directory per esaminare le seguenti informazioni sul punto di accesso e sul bucket di directory associato:

- Proprietà:
 - Nome bucket di directory

- ID account del proprietario del bucket della directory
- Regione AWS
- Tipo di posizione del bucket di directory
- Nome della posizione del bucket di directory
- Data di creazione del punto di accesso
- Origine della rete
- VPC ID
- URI S3
- ARN del punto di accesso
- Alias del punto di accesso
- Autorizzazioni:
 - Esiti dell'analisi degli accessi esterni di IAM
 - Ambito del punto di accesso
 - Policy del punto di accesso

Per visualizzare i dettagli del punto di accesso nel Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione a sinistra della console scegli Punti di accesso per bucket di directory.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegli il nome del punto di accesso da gestire.
6. Scegli la scheda Proprietà o la scheda Autorizzazioni.

Utilizzo di AWS CLI

Il seguente comando di `get-access-point` esempio mostra come è possibile utilizzare il AWS CLI per visualizzare i dettagli del punto di accesso.

Il comando seguente elenca i dettagli del punto di accesso *my-access-point--zoneID--xa-s3* per Account AWS *111122223333*.

```
aws s3control get-access-point --name my-access-point--zoneID--xa-s3 --account-id 111122223333
```

Example dell'output del comando **get-access-point**

```
{
  "Name": "example-access-point--zoneID--xa-s3",
  "Bucket": "amzn-s3-demo-bucket--zone-id--x-s3",
  "NetworkOrigin": "Internet",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "IgnorePublicAcls": true,
    "BlockPublicPolicy": true,
    "RestrictPublicBuckets": true
  },
  "CreationDate": "2025-04-23T18:26:22.146000+00:00",
  "Alias": "example-access-point--zoneID--xa-s3",
  "AccessPointArn": "arn:aws:s3express:region:111122223333:accesspoint/example-access-point--zoneID--xa-s3",
  "BucketAccountId": "296805379465"
}
```

Per ulteriori informazioni ed esempi, consulta [get-access-point](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per visualizzare i dettagli del punto di accesso. Per ulteriori informazioni, consulta [GetAccessPoint](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per visualizzare i dettagli dei tuoi punti di accesso. Per ulteriori informazioni, consulta [l'elenco degli SDK supportati](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

Visualizzazione, modifica o eliminazione delle policy dei punti di accesso

Puoi utilizzare una policy AWS Identity and Access Management (IAM) sui punti di accesso per controllare il principale e la risorsa che può accedere al punto di accesso. L'ambito del punto di accesso gestisce i prefissi e le autorizzazioni API per il punto di accesso. Puoi creare, modificare ed eliminare una policy per i punti di accesso utilizzando l' AWS Command Line Interface API REST o AWS gli SDK. Per ulteriori informazioni sull'ambito dei punti di accesso, consulta [Gestione dell'ambito dei punti di accesso per bucket di directory](#).

Note

Poiché i bucket di directory utilizzano l'autorizzazione basata sulla sessione, la policy deve sempre includere l'azione `s3express:CreateSession`.

Utilizzo della console S3

Come visualizzare, modificare o eliminare una policy del punto di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione a sinistra della console scegli Punti di accesso per bucket di directory.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegli il nome del punto di accesso da gestire.
6. Scegli la scheda Autorizzazioni.
7. Per creare o modificare la policy del punto di accesso, in Policy del punto di accesso, scegli Modifica. Modifica la policy. Selezionare Salva.
8. Per eliminare la policy del punto di accesso, in Policy del punto di accesso, scegli Elimina. Nella finestra Elimina la policy del punto di accesso, digita **confirm** e scegli Elimina.

Utilizzo di AWS CLI

È possibile utilizzare i comandi `get-access-point-policy`, `put-access-point-policy` e `delete-access-point-policy` per visualizzare, modificare o eliminare una policy del punto di accesso. Per ulteriori informazioni, vedi, [get-access-point-policy](#), [put-access-point-policy](#), o [delete-access-point-policy](#) nel AWS CLI Command Reference.

Utilizzo della REST API

È possibile utilizzare le operazioni REST API `GetAccessPointPolicy`, `DeleteAccessPointPolicy` e `PutAccessPointPolicy` per visualizzare, eliminare o modificare una policy del punto di accesso. Per ulteriori informazioni, consulta [PutAccessPointPolicy](#), [GetAccessPointPolicy](#) o [DeleteAccessPointPolicy](#) nella Guida di riferimento delle API Amazon Simple Storage Service.

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per visualizzare, eliminare o modificare una politica del punto di accesso. Per ulteriori informazioni, consulta l'elenco degli SDK supportati per e [PutAccessControlPolicy](#) nell'API [GetAccessControlPolicy](#) [DeleteAccessControlPolicy](#) Reference di Amazon Simple Storage Service.

Gestione dell'ambito dei punti di accesso per bucket di directory

Questa sezione spiega come visualizzare e modificare l'ambito dei punti di accesso per i bucket di directory utilizzando l' AWS Command Line Interface API REST o AWS gli SDK. È possibile utilizzare l'ambito del punto di accesso per limitare l'accesso a prefissi od operazioni API specifici.

Argomenti

- [Visualizzazione dell'ambito dei punti di accesso per bucket di directory](#)
- [Modifica dell'ambito del punto di accesso per bucket di directory](#)
- [Eliminazione dell'ambito dei punti di accesso per bucket di directory](#)

Visualizzazione dell'ambito dei punti di accesso per bucket di directory

Puoi utilizzare l' Console di gestione AWS API REST o AWS Command Line Interface gli AWS SDK per visualizzare l'ambito del tuo punto di accesso per i bucket di directory.

Utilizzo della console S3

Come visualizzare l'ambito del punto di accesso per bucket di directory

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione a sinistra della console scegli Punti di accesso per bucket di directory.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegli il nome del punto di accesso da gestire.
6. Scegli la scheda Autorizzazioni.
7. In Ambito del punto di accesso potrai vedere i prefissi e le autorizzazioni applicati al punto di accesso.

Utilizzo di AWS CLI

Il seguente comando di `get-access-point-scope` esempio mostra come è possibile utilizzare il AWS CLI per visualizzare l'ambito del punto di accesso.

Il comando seguente mostra l'ambito del punto di accesso *my-access-point* -- *zoneID* --xa-s3 for. Account AWS *111122223333*

```
aws s3control get-access-point-scope --name my-access-point--zoneID--xa-s3 --account-id 111122223333
```

Per ulteriori informazioni ed esempi, vedere <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3control/get-access-point-scope.html> `get-access-point-scope` nel Command Reference. AWS CLI

Example risultato di `get-access-point-scope`

```
{
  "Scope": {
```

```

    "Permissions": [
        "ListBucket",
        "PutObject"
    ]
    "Prefixes": [
        "Prefix": "MyPrefix1*",
        "Prefix": "MyObjectName.csv"
    ]
}

```

Utilizzo della REST API

La richiesta di esempio `GetAccessPointScope` seguente mostra come utilizzare la REST API per visualizzare l'ambito del punto di accesso.

La richiesta seguente mostra l'ambito del punto *my-access-point* di accesso `-- --xa-s3` per *region zoneID* Account AWS *111122223333*

```

GET /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333

```

Example risultato di `GetAccessPointScope`

```

HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<GetAccessPointScopeResult>
  <Scope>
    <Prefixes>
      <Prefix>MyPrefix1*</Prefix>
      <Prefix>MyObjectName.csv</Prefix>
    </Prefixes>
    <Permissions>
      <Permission>ListBucket</Permission>
      <Permission>PutObject</Permission>
    </Permissions>
  </Scope>
</GetAccessPointScopeResult>

```

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per visualizzare l'ambito del tuo punto di accesso. Per ulteriori informazioni, consulta [l'elenco degli SDK supportati](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

Modifica dell'ambito del punto di accesso per bucket di directory

Puoi utilizzare la Console di gestione AWS API REST o AWS Command Line Interface gli AWS SDK per modificare l'ambito dei tuoi punti di accesso per i bucket di directory. L'ambito del punto di accesso viene utilizzato per limitare l'accesso a prefissi od operazioni API specifici oppure una combinazione di entrambi.

Puoi includere una o più delle seguenti operazioni API come autorizzazioni:

- PutObject
- GetObject
- DeleteObject
- ListBucket (richiesto per ListObjectsV2)
- GetObjectAttributes
- AbortMultipartUploads
- ListBucketMultipartUploads
- ListMultipartUploadParts

Note

È possibile specificare qualsiasi numero di prefissi, ma la lunghezza totale dei caratteri di tutti i prefissi deve essere inferiore a 256 byte.

Utilizzo della console S3

Come modificare l'ambito del punto di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione a sinistra della console scegli Punti di accesso per bucket di directory.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegli il nome del punto di accesso da gestire.
6. Scegli la scheda Autorizzazioni.
7. Scegli Modifica nella sezione Ambito del punto di accesso.
8. Per aggiungere o rimuovere prefissi:
 - a. Per aggiungere un prefisso, scegli Aggiungi prefisso. Nel campo Prefisso, inserisci il prefisso del bucket di directory. Ripeti l'operazione per aggiungere altri prefissi.
 - b. Per rimuovere un prefisso, scegli Rimuovi.
9. Per aggiungere o rimuovere autorizzazioni:
 - a. Per aggiungere un'autorizzazione, scegli l'autorizzazione nel campo Scegli le operazioni sui dati.
 - b. Per rimuovere un'autorizzazione, scegli la X accanto all'autorizzazione.
10. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Il seguente comando di `put-access-point-scope` esempio mostra come è possibile utilizzare il AWS CLI per modificare l'ambito del punto di accesso.

Il comando seguente modifica l'ambito del punto di accesso di *my-access-point* -- *zoneID* --xa-s3 for. Account AWS *111122223333*

Note

È possibile utilizzare i caratteri jolly nei prefissi utilizzando il carattere asterisco (*). Per utilizzare il carattere asterisco come valore letterale, si aggiunge una barra rovesciata (\) prima dell'asterisco per eseguirne l'escape.

Tutti i prefissi terminano implicitamente con '*', il che significa che vengono inclusi tutti i percorsi all'interno del prefisso.

Quando si modifica l'ambito di un punto di accesso con AWS CLI, si sostituisce l'ambito esistente.

```
aws s3control put-access-point-scope --name my-access-point--zoneID--xa-s3 --account-id 111122223333 --scope Prefixes=string,Permissions=string
```

Per ulteriori informazioni ed esempi, vedere <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3control/put-access-point-scope.html> put-access-point-scope nel Command Reference. AWS CLI

Utilizzo della REST API

La richiesta di esempio PutAccessPointScope seguente mostra come utilizzare la REST API per modificare l'ambito del punto di accesso.

La richiesta seguente modifica l'ambito del punto di accesso di -- --xa-s3 for. *my-access-point zoneID* Account AWS *111122223333*

Note

È possibile utilizzare i caratteri jolly nei prefissi utilizzando il carattere asterisco (*). Per utilizzare il carattere asterisco come valore letterale, si aggiunge una barra rovesciata (\) prima dell'asterisco per eseguirne l'escape.

Tutti i prefissi terminano implicitamente con '*', il che significa che vengono inclusi tutti i percorsi all'interno del prefisso.

Quando si modifica l'ambito di un punto di accesso con l'API, si sostituisce l'ambito esistente.

```
PUT /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<PutAccessPointScopeRequest>
  <Scope>
    <Prefixes>
```

```
<Prefix>Jane/*</Prefix>
</Prefixes>
<Permissions>
  <Permission>PutObject</Permission>
  <Permission>GetObject</Permission>
</Permissions>
<Scope>
</PutAccessPointScopeRequest>
```

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK o AWS CLI l'API REST per modificare l'ambito del tuo punto di accesso. Per ulteriori informazioni, consulta [l'elenco degli SDK supportati](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

Eliminazione dell'ambito dei punti di accesso per bucket di directory

Puoi utilizzare l' Console di gestione AWS API REST o AWS Command Line Interface gli AWS SDK per eliminare l'ambito dei tuoi punti di accesso per i bucket di directory.

Note

Quando si elimina l'ambito di un punto di accesso, vengono eliminati tutti i prefissi e le autorizzazioni.

Utilizzo della console S3

Come eliminare l'ambito del punto di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione a sinistra della console scegli Punti di accesso per bucket di directory.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegli il nome del punto di accesso da gestire.

6. Scegli la scheda Autorizzazioni.
7. In Ambito del punto di accesso, scegli Elimina.
8. Nel campo Per confermare l'eliminazione, digita "confirm", inserisci **confirm**.
9. Scegliere Elimina.

Utilizzo di AWS CLI

Il seguente comando di `delete-access-point-scope` esempio mostra come è possibile utilizzare il AWS CLI per eliminare l'ambito del punto di accesso.

Il comando seguente elimina l'ambito del punto di accesso *my-access-point* -- *zoneID* --xa-s3 for. Account AWS *111122223333*

```
aws s3control delete-access-point-scope --name my-access-point--region-zoneID--xa-s3 --account-id 111122223333
```

Per ulteriori informazioni ed esempi, vedere <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3control/delete-access-point-scope.html> `delete-access-point-scope` nel Command Reference. AWS CLI

Utilizzo della REST API

La richiesta seguente elimina l'ambito del punto di accesso -- --xa-s3 for. *my-access-point zoneID* Account AWS *111122223333*

```
DELETE /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Utilizzo di AWS SDK

Puoi utilizzare gli AWS SDK per eliminare l'ambito del tuo punto di accesso. Per ulteriori informazioni, consulta [l'elenco degli SDK supportati](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

Eliminazione del punto di accesso per bucket di directory

Questa sezione spiega come eliminare il punto di accesso utilizzando l'API REST Console di gestione AWS AWS Command Line Interface, o gli AWS SDK.

 Note

Prima di eliminare un bucket di directory collegato a un punto di accesso, è necessario eliminare il punto di accesso.

Utilizzo della console S3

Per eliminare i punti di accesso per i bucket di directory nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione a sinistra della console scegli Punti di accesso per bucket di directory.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegli il nome del punto di accesso che desideri eliminare.
6. Scegliere Elimina.
7. Digita **confirm** per confermare l'eliminazione, quindi scegli Elimina.

Utilizzo di AWS CLI

Il seguente comando di `delete-access-point` esempio mostra come è possibile utilizzare AWS CLI per eliminare il punto di accesso.

Il comando seguente elimina il punto di accesso *my-access-point* -- *zoneID* --xa-s3 for. Account AWS *11112223333*

```
aws s3control delete-access-point --name my-access-point--zoneID--xa-s3 --account-id 11112223333
```

Per ulteriori informazioni ed esempi, consulta [delete-access-point](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per eliminare il punto di accesso. Per ulteriori informazioni, consulta [DeleteAccessPoint](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

È possibile utilizzare gli AWS SDK per eliminare i punti di accesso. Per ulteriori informazioni, consulta [l'elenco degli SDK supportati](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di tag con Punti di accesso S3 per bucket di directory

Un AWS tag è una coppia chiave-valore che contiene i metadati sulle risorse, in questo caso gli access point Amazon S3 per bucket di directory. È possibile applicare i tag ai punti di accesso al momento della creazione o gestire i tag dei punti di accesso esistenti. Per informazioni generali sui tag, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

Note

Non sono previsti costi aggiuntivi per l'utilizzo dei tag sui punti di accesso per bucket di directory oltre alle tariffe di richiesta API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Metodi comuni per utilizzare i tag con i punti di accesso per bucket di directory

Attribute-based il controllo degli accessi (ABAC) consente di scalare le autorizzazioni di accesso e concedere l'accesso ai punti di accesso per i bucket di directory in base ai relativi tag. Per ulteriori informazioni su ABAC in Amazon S3, consulta [Utilizzo dei tag per ABAC](#).

ABAC per Punti di accesso S3

Punti di accesso Amazon S3 supporta il controllo degli accessi basato su attributi (ABAC) tramite tag. Utilizza le chiavi di condizione basate su tag nelle policy AWS delle tue organizzazioni, IAM e Access Points. Per le aziende, ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle policy IAM, è possibile controllare l'accesso ai punti di accesso per bucket di directory in base ai tag del bucket utilizzando le seguenti [chiavi di condizione globali](#):

- `aws:ResourceTag/key-name`
 - Utilizzare questa chiave per confrontare la coppia chiave-valore del tag specificata nella policy con la coppia chiave-valore associata alla risorsa. Ad esempio, puoi richiedere che l'accesso a una risorsa sia consentito solo se la risorsa dispone di una chiave di tag Dept collegata al valore Marketing. Per ulteriori informazioni, consulta [Controllare l'accesso alle AWS risorse](#).
- `aws:RequestTag/key-name`
 - Utilizzare questa chiave per confrontare la coppia chiave-valore del tag passata nella richiesta con la coppia del tag specificata nella policy. Ad esempio, è possibile controllare che la richiesta includa la chiave del tag Dept e che abbia il valore Accounting. Per ulteriori informazioni, vedere [Controllo dell'accesso durante AWS le richieste](#). È possibile utilizzare questa chiave di condizione per limitare quali coppie chiave-valore di tag possono essere passate durante le operazioni API TagResource e CreateAccessPoint.
- `aws:TagKeys`
 - Utilizzare questa chiave per confrontare le chiavi dei tag in una richiesta con quelle specificate nella policy. Nell'utilizzo delle policy per controllare gli accessi tramite tag, è consigliabile utilizzare la chiave di condizione `aws:TagKeys` per definire le chiavi di tag ammesse. Per esempi di policy e ulteriori informazioni, consulta [Controllo dell'accesso in base alle chiavi di tag](#). È possibile creare un punto di accesso per bucket di directory con tag. Per consentire il tagging durante l'operazione API CreateAccessPoint, è necessario creare una policy che comprende entrambe le azioni `s3express:TagResource` e `s3express:CreateAccessPoint`. È quindi possibile utilizzare la chiave di condizione `aws:TagKeys` per implementare nella richiesta CreateAccessPoint specifici tag.
- `s3express:AccessPointTag/tag-key`
 - Utilizzare questa chiave di condizione per fornire le autorizzazioni a dati specifici tramite punti di accesso con tag. Quando si utilizza `aws:ResourceTag/tag-key` in una policy IAM, sia il punto di accesso sia il bucket a cui punta il punto di accesso devono avere lo stesso tag perché entrambi vengono presi in considerazione durante l'autorizzazione. Per controllare l'accesso ai dati in modo specifico solo tramite il tag del punto di accesso, è possibile utilizzare la chiave di condizione `s3express:AccessPointTag/tag-key`.

Esempi di policy ABAC per i punti di accesso per bucket di directory

Di seguito sono riportati esempi di policy ABAC per i punti di accesso per bucket di directory.

1.1 - Policy IAM per creare o modificare punti di accesso con tag specifici

In questa policy IAM, gli utenti o i ruoli con questa policy possono creare punti di accesso solo se applicano ai punti di accesso i tag con la chiave di tag `project` e il valore di tag `Trinity` nella richiesta di creazione dei punti di accesso. Possono anche aggiungere o modificare i tag sui punti di accesso esistenti per i bucket di directory, purché la richiesta `TagResource` includa la coppia chiave-valore `project:Trinity` del tag.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAccessPointWithTags",
      "Effect": "Allow",
      "Action": [
        "s3express:CreateAccessPoint",
        "s3express:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
            "Trinity"
          ]
        }
      }
    }
  ]
}
```

1.2 - Policy del punto di accesso per limitare le operazioni sul bucket con tag

In questa policy del punto di accesso, i principali IAM (utenti e ruoli) possono eseguire operazioni utilizzando l'azione `CreateSession` sul punto di accesso solo se il valore del tag `project` del punto di accesso corrisponde al valore del tag `project` del principale.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowObjectOperations",
      "Effect": "Allow",
```

```

    "Principal": {
      "AWS": "111122223333"
    },
    "Action": "s3express:CreateSession",
    "Resource": "arn:aws::s3express:region:111122223333:access-point/my-access-
point",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
      }
    }
  }
}

```

1.3 - Policy IAM per modificare i tag sulle risorse esistenti mantenendo la governance dei tag

In questa policy IAM, i principali IAM (utenti o ruoli) possono modificare i tag su un punto di accesso solo se il valore del tag `project` del punto di accesso corrisponde al valore del tag `project` del principale. Solo i quattro tag `project`, `environment`, `owner` e `cost-center` specificati nelle chiavi di condizione `aws:TagKeys` sono consentiti per questi punti di accesso. Ciò aiuta a rafforzare la governance dei tag, impedisce modifiche non autorizzate dei tag e mantiene lo schema di tagging coerente tra i punti di accesso.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3express:TagResource"
      ],
      "Resource": "arn:aws::s3express:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",
            "owner",

```

```

        "cost-center"
      ]
    }
  }
}
]
}

```

1.4 - Utilizzo della chiave s3express: condition AccessPointTag

In questa policy IAM, l'istruzione di condizione consente l'accesso ai dati del bucket solo se il punto di accesso utilizzato per accedere al bucket ha la chiave di tag Environment e il valore di tag Production.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToSpecificAccessPoint",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws::s3express:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "s3express:AccessPointTag/Environment": "Production"
        }
      }
    }
  ]
}

```

Utilizzo di tag con i punti di accesso per bucket di directory

Puoi aggiungere o gestire tag per i punti di accesso per i bucket di directory utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI), AWS gli SDK o utilizzando le API S3:, e.

[TagResource](#) [UntagResource](#) [ListTagsForResource](#) Per ulteriori informazioni, consulta:

Argomenti

- [Creazione di punti di accesso per bucket di directory con tag](#)
- [Aggiunta di un tag a un punto di accesso per bucket di directory](#)
- [Visualizzazione dei tag di un punto di accesso per bucket di directory](#)

- [Eliminazione di un tag da un punto di accesso per bucket di directory](#)

Creazione di punti di accesso per bucket di directory con tag

È possibile applicare i tag ai Punti di accesso Amazon S3 per bucket di directory al momento della creazione. Per ulteriori informazioni, consulta [Utilizzo di tag con Punti di accesso S3 per bucket di directory](#).

Permissions

Per creare un punto di accesso per bucket di directory con tag, è necessario disporre delle seguenti autorizzazioni:

- `s3express:CreateAccessPoint`
- `s3express:TagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di creare un punto di accesso per bucket di directory con tag, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per creare il punto di accesso per bucket di directory e aggiungere un tag.
- Controllare la policy dell'utente IAM per eventuali condizioni del controllo degli accessi basato su attributi (ABAC). Potrebbe essere necessario etichettare i punti di accesso per bucket di directory solo con chiavi e valori di tag specifici. Per ulteriori informazioni, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

Fasi

Puoi creare un punto di accesso per i bucket di directory con i tag applicati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per creare un punto di accesso per bucket di directory con tag utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso (bucket di directory).
3. Scegli Crea punto di accesso per creare un nuovo punto di accesso.
4. Immetti un nome per il punto di accesso. Per ulteriori informazioni, consulta [Punti di accesso per i bucket di directory: regole di denominazione, restrizioni e limitazioni](#).
5. Nella pagina Crea punto di accesso, Tag è un'opzione per la creazione di un nuovo punto di accesso.
6. Scegli Aggiungi nuovo tag per aprire l'editor di tag e inserisci una coppia chiave-valore di tag. La chiave di tag è obbligatoria, mentre il valore è facoltativo.
7. Per aggiungere un altro tag, scegli nuovamente Aggiungi nuovo tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
8. Dopo aver specificato le opzioni per il nuovo punto di accesso, scegli Crea punto di accesso.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come creare un punto di accesso con tag utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
CreateAccessPointRequest createAccessPointRequest =  
    CreateAccessPointRequest.builder()  
        .accountId(111122223333)  
        .name(my-access-point)  
        .bucket(amzn-s3-demo-bucket--zone-id--x-s3)  
  
        .tags(Collections.singletonList(Tag.builder().key("key1").value("value1").build()))  
        .build();  
awss3Control.createAccessPoint(createAccessPointRequest);
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la creazione di un bucket di directory con tag, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [CreateBucket](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come creare un punto di accesso per bucket di directory con tag utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Quando si crea un punto di accesso per bucket di directory, è necessario fornire i dettagli di configurazione e utilizzare la seguente convenzione di denominazione: *my-access-point*

Richiesta:

```
aws s3control create-access-point \  
--account-id 111122223333 \  
--name my-access-point \  
--bucket amzn-s3-demo-bucket--zone-id--x-s3 \  
--profile personal \  
--tags Key=key1,Value=value1 Key=MyKey2,Value=value2 \  
--region region
```

Aggiunta di un tag a un punto di accesso per bucket di directory

È possibile aggiungere i tag ai Punti di accesso Amazon S3 per bucket di directory e modificare questi tag. Per ulteriori informazioni, consulta [Utilizzo di tag con Punti di accesso S3 per bucket di directory](#).

Permissions

Per aggiungere un tag a un punto di accesso per bucket di directory, è necessario disporre della seguente autorizzazione:

- `s3express:TagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di aggiungere un tag a un punto di accesso per bucket di directory, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per aggiungere un tag a un punto di accesso per bucket di directory.
- Se hai tentato di aggiungere una chiave tag che inizia con il prefisso AWS riservato `aws :`, cambia la chiave del tag e riprova.

Fasi

Puoi aggiungere tag ai punti di accesso per i bucket di directory utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per aggiungere tag a un punto di accesso per bucket di directory utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso (bucket di directory).
3. Scegliere il nome del punto di accesso.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri la sezione Tag e scegli Aggiungi nuovo tag.
6. Viene visualizzata la pagina Aggiungi tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
7. Se si aggiunge un nuovo tag con lo stesso nome di chiave di un tag esistente, il valore del nuovo tag sovrascrive il valore del tag esistente.
8. In questa pagina è anche possibile modificare i valori dei tag esistenti.
9. Dopo aver aggiunto i tag, scegli Salva le modifiche.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come aggiungere tag a un punto di accesso per bucket di directory utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;
```

```
import software.amazon.awssdk.services.s3control.model.TagResourceResponse;

public class TagResourceExample {
    public static void tagResourceExample() {
        S3ControlClient s3Control =
            S3ControlClient.builder().region(Region.US_WEST_2).build();

        TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
            .resourceArn("arn:aws::s3:region:111122223333:accesspoint/my-access-
point/*")
            .accountId("111122223333")
            .tags(Tag.builder().key("key1").value("value1").build())
            .build();

        TagResourceResponse response = s3Control.tagResource(tagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'aggiunta di tag a un punto di accesso per bucket di directory, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [TagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come aggiungere tag a un bucket di directory utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control tag-resource \
--account-id 111122223333 \
```

```
--resource-arn arn:aws::s3express:region:444455556666:bucket/prefix--use1-az4--x-s3 \  
--tags "Key=key1,Value=value1"
```

Risposta:

```
{  
  "ResponseMetadata": {  
    "RequestId": "EXAMPLE123456789",  
    "HTTPStatusCode": 200,  
    "HTTPHeaders": {  
      "date": "Wed, 19 Jun 2025 10:30:00 GMT",  
      "content-length": "0"  
    },  
    "RetryAttempts": 0  
  }  
}
```

Visualizzazione dei tag di un punto di accesso per bucket di directory

È possibile visualizzare o elencare i tag applicati ai Punti di accesso Amazon S3 per bucket di directory. Per ulteriori informazioni, consulta [Utilizzo di tag con i bucket di directory S3](#).

Permissions

Per visualizzare i tag applicati a un punto di accesso, è necessario disporre della seguente autorizzazione:

- `s3express:ListTagsForResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di elencare o visualizzare i tag di un punto di accesso per bucket di directory, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per visualizzare o elencare i tag del punto di accesso per bucket di directory.

Fasi

Puoi visualizzare i tag applicati ai punti di accesso per i bucket di directory utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare i tag applicati a un punto di accesso per bucket di directory utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso (bucket di directory).
3. Scegliere il nome del punto di accesso.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag per visualizzare tutti i tag applicati al punto di accesso per bucket di directory.
6. La sezione Tag mostra i User-defined tag per impostazione predefinita. È possibile selezionare la scheda dei tag AWS generati per visualizzare i tag applicati al punto di accesso dai AWS servizi.

Utilizzo di AWS SDK

Questa sezione fornisce un esempio di come visualizzare i tag applicati a un punto di accesso per i bucket di directory utilizzando gli AWS SDK.

SDK for Java 2.x

Questo esempio mostra come visualizzare i tag applicati a un punto di accesso per i bucket di directory utilizzando AWS SDK for Java 2.x.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResourceExample {
    public static void listTagsForResourceExample() {
        S3ControlClient s3Control =
            S3ControlClient.builder().region(Region.US_WEST_2).build();

        ListTagsForResourceRequest listTagsForResourceRequest =
            ListTagsForResourceRequest.builder()
                .resourceArn("arn:aws::s3:us-west-2:111122223333:accesspoint/my-
access-point/*")
```

```
        .accountId("111122223333")
        .build();
    ListTagsForResourceResponse response =
s3Control.listTagsForResource(listTagsForResourceRequest);
    System.out.println("Tags on my resource:");
    System.out.println(response.toString());
}
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la visualizzazione dei tag applicati a un bucket di directory, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [ListTagsforResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

L'esempio della CLI seguente mostra come visualizzare i tag applicati a un punto di accesso per bucket di directory. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3express:region:444455556666:bucket/prefix--use1-az4--x-s3 \
```

Risposta con tag:

```
{
  "Tags": [
    {
      "Key": "MyKey1",
      "Value": "MyValue1"
    },
  ],
}
```

```
{
  "Key": "MyKey2",
  "Value": "MyValue2"
},
{
  "Key": "MyKey3",
  "Value": "MyValue3"
}
]
```

Risposta senza tag:

```
{
  "Tags": []
}
```

Eliminazione di un tag da un punto di accesso per bucket di directory

È possibile rimuovere i tag dai punti di accesso per bucket di directory. Per ulteriori informazioni, consulta [Utilizzo di tag con Punti di accesso S3 per bucket di directory](#).

Note

Se si elimina un tag e in seguito si scopre che veniva utilizzato per monitorare i costi o per il controllo degli accessi, è possibile aggiungere nuovamente il tag al punto di accesso per bucket di directory.

Permissions

Per eliminare un tag da un punto di accesso per bucket di directory, è necessario disporre della seguente autorizzazione:

- `s3express:UntagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di eliminare un tag da un punto di accesso per bucket di directory, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per eliminare un tag da un punto di accesso per bucket di directory.

Fasi

Puoi eliminare i tag dai punti di accesso per i bucket di directory utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per eliminare i tag da un punto di accesso per bucket di directory utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso (bucket di directory).
3. Scegliere il nome del punto di accesso.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag e seleziona la casella di controllo accanto al tag o ai tag che desideri eliminare.
6. Scegliere Elimina.
7. Viene visualizzato il pop-up Elimina tag definiti dall'utente che chiede di confermare l'eliminazione del tag o dei tag selezionati.
8. Seleziona Elimina per confermare.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come eliminare i tag da un bucket di directory utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResourceExample {
    public static void listTagsForResourceExample() {
```

```

S3ControlClient s3Control =
S3ControlClient.builder().region(Region.US_WEST_2).build();

UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
    .resourceArn("arn:aws::s3:region:111122223333:accesspoint/my-access-
point/*")
    .accountId("111122223333")
    .tagKeys("key1")
    .build();

UntagResourceResponse response =
s3Control.untagResource(untagResourceRequest);
System.out.println("Status code (should be 204):");
System.out.println(response.sdkHttpResponse().statusCode());
    }
}

```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'eliminazione dei tag da un punto di accesso, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [UnTagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come eliminare i tag da un punto di accesso utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```

aws s3control untag-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3:region:111122223333:accesspoint/my-access-point/* \
--tag-keys "key1" "key2"

```

Risposta:

```
{
  "ResponseMetadata": {
    "RequestId": "EXAMPLE123456789",
    "HTTPStatusCode": 204,
    "HTTPHeaders": {
      "date": "Wed, 19 Jun 2025 10:30:00 GMT",
      "content-length": "0"
    },
    "RetryAttempts": 0
  }
}
```

Registrazione con AWS CloudTrail per bucket di directory

Amazon S3 è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o servizio. AWS CloudTrail acquisisce tutte le chiamate API per Amazon S3 come eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon S3, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e dettagli aggiuntivi. Quando si verifica un'attività di evento supportata in Amazon S3, tale attività viene registrata in un CloudTrail evento. Puoi utilizzare AWS CloudTrail trail per registrare gli eventi di gestione e gli eventi di dati per i bucket di directory. Per ulteriori informazioni, consulta [Amazon S3 CloudTrail events](#) e [What is? AWS CloudTrail](#) nella Guida per l'AWS CloudTrail utente.

CloudTrail eventi di gestione per bucket di directory

Per impostazione predefinita, CloudTrail registra le azioni a livello di bucket per i bucket di directory come eventi di gestione. Gli eventi di CloudTrail gestione eventsource per i bucket di directory sono: `s3express.amazonaws.com`. Quando configuri il tuo AWS account, gli eventi di CloudTrail gestione sono abilitati per impostazione predefinita. Vengono registrate le seguenti operazioni API regionali degli endpoint (a livello di bucket o piano di controllo, operazioni API). CloudTrail

- [CreateBucket](#)
- [DeleteBucket](#)
- [DeleteBucketPolicy](#)
- [PutBucketPolicy](#)
- [GetBucketPolicy](#)
- [ListDirectoryBuckets](#)

- [ListMultipartUploads](#)
- [GetBucketEncryption](#)
- [PutBucketEncryption](#)
- [DeleteBucketEncryption](#)

Note

ListMultipartUploads è un'operazione API dell'endpoint di zona. Tuttavia, questa operazione API viene registrata come evento di CloudTrail gestione. Per ulteriori informazioni, consulta [ListMultipartUploads](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Per ulteriori informazioni sugli eventi di CloudTrail gestione, vedere [Registrazione degli eventi di gestione](#) nella Guida per l'AWS CloudTrail utente.

CloudTrail eventi di dati per bucket di directory

Gli eventi di dati forniscono informazioni sulle operazioni delle risorse eseguite su o in una risorsa (ad esempio, lettura o scrittura su un oggetto Amazon S3). Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, i CloudTrail percorsi non registrano gli eventi di dati, ma è possibile configurare i percorsi per registrare gli eventi di dati per gli oggetti archiviati in bucket e bucket di directory generici. Per ulteriori informazioni, consulta [Abilitazione della registrazione degli oggetti in un bucket utilizzando la console](#).

Quando registri gli eventi di dati per un trail in CloudTrail, puoi scegliere di utilizzare selettori di eventi avanzati o selettori di eventi di base. Per registrare gli eventi di dati per gli oggetti memorizzati nei bucket della directory, è necessario utilizzare selettori di eventi avanzati.

Quando si configurano i selettori avanzati di risorse, si sceglie o si specifica il tipo di risorsa che è `AWS::S3Express::Object`.

Vengono registrate le seguenti operazioni API degli endpoint zonali (a livello di oggetto o piano dati, operazioni API). CloudTrail

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)

- [CreateSession](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [DeleteObject](#)
- [DeleteObjects](#)
- [GetObject](#)
- [GetObjectAttributes](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListObjectsV2](#)
- [ListParts](#)
- [PutObject](#)
- [RenameObject](#)
- [UploadPart](#)
- [UploadPartCopy](#)

Per ulteriori informazioni sugli eventi CloudTrail relativi ai dati, vedere [Registrazione degli eventi relativi ai dati nella Guida per l'utente](#). AWS CloudTrail

Per ulteriori informazioni sugli CloudTrail eventi per i bucket di directory, consulta i seguenti argomenti:

Argomenti

- [CloudTrail esempi di file di registro per bucket di directory](#)

CloudTrail esempi di file di registro per bucket di directory

Un file di CloudTrail registro include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. Questo argomento contiene esempi di eventi di CloudTrail dati ed eventi di gestione per bucket di directory.

Argomenti

- [CloudTrail esempi di file di registro degli eventi di dati per i bucket di directory](#)

CloudTrail esempi di file di registro degli eventi di dati per i bucket di directory

L'esempio seguente mostra un esempio di file di CloudTrail registro che lo dimostra [CreateSession](#).

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI DPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI DPPEZS35WEXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/RoleToBeAssumed",
        "accountId": "111122223333",
        "userName": "RoleToBeAssumed"
      },
    },

    "attributes": {
      "creationDate": "2024-07-02T00:21:16Z",
      "mfaAuthenticated": "false"
    }
  },
  "eventTime": "2024-07-02T00:22:11Z",
  "eventSource": "s3express.amazonaws.com",
  "eventName": "CreateSession",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "72.21.198.68",
  "userAgent": "aws-sdk-java/2.20.160-SNAPSHOT
Linux/5.10.216-225.855.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/11.0.23+9-LTS
Java/11.0.23 vendor/Amazon.com_Inc. md/internal exec-env/AWS_Lambda_java11 io/sync
http/Apache cfg/retry-mode/standard",
  "requestParameters": {
    "bucketName": "bucket-base-name--usw2-az1--x-s3".
    "host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
    "x-amz-create-session-mode": "ReadWrite"
  },
  "responseElements": {
    "credentials": {
```

```

        "accessKeyId": "AKIAI44QH8DHBEXAMPLE"
        "expiration": "\"Mar 20, 2024, 11:16:09 PM\"",
        "sessionToken": "<session token string>"
    },
},
"additionalEventData": {
    "SignatureVersion": "SigV4",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "bytesTransferredIn": 0,
    "AuthenticationMethod": "AuthHeader",
    "xAmzId2": "q6xhNJYmhg",
    "bytesTransferredOut": 1815,
    "availabilityZone": "usw2-az1"
},
"requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
"eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
"readOnly": true,
"resources": [
    {
        "type": "AWS::S3Express::Object",
        "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-az1--x-s3"
    },
    {
        "accountId": "111122223333"
        "type": "AWS::S3Express::DirectoryBucket",
        "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-az1--x-s3"
    }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "111122223333",
"eventCategory": "Data",
"tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-west-2.amazonaws.com"
}
}

```

Per utilizzare le operazioni API endpoint di zona (operazioni a livello di oggetto o di piano dati), è possibile utilizzare l'operazione API `CreateSession` per creare e gestire sessioni ottimizzate per l'autorizzazione a bassa latenza delle richieste di dati. È inoltre possibile utilizzare `CreateSession` per ridurre la quantità di registrazioni. Per identificare quali operazioni API di zona sono state eseguite durante una sessione, è possibile far corrispondere il `accessKeyId` sotto il `responseElements` nel file di log `CreateSession` con il `accessKeyId` nel file di log di altre operazioni API di zona. Per ulteriori informazioni, consulta [Autorizzazione CreateSession](#).

L'esempio seguente mostra un esempio di file di CloudTrail registro che dimostra l'operazione [GetObject](#) API autenticata da `CreateSession`

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI DPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "creationDate": "2024-07-02T00:21:49Z"
      }
    }
  },
  "eventTime": "2024-07-02T00:22:01Z",
  "eventSource": "s3express.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "72.21.198.68",
  "userAgent": "aws-sdk-java/2.25.66 Linux/5.10.216-225.855.amzn2.x86_64
OpenJDK_64-Bit_Server_VM/17.0.11+9-LTS Java/17.0.11 vendor/Amazon.com_Inc. md/internal
exec-env/AWS_Lambda_java17 io/sync http/Apache cfg/retry-mode/legacy",
  "requestParameters": {
    "bucketName": "bucket-base-name--usw2-az1--x-s3",
    "x-amz-checksum-mode": "ENABLED",
    "Host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
    "key": "test-get-obj-with-checksum"
  },
  "responseElements": null,
  "additionalEventData": {
```



```

    "SignatureVersion": "Sigv4",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "bytesTransferredIn": 0,
    "AuthenticationMethod": "AuthHeader",
    "x-amz-id-2": "o0y6w8K7LFsyFN",
    "bytesTransferredOut": 9,
    "availabilityZone": "usw2-az1",
    "sessionModeApplied": "ReadWrite"
  },
  "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
  "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
  "readOnly": true,
  "resources": [
    {
      "type": "AWS::S3Express::Object",
      "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-az1--x-s3"
    },
    {
      "accountId": "111122223333",
      "type": "AWS::S3Express::DirectoryBucket",
      "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-az1--x-s3"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "111122223333",
  "eventCategory": "Data",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-west-2.amazonaws.com"
  }
}

```

Nell'esempio di file di GetObject registro riportato sopra, accessKeyId (AKIAI44QH8DHBEXAMPLE) corrisponde a quello riportato sotto nell'esempio di file di registro. accessKeyId responseElements CreateSession La corrispondenza accessKeyId indica la sessione in cui è stata eseguita l'operazione GetObject.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra un'DeleteObjectsazione su un bucket di directory, richiamato da S3 Lifecycle. Per ulteriori informazioni, consulta [Working with S3 Lifecycle for directory buckets](#).

```
eventVersion:"1.09",
  userIdentity:{

    type:"AWSService",
    invokedBy:"lifecycle.s3.amazonaws.com"
  },
  eventTime:"2024-09-11T00:55:54Z",
  eventSource:"s3express.amazonaws.com",
  eventName:"DeleteObjects",
  awsRegion:"us-east-2",
  sourceIPAddress:"lifecycle.s3.amazonaws.com",
  userAgent:"gamma.lifecycle.s3.amazonaws.com",
  requestParameters:{

    bucketName:"amzn-s3-demo-bucket--use2-az2--x-s3",
    'x-amz-expected-bucket-owner':"637423581905",
    Host:"amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-az2.express.s3.aws.dev",
    delete:"",
    'x-amz-sdk-checksum-algorithm':"CRC32C"
  },
  responseElements:null,
  additionalEventData:{

    SignatureVersion:"Sigv4",
    CipherSuite:"TLS_AES_128_GCM_SHA256",
    bytesTransferredIn:41903,
    AuthenticationMethod:"AuthHeader",
    'x-amz-id-2':"9H5YWZY0",
    bytesTransferredOut:35316,
    availabilityZone:"use2-az2",
    sessionModeApplied:"ReadWrite"
  },
  requestID:"011eeadd04000191",
  eventID:"d3d8b116-219d-4ee6-a072-5f9950733c74",
  readOnly:false,
  resources:[

    {
```

```

    type:"AWS::S3Express::Object",
    ARNPrefix:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--
use2-az2--x-s3/"
  },
  {
    accountId:"637423581905",
    type:"AWS::S3Express::DirectoryBucket",
    ARN:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--use2-
az2--x-s3"
  }
],
eventType:"AwsApiCall",
managementEvent:false,
recipientAccountId:"637423581905",
sharedEventID:"59f877ac-1dd9-415d-b315-9bb8133289ce",
eventCategory:"Data"
}

```

L'esempio seguente mostra una voce di CloudTrail registro che dimostra una Access Denied richiesta su un'azione richiamata da S3 Lifecycle. CreateSession Per ulteriori informazioni, consulta [CreateSession](#).

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "gamma.lifecycle.s3.amazonaws.com"
  },
  "eventTime": "2024-09-11T18:13:08Z",
  "eventSource": "s3express.amazonaws.com",
  "eventName": "CreateSession",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "gamma.lifecycle.s3.amazonaws.com",
  "userAgent": "gamma.lifecycle.s3.amazonaws.com",
  "errorCode": "AccessDenied",
  "errorMessage": "Access Denied",
  "requestParameters": {
    "bucketName": "amzn-s3-demo-bucket--use2-az2--x-s3",
    "Host": "amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-
az2.express.s3.aws.dev",
    "x-amz-create-session-mode": "ReadWrite",
    "x-amz-server-side-encryption": "AES256"
  }
}

```

```

},
"responseElements": null,
"additionalEventData": {
  "SignatureVersion": "Sigv4",
  "CipherSuite": "TLS_AES_128_GCM_SHA256",
  "bytesTransferredIn": 0,
  "AuthenticationMethod": "AuthHeader",
  "x-amz-id-2": "zuDDC1VNbC4LoNwUIc5",
  "bytesTransferredOut": 210,
  "availabilityZone": "use2-az2"
},
"requestID": "010932f174000191e24a0",
"eventID": "dce7cc46-4cd3-46c0-9a47-d1b8b70e301c",
"readOnly": true,
"resources": [{
  "type": "AWS::S3Express::Object",
  "ARNPrefix": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3/"
},
{
  "accountId": "637423581905",
  "type": "AWS::S3Express::DirectoryBucket",
  "ARN": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
}
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "637423581905",
"sharedEventID": "da96b5bd-6066-4a8d-ad8d-f7f427ca7d58",
"eventCategory": "Data"
}

```

Metriche di monitoraggio con Amazon per i bucket di directory CloudWatch

CloudWatch Le metriche di Amazon per i bucket di directory possono aiutarti a comprendere e migliorare le prestazioni delle applicazioni che utilizzano i bucket di directory. Esistono diversi set di CloudWatch metriche che puoi utilizzare con i bucket di directory per la classe di storage S3 Express

One Zone e la classe di archiviazione S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA) in una zona locale.

Metriche di archiviazione giornaliere

Monitora la quantità di dati archiviati nei bucket di directory, inclusa la dimensione totale in byte e il numero di oggetti. Queste metriche di archiviazione per S3 Express One Zone vengono riportate una volta al giorno e vengono fornite a tutti i clienti senza costi aggiuntivi.

Metriche di richiesta

Monitora le richieste dei bucket di directory per identificare e intervenire rapidamente sui problemi operativi. I parametri sono disponibili a intervalli di 1 minuto dopo una determinata latenza di elaborazione. Queste CloudWatch metriche vengono fatturate alla stessa tariffa delle metriche personalizzate di Amazon CloudWatch . Per informazioni sui CloudWatch prezzi, consulta [i prezzi di Amazon. CloudWatch](#) . Per informazioni su come ottenere questi parametri, consulta [Configurazione delle metriche delle richieste per i bucket di directory](#).

Quando sono abilitati, i parametri della richiesta vengono indicati per tutte le operazioni sull'oggetto. Per impostazione predefinita, queste metriche da 1 minuto sono disponibili a livello di bucket di directory. Puoi anche definire un filtro per le metriche utilizzando una directory o un punto di accesso condiviso:

- **Punto di accesso:** i punti di accesso sono denominati endpoint di rete collegati a bucket di directory e semplificano la gestione dell'accesso ai dati su larga scala per i set di dati condivisi in S3. Con il filtro del punto di accesso, puoi ottenere informazioni dettagliate sull'utilizzo del punto di accesso. Per ulteriori informazioni sui punti di accesso per bucket di directory, consulta [Gestione dell'accesso ai set di dati condivisi in bucket di directory con punti di accesso](#).
- **Directory:** i bucket di directory utilizzano le directory effettive per organizzare gli oggetti gerarchicamente. Una directory consente di raggruppare oggetti simili in un bucket di directory. Se si filtra per directory, gli oggetti archiviati nella stessa directory vengono inclusi nella configurazione delle metriche.

Per allineare queste metriche a specifiche applicazioni aziendali, flussi di lavoro o organizzazioni interne, puoi filtrare in base a una directory o a un punto di accesso condiviso.

Tutte le CloudWatch statistiche vengono conservate per un periodo di 15 mesi in modo da poter accedere alle informazioni cronologiche e avere una prospettiva migliore sulle prestazioni dell'applicazione o del servizio web. Per ulteriori informazioni CloudWatch, consulta [Cos'è Amazon CloudWatch?](#) nella Guida per CloudWatch l'utente di Amazon. Potresti aver bisogno di alcune

configurazioni aggiuntive per i tuoi CloudWatch allarmi, a seconda dei casi d'uso. Ad esempio, puoi utilizzare un'espressione matematica metrica per creare un allarme. Per ulteriori informazioni, consulta [Use CloudWatch metrics](#), [Use metric math](#), [Using Amazon CloudWatch alarms](#) e [Create a CloudWatch alarm based on a metric math expression nella Amazon User Guide](#). CloudWatch

Best-effort CloudWatch consegna delle metriche

CloudWatch le metriche vengono fornite con il massimo impegno possibile. La maggior parte delle richieste per un oggetto Amazon S3 con metriche di richiesta comportano l'invio di un punto dati a CloudWatch.

La completezza e la tempestività dei parametri non è garantita. È possibile che il data point per una richiesta specifica venga restituito con un timestamp successivo a quello del momento effettivo di elaborazione della richiesta. Il data point potrebbe subire un ritardo di un minuto prima di essere disponibile oppure potrebbe non essere consegnato affatto. CloudWatch le metriche relative alle richieste ti danno un'idea della natura del traffico diretto verso il tuo bucket in tempo quasi reale, ma non intendono essere un resoconto completo di tutte le richieste.

Dalla natura best-effort di questa funzione deriva che i report disponibili nella [dashboard di gestione dei costi e della fatturazione](#) potrebbero includere una o più richieste di accesso che non compaiono nelle metriche del bucket.

Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

- [Metriche e dimensioni per i bucket di directory](#)
- [Configurazione delle metriche delle richieste per i bucket di directory](#)

Metriche e dimensioni per i bucket di directory

Le metriche e le dimensioni che S3 Express One Zone invia ad Amazon CloudWatch sono elencate nelle tabelle seguenti.

Best-effort CloudWatch consegna delle metriche

CloudWatch le metriche vengono fornite con il massimo impegno possibile. La maggior parte delle richieste per un oggetto Amazon S3 con metriche di richiesta comportano l'invio di un punto dati a CloudWatch.

La completezza e la tempestività dei parametri non è garantita. È possibile che il data point per una richiesta specifica venga restituito con un timestamp successivo a quello del momento effettivo di elaborazione della richiesta. Il data point potrebbe subire un ritardo di un minuto prima di essere disponibile oppure potrebbe non essere consegnato affatto. CloudWatch CloudWatch le metriche relative alle richieste ti danno un'idea della natura del traffico diretto verso il tuo bucket in tempo quasi reale, ma non intendono essere un resoconto completo di tutte le richieste.

Dalla natura best-effort di questa funzione deriva che i report disponibili nella [dashboard di gestione dei costi e della fatturazione](#) potrebbero includere una o più richieste di accesso che non compaiono nelle metriche del bucket.

Argomenti

- [Metriche di archiviazione giornaliera di Amazon S3 per i bucket di directory in CloudWatch](#)
- [Metriche di richiesta di Amazon S3 per i bucket di directory in CloudWatch](#)
- [Dimensioni Amazon S3 per i bucket di directory](#)

Metriche di archiviazione giornaliera di Amazon S3 per i bucket di directory in CloudWatch

Il AWS/S3 namespace include le seguenti metriche di archiviazione giornaliera per i bucket di directory.

Metrica	Description
BucketSizeBytes	<p>La quantità di dati in byte archiviata in un bucket di directory. Questo valore viene calcolato sommando le dimensioni di tutti gli oggetti e i metadati (ad esempio i nomi dei bucket) nel bucket, inclusa la dimensione di tutte le parti per tutti i caricamenti multiparte incompleti nel bucket.</p> <p>Unità: byte</p> <p>Statistiche valide: media</p>
NumberOfObjects	<p>Il numero totale di oggetti archiviati in un bucket di directory. Questo valore viene calcolato contando tutti gli oggetti nel bucket e non include i caricamenti multiparte incompleti nel bucket.</p> <p>Unità: numero</p>

Metrica	Description
	Statistiche valide: media

Metriche di richiesta di Amazon S3 per i bucket di directory in CloudWatch

Il AWS/S3 namespace include le seguenti metriche di richiesta per i bucket di directory.

Metrica	Description
AllRequests	<p>Il numero totale di richieste HTTP effettuate a un bucket di directory, indipendentemente dal tipo. Se utilizzi la configurazione di una metrica con un filtro, questa metrica restituisce solo le richieste HTTP che soddisfano i requisiti del filtro.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
GetRequests	<p>Il numero di GET richieste HTTP effettuate per oggetti in un bucket di directory. Non sono incluse le operazioni LIST. Questa metrica viene incrementata per l'origine di ogni richiesta CopyObject .</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p> <div> Note Le richieste impaginate orientate agli elenchi, come ListMultiPartUploads, e altre ListParts, non sono incluse in questa metrica.</div>
PutRequests	<p>Il numero di PUT richieste HTTP effettuate per oggetti in un bucket di directory. Questa metrica viene incrementata per la destinazione di ogni richiesta CopyObject .</p> <p>Unità: numero</p>

Metrica	Description
	Statistiche valide: somma
DeleteRequests	<p>Il numero di DELETE richieste HTTP effettuate per oggetti in un bucket di directory. Questa metrica include anche DeleteObjects richieste. Questa metrica mostra il numero di richieste effettuate e non il numero di oggetti eliminati.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
HeadRequests	<p>Il numero di HEAD richieste HTTP effettuate a un bucket di directory.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
PostRequests	<p>Il numero di POST richieste HTTP effettuate a un bucket di directory.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p> <div> Note DeleteObjects le richieste non sono incluse in questa metrica.</div>
ListRequests	<p>Il numero di richieste HTTP che elencano il contenuto di un bucket di directory.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>

Metrica	Description
BytesDownloaded	<p>Il numero di byte scaricati per le richieste effettuate in un bucket di directory, in cui la risposta include un corpo.</p> <p>Unità: byte</p> <p>Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo, massimo (come p100), qualsiasi percentile tra p0,0 e p99,9</p>
BytesUploaded	<p>Il numero di byte caricati per le richieste effettuate in un bucket di directory, in cui la richiesta include un corpo.</p> <p>Unità: byte</p> <p>Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo, massimo (come p100), qualsiasi percentile tra p0,0 e p99,9</p>
4xxErrors	<p>Il numero di richieste di codice di stato di errore del client HTTP 4 xx effettuate a un bucket di directory con un valore pari a 0 o 1. La statistica Average (Media) mostra la frequenza degli errori, mentre la statistica Sum (Somma) mostra il conteggio per un tipo specifico di errore, per ogni periodo.</p> <p>Unità: numero</p> <p>Statistiche valide: media (report per richiesta), somma (report per periodo), minimo, massimo, numero di esempi</p>

Metrica	Description
5xxErrors	<p>Il numero di richieste di codice di stato di errore del server HTTP 5xx effettuate a un bucket di directory con un valore 0 o 1. La statistica Average (Media) mostra la frequenza degli errori, mentre la statistica Sum (Somma) mostra il conteggio per un tipo specifico di errore, per ogni periodo.</p> <p>Unità: numero</p> <p>Statistiche valide: media (report per richiesta), somma (report per periodo), minimo, massimo, numero di esempi</p>
FirstByteLatency	<p>Il tempo per richiesta che intercorre tra la ricezione della richiesta completa da parte di un bucket di directory e il momento in cui la risposta inizia a essere restituita.</p> <p>Unità: millisecondi</p> <p>Statistiche valide: Average (Media), Sum (Somma), Min (Minimo), Max (Massimo) (come p100), Sample Count (Numero di esempi), qualsiasi percentile tra p0,0 e p100</p>
TotalRequestLatency	<p>Il tempo trascorso per richiesta dal primo byte ricevuto all'ultimo byte inviato a un bucket di directory. Questa metrica include il tempo necessario per ricevere il corpo della richiesta e inviare il corpo della risposta, non incluso in FirstByteLatency .</p> <p>Unità: millisecondi</p> <p>Statistiche valide: Average (Media), Sum (Somma), Min (Minimo), Max (Massimo) (come p100), Sample Count (Numero di esempi), qualsiasi percentile tra p0,0 e p100</p>

Dimensioni Amazon S3 per i bucket di directory

Le seguenti dimensioni vengono utilizzate per filtrare le metriche di Amazon S3 per i bucket di directory.

Dimensione	Description
BucketName	Questa dimensione filtra i dati richiesti solo per il bucket di directory identificato.
FilterId	Questa dimensione filtra le configurazioni delle metriche specificate per le metriche di richiesta in un bucket di directory. Il filtro di configurazione delle metriche viene impostato quando si configurano le metriche delle richieste. Per ulteriori informazioni, consulta Configurazione delle metriche delle richieste per i bucket di directory .

Configurazione delle metriche delle richieste per i bucket di directory

Puoi configurare le metriche delle richieste per i bucket di directory per monitorare le prestazioni operative del tuo storage S3 Express One Zone. Le metriche delle richieste sono disponibili a intervalli di 1 minuto e consentono di identificare e risolvere rapidamente i problemi operativi.

Puoi configurare le metriche delle richieste per i bucket di directory utilizzando la console Amazon S3, la AWS Command Line Interface (AWS CLI) o l'API REST di Amazon S3.

Utilizzo della console S3

Puoi utilizzare la console Amazon S3 per configurare le metriche delle richieste per i tuoi bucket di directory.

Per configurare le metriche delle richieste per un bucket di directory

1. Accedi e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Nell'elenco dei bucket, scegli il nome del bucket di directory che contiene gli oggetti per i quali desideri richiedere le metriche.
4. Seleziona la scheda Parametri.
5. In Bucket metrics (Parametri bucket) scegli View additional charts (Visualizza grafici aggiuntivi).
6. Scegli la scheda Request metrics (Parametri di richiesta).
7. Scegli Create Filter (Crea filtro).
8. Nella casella Filter name (Nome filtro) immettere il nome del filtro.

I nomi possono contenere solo lettere, numeri, punti, trattini e caratteri di sottolineatura. Si consiglia di utilizzare il nome `EntireBucket` per un filtro che si applica a tutti gli oggetti.

9. In Ambito del filtro, scegli una delle seguenti opzioni:

- Questo filtro si applica a tutti gli oggetti del bucket: non è necessario specificare un filtro.
- Limita l'ambito di questo filtro utilizzando la directory o il punto di accesso: specifichi un filtro. Per limitare l'ambito, è possibile filtrare per directory o punto di accesso.

Puoi anche definire un filtro in modo che le metriche vengano raccolte e riportate solo su un sottoinsieme di oggetti nel bucket di directory.

10. Se hai scelto di limitare l'ambito del filtro, specifica i dettagli del filtro:

- Per filtrare in base alla directory, immettete il nome della directory.
- Per filtrare in base al punto di accesso, inserisci l'ARN del punto di accesso.

11. Scegli **Save changes** (Salva modifiche).

12. Nella scheda **Request metrics** (Parametri di richiesta), in **Filters** (Filtri), scegliere il filtro appena creato.

Dopo circa 15 minuti, CloudWatch inizia a tracciare queste metriche di richiesta. Puoi visualizzarli nella scheda **Request metrics** (Parametri di richiesta). Puoi visualizzare i grafici delle metriche su Amazon S3 o sulla console. CloudWatch Le metriche delle richieste vengono fatturate alla tariffa standard. CloudWatch Per ulteriori informazioni, consulta i prezzi di [Amazon CloudWatch](#).

Utilizzo di AWS CLI

Puoi utilizzare AWS CLI per configurare le metriche delle richieste per i tuoi bucket di directory.

1. Installa e configura il. AWS CLI Per le istruzioni, consulta [Installazione, aggiornamento e disinstallazione della AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface.
2. Aprire un terminale.
3. Eseguire il comando riportato di seguito per aggiungere una configurazione di parametro.

```
aws s3api put-bucket-metrics-configuration --endpoint https://s3express-control.region-code.amazonaws.com --bucket directory-bucket-name --id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id"}'
```

Utilizzo della REST API

Puoi utilizzare l'API REST di Amazon S3 per configurare le metriche delle richieste per i tuoi bucket di directory. Quando si utilizza l'API REST con bucket di directory, è necessario utilizzare l'endpoint S3 Express One Zone con l'endpoint di controllo regionale nel formato: `https://s3express-control.region-code.amazonaws.com`

Per ulteriori informazioni sulle operazioni dell'API REST, consulta i seguenti argomenti nell'Amazon S3 API Reference:

- [Metriche PUT Bucket](#)
- [Metriche GET Bucket](#)
- [ELIMINA le metriche Bucket](#)
- [Elenca le metriche di Bucket](#)

Ottimizzazione delle prestazioni del bucket della directory

Per ottenere le migliori prestazioni quando si utilizzano i bucket di directory, si consiglia di seguire le seguenti linee guida.

Per ulteriori informazioni sulle best practice per S3 Express One Zone, consulta [Best practice per ottimizzare le prestazioni di S3 Express One Zone](#).

Utilizzo dell'autenticazione basata sulla sessione

I bucket di directory supportano un nuovo meccanismo di autorizzazione basato sulla sessione per autenticare e autorizzare le richieste a un bucket di directory. Con l'autenticazione basata sulla sessione, AWS gli SDK utilizzano automaticamente l'operazione `CreateSession` API per creare un token di sessione temporaneo che può essere utilizzato per l'autorizzazione a bassa latenza delle richieste di dati a un bucket di directory.

Gli AWS SDK utilizzano l'operazione `CreateSession` API per richiedere credenziali temporanee, quindi creano e aggiornano automaticamente i token per te per tuo conto ogni 5 minuti. Per sfruttare i vantaggi prestazionali dei bucket di directory, ti consigliamo di utilizzare gli AWS SDK per avviare e gestire la richiesta API `CreateSession`. Per ulteriori informazioni sul modello basato sulla sessione, consulta [Autorizzazione delle operazioni API dell'endpoint di zona con `CreateSession`](#).

Best practice per il checksum S3 aggiuntivo

I bucket di directory offrono la possibilità di scegli l'algoritmo di checksum utilizzato per convalidare i dati durante il caricamento o il download. Puoi selezionare uno dei seguenti algoritmi di controllo dell'integrità dei dati Secure Hash Algorithms (SHA) o Cyclic Redundancy Check (CRC): CRC32, CRC32C e SHA-1 SHA-256 MD5-based i checksum non sono supportati con la classe di storage S3 Express One Zone.

CRC32 è il checksum predefinito utilizzato dagli AWS SDK per la trasmissione di dati da o verso bucket di directory. Si consiglia di utilizzare CRC32 e CRC32C per ottenere le migliori prestazioni con i bucket di directory.

Usa l'ultima versione di AWS SDK e librerie di runtime comuni

Molti AWS SDK forniscono anche le librerie AWS Common Runtime (CRT) per accelerare ulteriormente le prestazioni nei client S3. Questi SDK includono AWS SDK for Java 2.x, AWS SDK per C++ e AWS SDK per Python (Boto3). Il client CRT-based S3 trasferisce oggetti da e verso bucket di directory con prestazioni e affidabilità migliorate utilizzando automaticamente l'operazione API di caricamento in più parti e il recupero dell'intervallo di byte per automatizzare le connessioni con ridimensionamento orizzontale.

Per ottenere le massime prestazioni con i bucket di directory, consigliamo di utilizzare l'ultima versione degli AWS SDK che includono le librerie CRT o di utilizzare (). AWS Command Line Interface AWS CLI

Sviluppo con i bucket di directory

Dopo aver creato il bucket della directory, è possibile iniziare immediatamente a leggere e scrivere a bassa latenza. Puoi comunicare con il bucket di directory mediante una connessione endpoint su un cloud privato virtuale (VPC) oppure puoi utilizzare le operazioni API zonali e regionali per gestire oggetti e bucket di directory. Puoi lavorare con i bucket di directory utilizzando gli AWS SDK, la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI) e le API REST di Amazon S3.

Argomenti

- [Endpoint regionali e di zona per i bucket di directory](#)
- [Lavorare con i bucket di directory utilizzando la console S3, AWS CLI e AWS SDK](#)
- [Operazioni API del bucket della directory](#)

Endpoint regionali e di zona per i bucket di directory

Per accedere agli endpoint regionali e di zona per i bucket di directory dal cloud privato virtuale (VPC), è possibile utilizzare gli endpoint VPC gateway. Dopo aver creato un endpoint gateway, è possibile aggiungerlo come destinazione nella tabella di routing per il traffico destinato dal VPC al bucket. L'utilizzo di endpoint gateway non comporta costi supplementari. Per ulteriori informazioni su come configurare gli endpoint VPC del gateway, consulta [Collegamento in rete per i bucket di directory](#).

Bucket-level Le operazioni API (piano di controllo) sono disponibili tramite un endpoint regionale e sono denominate operazioni API per endpoint regionali. Esempi di operazioni API degli endpoint regionali sono `CreateBucket` e `DeleteBucket`.

Per caricare e gestire gli oggetti si utilizza l'opzione Zonale (livello di oggetto o operazioni API endpoint del piano dati). Le operazioni API degli endpoint zonali sono disponibili tramite un endpoint zonale. Esempi di operazioni API zonali sono `PutObject` e `CopyObject`.

Per ulteriori informazioni sugli endpoint regionali e di zona per i bucket di directory nelle zone di disponibilità, consulta [Endpoint regionali e di zona per i bucket di directory in una zona di disponibilità](#).

Per ulteriori informazioni sugli endpoint regionali e di zona per i bucket di directory nelle Zone locali, consulta [Concetti per i bucket di directory nelle Zone locali](#).

Lavorare con i bucket di directory utilizzando la console S3, AWS CLI e AWS SDK

Puoi lavorare con la classe di storage e i bucket di directory S3 Express One Zone utilizzando gli AWS SDK, la console Amazon S3, AWS Command Line Interface (AWS CLI) e l'API REST di Amazon S3.

Console S3

Per iniziare a utilizzare la console S3, completa la procedura seguente:

- [Creazione di bucket di directory in una zona di disponibilità](#)
- [Svuotamento di un bucket di directory](#)
- [Eliminazione di un bucket di directory](#)

Per un'esercitazione completa, consulta [Esercitazione: come iniziare con S3 Express One Zone](#).

AWS SDK

S3 Express One Zone supporta i seguenti SDK: AWS

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK for Java 2.x
- AWS SDK per JavaScript v3
- AWS SDK per .NET
- AWS SDK per PHP
- AWS SDK per Python (Boto3)
- AWS SDK per Ruby
- AWS SDK per Kotlin
- AWS SDK per Rust

Quando si utilizza S3 Express One Zone, si consiglia di utilizzare la versione più recente degli SDK AWS . Gli AWS SDK supportati per S3 Express One Zone gestiscono l'avvio, l'aggiornamento e la chiusura della sessione per conto dell'utente. Ciò significa che puoi iniziare immediatamente a utilizzare le operazioni API dopo aver scaricato e installato gli AWS SDK e aver configurato le autorizzazioni IAM necessarie. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).

Per informazioni sugli AWS SDK, incluso come scaricarli e installarli, consulta [Tools to Build on. AWS](#)

Per esempi di AWS SDK, consulta quanto segue:

- [Creazione di bucket di directory in una zona di disponibilità](#)
- [Svuotamento di un bucket di directory](#)
- [Eliminazione di un bucket di directory](#)

AWS Command Line Interface (AWS CLI)

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare bucket di directory e utilizzare le operazioni API degli endpoint regionali e zonali supportate per S3 Express One Zone.

Per iniziare con AWS CLI, vedi [Guida introduttiva a AWS CLI](#) nel Command Reference. AWS CLI

Note

Per utilizzare i bucket di directory con i `aws s3` comandi di [alto livello](#), aggiorna il tuo AWS CLI alla versione più recente. Per ulteriori informazioni su come installare e configurare AWS CLI, consulta [Installare o aggiornare la versione più recente di AWS CLI](#) nel AWS CLI Command Reference.

Per AWS CLI alcuni esempi, vedere quanto segue:

- [Creazione di bucket di directory in una zona di disponibilità](#)
- [Svuotamento di un bucket di directory](#)
- [Eliminazione di un bucket di directory](#)

Operazioni API del bucket della directory

Per gestire i bucket della directory, è possibile utilizzare le operazioni API endpoint regionali (a livello di bucket o di piano di controllo (control-plane)). Per gestire gli oggetti nei bucket della directory, è possibile utilizzare le operazioni API endpoint di zona (a livello di oggetto o di piano dati). Per ulteriori informazioni, consulta [Collegamento in rete per i bucket di directory](#) e [Endpoint ed endpoint VPC del gateway](#).

Operazioni API degli endpoint regionali

Le seguenti operazioni API dell'endpoint regionale sono supportate per i bucket di directory:

- [CreateAccessPoint](#)
- [CreateBucket](#)
- [DeleteAccessPoint](#)
- [DeleteAccessPointPolicy](#)
- [DeleteAccessPointScope](#)
- [DeleteBucket](#)
- [DeleteBucketInventoryConfiguration](#)
- [DeleteBucketLifecycle](#)

- [DeleteBucketPolicy](#)
- [GetAccessPoint](#)
- [GetAccessPointPolicy](#)
- [GetAccessPointScope](#)
- [GetBucketInventoryConfiguration](#)
- [GetBucketLifecycleConfiguration](#)
- [GetBucketPolicy](#)
- [ListAccessPointsForDirectoryBuckets](#)
- [ListBucketInventoryConfigurations](#)
- [ListDirectoryBuckets](#)
- [ListTagsForResource](#)
- [PutAccessPointPolicy](#)
- [PutAccessPointScope](#)
- [PutBucketInventoryConfiguration](#)
- [PutBucketLifecycleConfiguration](#)
- [PutBucketPolicy](#)
- [DeleteBucketEncryption](#)
- [GetBucketEncryption](#)
- [PutBucketEncryption](#)
- [TagResource](#)
- [UntagResource](#)

Operazioni API dell'endpoint di zona

Le seguenti operazioni API dell'endpoint di zona sono supportate per i bucket di directory:

- [CreateSession](#)
- [CopyObject](#)
- [DeleteObject](#)
- [DeleteObjects](#)
- [GetObject](#)

- [GetObjectAttributes](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListObjectsV2](#)
- [PutObject](#)
- [RenameObject](#)
- [AbortMultipartUpload](#)
- [CompleteMultiPartUpload](#)
- [CreateMultipartUpload](#)
- [ListMultipartUploads](#)
- [ListParts](#)
- [UploadPart](#)
- [UploadPartCopy](#)

Utilizzo di tag con i bucket di directory S3

Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso i bucket di directory Amazon S3. È possibile applicare i tag ai bucket di directory S3 al momento della creazione o gestire i tag sui bucket di directory esistenti. Per informazioni generali sui tag, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

Note

Non sono previsti costi aggiuntivi per l'utilizzo dei tag sui bucket di directory oltre alle tariffe di richiesta API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Metodi comuni per utilizzare i tag con i bucket di directory

Si utilizzano i tag nei bucket di directory S3 per:

1. Allocazione dei costi: monitorare i costi di archiviazione in base al tag del bucket in Gestione costi e fatturazione AWS. Per ulteriori informazioni, consultare [Utilizzo dei tag per l'allocazione dei costi](#).

2. Attribute-based controllo degli accessi (ABAC): ridimensiona le autorizzazioni di accesso e concedi l'accesso ai bucket di directory S3 in base ai relativi tag. Per ulteriori informazioni, consulta [Utilizzo dei tag per ABAC](#).

Note

È possibile utilizzare gli stessi tag sia per l'allocazione dei costi che per il controllo degli accessi.

ABAC per bucket di directory S3

I bucket di directory Amazon S3 supportano il controllo degli accessi basato su attributi (ABAC) con tag. Utilizza le chiavi di condizione basate su tag nelle policy delle tue AWS organizzazioni, in IAM e nei bucket di directory S3. Per le aziende, ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle policy IAM, è possibile controllare l'accesso ai bucket di directory S3 in base ai tag del bucket utilizzando le seguenti [chiavi di condizione globali](#):

- `aws:ResourceTag/key-name`
 - Utilizzare questa chiave per confrontare la coppia chiave-valore del tag specificata nella policy con la coppia chiave-valore associata alla risorsa. Ad esempio, puoi richiedere che l'accesso a una risorsa sia consentito solo se la risorsa dispone di una chiave di tag `Dept` collegata al valore `Marketing`. Per ulteriori informazioni, consulta [Controllare l'accesso alle AWS risorse](#).
- `aws:RequestTag/key-name`
 - Utilizzare questa chiave per confrontare la coppia chiave-valore del tag passata nella richiesta con la coppia del tag specificata nella policy. Ad esempio, è possibile controllare che la richiesta includa la chiave del tag `Dept` e che abbia il valore `Accounting`. Per ulteriori informazioni, vedere [Controllo dell'accesso durante AWS le richieste](#). È possibile utilizzare questa chiave di condizione per limitare quali coppie chiave-valore di tag possono essere passate durante le operazioni API `TagResource` e `CreateBucket`.
- `aws:TagKeys`
 - Utilizzare questa chiave per confrontare le chiavi dei tag in una richiesta con quelle specificate nella policy. Nell'utilizzo delle policy per controllare gli accessi tramite tag, è consigliabile utilizzare la chiave di condizione `aws:TagKeys` per definire le chiavi di tag ammesse. Per

esempi di policy e ulteriori informazioni, consulta [Controllo dell'accesso in base alle chiavi di tag](#). È possibile creare un bucket di directory S3 con tag. Per consentire il tagging durante l'operazione API `CreateBucket`, è necessario creare una policy che comprende entrambe le azioni `s3express:TagResource` e `s3express>CreateBucket`. È quindi possibile utilizzare la chiave di condizione `aws:TagKeys` per implementare nella richiesta `CreateBucket` specifici tag.

- `s3express:BucketTag/tag-key`
 - Utilizzare questa chiave di condizione per fornire le autorizzazioni a dati specifici in bucket di directory con tag. Quando si accede a un bucket di directory utilizzando un punto di accesso, questa chiave di condizione fa riferimento ai tag del bucket di directory durante l'autorizzazione del punto di accesso e del bucket di directory, mentre `aws:ResourceTag/tag-key` fa riferimento solo ai tag della risorsa per cui viene autorizzata.

Esempi di policy ABAC per bucket di directory

Di seguito sono riportati esempi di policy ABAC per i bucket di directory Amazon S3.

1.1 - Policy IAM per creare o modificare bucket con tag specifici

In questa policy IAM, gli utenti o i ruoli con questa policy possono creare bucket di directory S3 solo se applicano ai bucket i tag con la chiave di tag `project` e il valore di tag `Trinity` nella richiesta di creazione del bucket. Possono anche aggiungere o modificare i tag sui bucket di directory S3 esistenti, purché la richiesta `TagResource` includa la coppia chiave-valore `project:Trinity` del tag. Questa policy non fornisce autorizzazioni di lettura, scrittura o eliminazione sui bucket o sui relativi oggetti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateBucketWithTags",
      "Effect": "Allow",
      "Action": [
        "s3express>CreateBucket",
        "s3express:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```

        "aws:RequestTag/project": [
            "Trinity"
        ]
    }
}
]
}

```

1.2 - Policy di bucket per limitare le operazioni sul bucket con tag

In questa policy di bucket, i principali IAM (utenti e ruoli) possono eseguire operazioni utilizzando l'azione `CreateSession` sul bucket solo se il valore del tag `project` del bucket corrisponde al valore del tag `project` del principale.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowObjectOperations",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3express:CreateSession",
      "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-
bucket--usw2-az1--x-s3",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}

```

1.3 - Policy IAM per modificare i tag sulle risorse esistenti mantenendo la governance dei tag

In questa policy IAM, i principali IAM (utenti o ruoli) possono modificare i tag su un bucket solo se il valore del tag `project` del bucket corrisponde al valore del tag `project` del principale. Solo i quattro tag `project`, `environment`, `owner` e `cost-center` specificati nelle chiavi di condizione `aws:TagKeys` sono consentiti per questi bucket di directory. Ciò aiuta a rafforzare la governance

dei tag, impedisce modifiche non autorizzate dei tag e mantiene lo schema di tagging coerente tra i bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3express:TagResource"
      ],
      "Resource": "arn:aws::s3express:us-west-2:111122223333:bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",
            "owner",
            "cost-center"
          ]
        }
      }
    }
  ]
}
```

1.4 - Utilizzo della chiave s3express: condition BucketTag

In questa policy IAM, l'istruzione di condizione consente l'accesso ai dati del bucket solo se il bucket ha la chiave di tag Environment e il valore di tag Production.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToSpecificAccessPoint",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws::s3express:us-west-2:111122223333:accesspoint/*",
```



```
    "Condition": {
      "StringEquals": {
        "s3express:BucketTag/Environment": "Production"
      }
    }
  ]
}
```

Gestione dei tag per bucket di directory

Puoi aggiungere o gestire tag per i bucket di directory S3 utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI), gli AWS SDK o utilizzando le API S3:, e. [TagResource](#) [UntagResource](#) [ListTagsForResource](#) Per ulteriori informazioni, consulta:

Argomenti

- [Creazione di bucket di directory con tag](#)
- [Aggiunta di un tag a un bucket di directory](#)
- [Visualizzazione dei tag di bucket di directory](#)
- [Eliminazione di un tag da un bucket di directory](#)

Creazione di bucket di directory con tag

È possibile applicare i tag ai bucket di directory Amazon S3 al momento della creazione. Non sono previsti costi aggiuntivi per l'utilizzo dei tag sui bucket di directory oltre alle tariffe di richiesta API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sul tagging dei bucket di directory, consulta [Utilizzo di tag con i bucket di directory S3](#).

Permissions

Per creare un bucket di directory con tag, è necessario disporre delle seguenti autorizzazioni:

- `s3express:CreateBucket`
- `s3express:TagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di creare un bucket di directory con tag, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per creare il bucket di directory e aggiungervi un tag.
- Controllare la policy dell'utente IAM per eventuali condizioni del controllo degli accessi basato su attributi (ABAC). Potrebbe essere necessario etichettare i bucket di directory solo con chiavi e valori di tag specifici. Per ulteriori informazioni, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

Fasi

Puoi creare un bucket di directory con i tag applicati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per creare un bucket di directory con tag utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Per creare un nuovo bucket di directory, scegli Crea bucket.
4. È possibile creare due tipi di bucket di directory:

Un bucket di directory in una zona di disponibilità per un carico di lavoro ad alte prestazioni. Per ulteriori informazioni, consulta [Carichi di lavoro ad alte prestazioni](#).

Un bucket di directory in una zona locale per un carico di lavoro di residenza dei dati. Per ulteriori informazioni, consulta [Carichi di lavoro di residenza dei dati](#).

5. Per entrambi i tipi di bucket di directory, nella pagina Crea bucket, Tag è un'opzione per la creazione di un nuovo bucket di directory.
6. Inserisci un nome per il bucket. Per ulteriori informazioni, consulta [Regole di denominazione dei bucket di directory](#).
7. Scegli Aggiungi nuovo tag per aprire l'editor di tag e inserisci una coppia chiave-valore di tag. La chiave di tag è obbligatoria, mentre il valore è facoltativo.

8. Per aggiungere un altro tag, scegli nuovamente Aggiungi nuovo tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
9. Dopo aver specificato le opzioni per il nuovo bucket di directory, scegli Crea bucket.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come creare un bucket di directory con tag utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.BucketInfo;
import software.amazon.awssdk.services.s3.model.BucketType;
import software.amazon.awssdk.services.s3.model.CreateBucketConfiguration;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.CreateBucketResponse;
import software.amazon.awssdk.services.s3.model.DataRedundancy;
import software.amazon.awssdk.services.s3.model.LocationInfo;
import software.amazon.awssdk.services.s3.model.LocationType;
import software.amazon.awssdk.services.s3.model.Tag;

public class CreateBucketWithTagsExample {
    public static void createBucketWithTagsExample() {
        S3Client s3 = S3Client.builder().region(Region.US_WEST_2).build();

        CreateBucketConfiguration bucketConfiguration =
            CreateBucketConfiguration.builder()
                .location(LocationInfo.builder()
                    .type(LocationType.AVAILABILITY_ZONE)
                    .name("usw2-az1").build())
                .bucket(BucketInfo.builder()
                    .type(BucketType.DIRECTORY)
                    .dataRedundancy(DataRedundancy.SINGLE_AVAILABILITY_ZONE)
                    .build())
                .tags(Tag.builder().key("MyTagKey").value("MyTagValue").build())
                .build();

        CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
            .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3--usw2-az1--x-s3")
            .createBucketConfiguration(bucketConfiguration)
```

```

        .build();

        CreateBucketResponse response = s3.createBucket(createBucketRequest);
        System.out.println("Status code (should be 200):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}

```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la creazione di un bucket di directory con tag, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [CreateBucket](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come creare un bucket di directory con tag utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Quando si crea un bucket di directory, è necessario fornire i dettagli di configurazione e utilizzare la seguente convenzione di denominazione: *bucket-base-name--zone-id--x-s3*

Richiesta:

```

aws s3api create-bucket \
--bucket bucket-base-name--zone-id--x-s3 \
--create-bucket-configuration "Location={Type=AvailabilityZone,Name=zone-id},Bucket={DataRedundancy=SingleAvailabilityZone,Type=Directory},Tags=[{Key=mykey1,Value=myvalue1},{Key=mykey2,Value=myvalue2}]"

```

Risposta:

```

{
  "Location": "http://bucket--use1-az4--x-s3.s3express-use1-az4.us-east-1.amazonaws.com/"
}

```

```
}
```

Aggiunta di un tag a un bucket di directory

È possibile aggiungere tag ai bucket di directory Amazon S3 e modificarli. Non sono previsti costi aggiuntivi per l'utilizzo dei tag sui bucket di directory oltre alle tariffe di richiesta API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sul tagging dei bucket di directory, consulta [Utilizzo di tag con i bucket di directory S3](#).

Permissions

Per aggiungere un tag a un bucket di directory, è necessario disporre della seguente autorizzazione:

- `s3express:TagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di aggiungere un tag a un bucket di directory, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per aggiungere un tag a un bucket di directory.
- Se hai tentato di aggiungere una chiave tag che inizia con il prefisso AWS riservato `aws :`, cambia la chiave del tag e riprova.

Fasi

Puoi aggiungere tag ai bucket di directory utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per aggiungere tag a un bucket di directory utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Scegliere il nome del bucket.

4. Scegliere la scheda Properties (Proprietà).
5. Scorri la sezione Tag e scegli Aggiungi nuovo tag.
6. Viene visualizzata la pagina Aggiungi tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
7. Se si aggiunge un nuovo tag con lo stesso nome di chiave di un tag esistente, il valore del nuovo tag sovrascrive il valore del tag esistente.
8. In questa pagina è anche possibile modificare i valori dei tag esistenti.
9. Dopo aver aggiunto i tag, scegli Salva le modifiche.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come aggiungere tag a un bucket di directory utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;
import software.amazon.awssdk.services.s3control.model.TagResourceResponse;

public class TagResourceExample {
    public static void tagResourceExample() {
        S3ControlClient s3Control =
            S3ControlClient.builder().region(Region.US_WEST_2).build();

        TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
            .resourceArn("arn:aws:s3express:us-west-2:111122223333:bucket/my-
            directory-bucket--usw2-az1--x-s3")
            .accountId("111122223333")
            .tags(Tag.builder().key("MyTagKey").value("MyTagValue").build())
            .build();

        TagResourceResponse response = s3Control.tagResource(tagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'aggiunta di tag a un bucket di directory, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [TagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come aggiungere tag a un bucket di directory utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control tag-resource \  
--account-id 111122223333 \  
--resource-arn arn:aws:s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3 \  
\  
--tags "Key=mykey,Value=myvalue"
```

Risposta:

```
{  
  "ResponseMetadata": {  
    "RequestId": "EXAMPLE123456789",  
    "HTTPStatusCode": 200,  
    "HTTPHeaders": {  
      "date": "Wed, 19 Jun 2025 10:30:00 GMT",  
      "content-length": "0"  
    },  
    "RetryAttempts": 0  
  }  
}
```

Visualizzazione dei tag di bucket di directory

È possibile visualizzare o elencare i tag applicati ai bucket di directory S3. Per ulteriori informazioni sui tag, consulta [Utilizzo di tag con i bucket di directory S3](#).

Permissions

Per visualizzare i tag applicati a un bucket di directory, è necessario disporre della seguente autorizzazione:

- `s3express:ListTagsForResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di elencare o visualizzare i tag di un bucket di directory, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per visualizzare o elencare i tag del bucket di directory.

Fasi

Puoi visualizzare i tag applicati ai bucket di directory utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare i tag applicati a un bucket di directory utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Scegliere il nome del bucket.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag per visualizzare tutti i tag applicati al bucket di directory.
6. La sezione Tag mostra i User-defined tag per impostazione predefinita. Puoi selezionare la scheda dei tag AWS generati per visualizzare i tag applicati al bucket di directory dai AWS servizi.

Utilizzo di AWS SDK

Questa sezione fornisce un esempio di come visualizzare i tag applicati a un bucket di directory utilizzando gli SDK. AWS

SDK for Java 2.x

Questo esempio mostra come visualizzare i tag applicati a un bucket di directory utilizzando AWS SDK for Java 2.x.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResourceExample {
    public static void listTagsForResourceExample() {
        S3ControlClient s3Control =
            S3ControlClient.builder().region(Region.US_WEST_2).build();

        ListTagsForResourceRequest listTagsForResourceRequest =
            ListTagsForResourceRequest.builder()
                .resourceArn("arn:aws:s3express:us-west-2:111122223333:bucket/my-
directory-bucket--usw2-az1--x-s3")
                .accountId("111122223333")
                .build();

        ListTagsForResourceResponse response =
            s3Control.listTagsForResource(listTagsForResourceRequest);
        System.out.println("Tags on my resource:");
        System.out.println(response.toString());
    }
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la visualizzazione dei tag applicati a un bucket di directory, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [ListTagsforResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

L'esempio della CLI seguente mostra come visualizzare i tag applicati a un bucket di directory. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control list-tags-for-resource \  
--account-id 111122223333 \  
--resource-arn arn:aws:s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3  
\  

```

Risposta con tag:

```
{  
  "Tags": [  
    {  
      "Key": "MyKey1",  
      "Value": "MyValue1"  
    },  
    {  
      "Key": "MyKey2",  
      "Value": "MyValue2"  
    },  
    {  
      "Key": "MyKey3",  
      "Value": "MyValue3"  
    }  
  ]  
}
```

Risposta senza tag:

```
{  
  "Tags": []  
}
```

Eliminazione di un tag da un bucket di directory

È possibile rimuovere i tag dai bucket di directory S3. Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso i bucket di directory Amazon S3. Per ulteriori informazioni sui tag, consulta [Utilizzo di tag con i bucket di directory S3](#).

Note

Se si elimina un tag e in seguito si scopre che veniva utilizzato per monitorare i costi o per il controllo degli accessi, è possibile aggiungere nuovamente il tag al bucket di directory.

Permissions

Per eliminare un tag da un bucket di directory, è necessario disporre della seguente autorizzazione:

- `s3express:UntagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di eliminare un tag da un bucket di directory, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per eliminare un tag da un bucket di directory.

Fasi

Puoi eliminare i tag dai bucket di directory utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per eliminare i tag da un bucket di directory utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di directory.
3. Scegliere il nome del bucket.
4. Scegliere la scheda Properties (Proprietà).

5. Scorri fino alla sezione Tag e seleziona la casella di controllo accanto al tag o ai tag che desideri eliminare.
6. Scegliere Elimina.
7. Viene visualizzato il pop-up Elimina tag definiti dall'utente che chiede di confermare l'eliminazione del tag o dei tag selezionati.
8. Seleziona Elimina per confermare.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come eliminare i tag da un bucket di directory utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;
import software.amazon.awssdk.services.s3control.model.UntagResourceResponse;

public class UntagResourceExample {
    public static void untagResourceExample() {
        S3ControlClient s3Control =
            S3ControlClient.builder().region(Region.US_WEST_2).build();

        UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
            .resourceArn("arn:aws:s3express:us-west-2:111122223333:bucket/my-
directory-bucket--usw2-az1--x-s3")
            .accountId("111122223333")
            .tagKeys("myTagKey")
            .build();

        UntagResourceResponse response =
            s3Control.untagResource(untagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'eliminazione di tag da un bucket di directory, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [UnTagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come eliminare i tag da un bucket di directory utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control untag-resource \  
--account-id 111122223333 \  
--resource-arn arn:aws:s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3 \  
\  
--tag-keys "tagkey1" "tagkey2"
```

Risposta:

```
{  
  "ResponseMetadata": {  
    "RequestId": "EXAMPLE123456789",  
    "HTTPStatusCode": 204,  
    "HTTPHeaders": {  
      "date": "Wed, 19 Jun 2025 10:30:00 GMT",  
      "content-length": "0"  
    },  
    "RetryAttempts": 0  
  }  
}
```

Test di resilienza in S3 Express One Zone

La classe di storage Amazon S3 Express One Zone supporta i test di resilienza con AWS Fault Injection Service (AWS FIS), un servizio completamente gestito per eseguire esperimenti di iniezione di guasti sui carichi di lavoro. AWS Con AWS FIS, puoi simulare le interruzioni della connettività dei bucket di directory, causando il timeout delle operazioni delle API degli endpoint zonali (a livello di oggetto o piano dati), come accadrebbe durante un'interruzione della zona di disponibilità.

Questi esperimenti consentono di:

- verificare che i sistemi di monitoraggio siano in grado di rilevare i problemi di accesso di S3 Express One Zone;
- testare e rafforzare i processi di ripristino;
- verificare che i meccanismi di failover delle applicazioni funzionino come previsto;
- garantire che il tempo di ripristino delle applicazioni soddisfi gli obiettivi del livello di servizio (SLO) e gli accordi sul livello di servizio (SLA) dell'organizzazione.

Testando la risposta dell'applicazione alle interruzioni simulate, ci si prepara meglio all'improbabile eventualità di un'effettiva interruzione della zona di disponibilità che influisca sull'accesso ai dati in S3 Express One Zone.

Come funziona

Il test utilizza l'azione `aws:network:disrupt-connectivity` con l'ambito impostato su S3 Express. Questa azione interrompe la connettività di rete agli endpoint S3 Express One Zone, causando il timeout delle richieste ai bucket di directory.

È possibile indicare le sottoreti in cui sono in esecuzione le applicazioni o gli endpoint VPC del gateway utilizzati per accedere a S3 Express One Zone. Per ulteriori informazioni, consulta [Disponibilità AZ: interruzione di corrente](#) nella Guida per l'utente di AWS Fault Injection Service .

Per testare la resilienza delle applicazioni che archiviano dati in S3 Express One Zone, consulta [Simulazione di un evento di connettività](#) nella Guida per l'utente di AWS Fault Injection Service .

Considerazioni e limitazioni

Tieni presente le seguenti considerazioni e limitazioni per le interruzioni di connettività nella classe di archiviazione Amazon S3 Express One Zone:

Considerazioni

- **Autorizzazioni IAM:** per utilizzarlo AWS FIS con S3 Express One Zone, è necessario configurare un ruolo IAM con le autorizzazioni appropriate. Per ulteriori informazioni sui AWS FIS ruoli, consulta [Creare un ruolo IAM per AWS FIS](#) nella Guida per l'AWS Fault Injection Service utente. È consigliabile assegnare queste autorizzazioni solo alle risorse necessarie.
- **Risoluzione della destinazione:** le destinazioni vengono risolte all'inizio dell'esperimento. Se durante l'esperimento viene eliminato un endpoint VPC di un gateway o una sottorete di destinazione, l'esperimento non riesce.
- **Impatto sulle risorse condivise:** se più applicazioni condividono le stesse sottoreti o gli stessi endpoint VPC del gateway, tutto il traffico verso S3 Express One Zone proveniente da queste applicazioni è interessato durante l'esperimento.
- **Comportamento di rollback:** al termine dell' AWS FIS azione, la connettività viene ripristinata automaticamente e le richieste riprenderanno l'operazione prevista senza intervento manuale.
- **Condizioni di arresto:** configura gli CloudWatch allarmi appropriati come condizioni di arresto per interrompere automaticamente gli esperimenti in caso di impatti imprevisti.

Limitazioni

- **Selezione della destinazione:** non è possibile definire come destinazione bucket di directory S3 specifici. L'azione ha effetto su tutti i bucket di directory a cui si accede tramite i componenti di rete di destinazione.
- **Obiettivi massimi:** esiste un numero massimo di sottoreti che puoi scegliere come target per azione. AWS FIS Per maggiori informazioni, consulta [Service Quotas di AWS Fault Injection Service](#) nella Guida per l'utente di AWS FIS .
- **Metodi di accesso:** l' AWS FIS azione influisce solo sulle richieste effettuate tramite Internet o gli endpoint del cloud privato virtuale (VPC) del gateway. Le richieste provenienti dagli endpoint VPC dell'interfaccia (AWS PrivateLink) non sono supportate.
- **Disponibilità regionale:** questa funzionalità è disponibile solo nelle [Regioni AWS in cui è supportato S3 Express One Zone](#).

Utilizzo di Tabelle Amazon S3 e dei bucket di tabelle

Tabelle Amazon S3 fornisce uno storage S3 ottimizzato per i carichi di lavoro di analisi, con funzionalità progettate per migliorare continuamente le prestazioni delle query e ridurre i costi di storage per le tabelle. Le tabelle S3 sono progettate appositamente per l'archiviazione di dati tabulari, come le transazioni di acquisto giornaliere, i dati dei sensori di streaming o le impressioni degli annunci. I dati tabulari rappresentano i dati in colonne e righe, come in una tabella di database.

I dati in Tabelle S3 sono archiviati in un nuovo tipo di bucket: un bucket di tabelle, che archivia le tabelle come sottorisorse. I bucket di tabelle supportano l'archiviazione delle tabelle nel formato Apache Iceberg. Utilizzando istruzioni SQL standard, è possibile eseguire query sulle tabelle con motori di query che supportano Iceberg, come Amazon Athena, Amazon Redshift e Apache Spark.

Argomenti

- [Funzionalità di Tabelle S3](#)
- [Servizi correlati](#)
- [Tutorial: Nozioni di base su Tabelle S3](#)
- [Secchi da tavolo](#)
- [Manutenzione di Tabelle S3](#)
- [Ottimizzazione dei costi per tabelle con Intelligent-Tiering](#)
- [Spazi dei nomi per le tabelle](#)
- [Tabelle nei bucket di tabelle S3](#)
- [Accesso ai dati delle tabelle](#)
- [Lavorare con Apache Iceberg V3](#)
- [Replica delle tabelle S3](#)
- [Tabelle S3 Regioni AWS, endpoint e quote di servizio](#)
- [Esecuzione di richieste a Tabelle S3 su IPv6](#)
- [Sicurezza per Tabelle S3](#)
- [Registrazione di log e monitoraggio per Tabelle S3](#)

Funzionalità di Tabelle S3

Purpose-built archiviazione per tabelle

I bucket di tabelle S3 sono progettati specificamente per le tabelle. I bucket di tabelle offrono transazioni al secondo (TPS) più elevate e un throughput di query migliore rispetto alle tabelle autogestite nei bucket per uso generico di S3. I bucket di tabelle offrono la stessa durata, disponibilità e scalabilità degli altri tipi di bucket di Amazon S3.

Built-in supporto per Apache Iceberg

Le tabelle nei bucket vengono archiviate nel formato [Apache Iceberg](#). È possibile eseguire query su queste tabelle utilizzando SQL standard nei motori di query che supportano Iceberg. Iceberg dispone di diverse funzionalità per ottimizzare le prestazioni delle query, tra cui l'evoluzione dello schema e l'evoluzione delle partizioni.

Con Iceberg è possibile modificare l'organizzazione dei dati in modo che possano evolversi nel tempo senza dover riscrivere le query o ricostruire le strutture di dati. Iceberg è progettato per contribuire a garantire la coerenza e l'affidabilità dei dati attraverso il supporto delle transazioni. Per agevolare la correzione dei problemi o eseguire query temporali, è possibile tenere traccia delle variazioni dei dati nel tempo e tornare alle versioni storiche.

Ottimizzazione automatizzata delle tabelle

Per ottimizzare le tabelle per le query, S3 esegue continuamente operazioni di manutenzione automatiche, come la compattazione, la gestione degli snapshot e la rimozione di file senza riferimenti. Queste operazioni aumentano le prestazioni delle tabelle compattando oggetti più piccoli in un numero inferiore di file di dimensioni maggiori. Le operazioni di manutenzione riducono anche i costi di archiviazione ripulendo gli oggetti inutilizzati. La manutenzione automatizzata semplifica il funzionamento dei data lake su larga scala, riducendo la necessità di manutenzione manuale delle tabelle. Per ogni tabella e bucket di tabelle, è possibile personalizzare le configurazioni di manutenzione.

Gestione degli accessi e sicurezza

È possibile gestire l'accesso sia per i bucket di tabelle che per le singole tabelle con AWS Identity and Access Management (IAM) e [Policy di controllo dei servizi](#) in AWS Organizations. Tabelle S3 utilizza uno spazio dei nomi di servizio diverso da Amazon S3: s3tables. Pertanto, è possibile progettare policy appositamente per il servizio Tabelle S3 e le relative risorse. È possibile progettare policy per concedere l'accesso a singole tabelle, a tutte le tabelle all'interno

di uno spazio dei nomi di tabelle o a interi bucket di tabelle. Tutte le impostazioni di Blocco dell'accesso pubblico Amazon S3 sono sempre abilitate per i bucket di tabelle e non possono essere disabilitate.

Integrazione con servizi di AWS analisi

Puoi integrare automaticamente i tuoi bucket da tavolo Amazon S3 AWS Glue Data Catalog tramite la console S3. Questa integrazione consente ai servizi di AWS analisi di scoprire e accedere automaticamente ai dati delle tabelle. Dopo l'integrazione, puoi lavorare con le tue tabelle utilizzando servizi di analisi come Amazon Athena, Amazon Redshift, Quick e altri. Per ulteriori informazioni sul funzionamento dell'integrazione, consulta [Integrazione di Amazon S3 Tables con AWS servizi di analisi](#).

Servizi correlati

Puoi utilizzare quanto segue Servizi AWS con S3 Tables per supportare le tue applicazioni di analisi specifiche.

- [Amazon Athena](#): Athena è un servizio di query interattivo che semplifica l'analisi dei dati direttamente in Amazon S3 utilizzando SQL standard. Athena può essere utilizzato anche per eseguire l'analisi dei dati in modo interattivo mediante Apache Spark senza dover pianificare, configurare o gestire le risorse. Quando si eseguono applicazioni Apache Spark su Athena, si invia il codice Spark per l'elaborazione e si ricevono direttamente i risultati.
- [AWS Glue](#)— AWS Glue è un servizio di integrazione dei dati senza server che consente di scoprire, preparare, spostare e integrare dati da più fonti. È possibile utilizzarlo AWS Glue per l'analisi, l'apprendimento automatico (ML) e lo sviluppo di applicazioni. AWS Glue include anche strumenti aggiuntivi per la produttività e le operazioni sui dati per la creazione, l'esecuzione di lavori e l'implementazione di flussi di lavoro aziendali.
- [Amazon SageMaker Unified Studio](#) : SageMaker Unified Studio offre un'esperienza integrata per l'analisi e l'intelligenza artificiale con accesso unificato a tutti i tuoi dati. Collabora e crea in SageMaker Unified Studio utilizzando AWS strumenti familiari per l'analisi SQL, l'elaborazione dei dati, lo sviluppo di modelli e l'intelligenza artificiale generativa, accelerati da Amazon Q Developer. <https://docs.aws.amazon.com/amazonq/latest/qdeveloper-ug/what-is.html>
- [Amazon EMR](#) : Amazon EMR è una piattaforma cluster gestita che semplifica l'esecuzione di framework di big data, come Apache Hadoop e, su AWS di essi, per elaborare e Apache Spark analizzare grandi quantità di dati.

- [Amazon Redshift](#): Amazon Redshift è un servizio di data warehouse nel cloud in scala petabyte. È possibile utilizzare Amazon Redshift serverless per accedere e analizzare i dati senza le configurazioni di un data warehouse con provisioning. Viene eseguito automaticamente il provisioning delle risorse e la capacità del data warehouse viene dimensionata in modo intelligente per fornire prestazioni rapide per carichi di lavoro maggiormente impegnativi e imprevedibili. Quando il data warehouse è inattivo non vengono addebitati costi, si paga solo l'utilizzo. Puoi caricare i dati e iniziare subito a eseguire query nell'editor di query Amazon Redshift v2 o nello strumento di business intelligence (BI) preferito.
- [Quick](#) — Quick è un servizio di analisi aziendale per creare visualizzazioni, eseguire analisi ad hoc e ottenere rapidamente informazioni aziendali dai tuoi dati. Quick rileva facilmente le fonti di AWS dati e offre prestazioni di interrogazione rapide e reattive utilizzando il motore di calcolo rapido Super-fast In-Memory, parallelo (SPICE).
- [AWS Lake Formation](#): Lake Formation è un servizio gestito che semplifica il processo di configurazione, protezione e gestione dei data lake. Lake Formation ti aiuta a individuare le origini dati e quindi a catalogare, pulire e trasformare i dati. Con Lake Formation, è possibile gestire un controllo granulare degli accessi per i dati del data lake su Amazon S3 e i relativi metadati in AWS Glue Data Catalog.

Tutorial: Nozioni di base su Tabelle S3

In questo tutorial, creerai un bucket di tabelle e integrerai i bucket di tabelle nella tua regione con i servizi di analisi. AWS Successivamente, utilizzerai la console AWS CLI o per creare il tuo primo namespace e la prima tabella nel tuo table bucket. Quindi, puoi iniziare a interrogare la tua tabella con Athena.

Tip

Per migrare dati tabulari da bucket per uso generico a bucket di tabelle, la Biblioteca di soluzioni AWS offre all'utente una soluzione guidata. Questa soluzione automatizza lo spostamento Apache Iceberg delle Apache Hive tabelle registrate AWS Glue Data Catalog e archiviate in bucket generici verso bucket di tabelle utilizzando AWS Step Functions e Amazon EMR con Apache Spark. Per ulteriori informazioni, consulta [Linee guida per la migrazione dei dati tabulari da Amazon S3 a Tabelle S3](#) nella Biblioteca di soluzioni AWS.

Argomenti

- [Fase 1: Crea un table bucket e integralo con AWS servizi di analisi](#)
- [Fase 2: creare un namespace di tabelle e una tabella](#)
- [Fase 3: Interroga i dati con SQL in Athena](#)

Fase 1: Crea un table bucket e integralo con AWS servizi di analisi

In questa fase utilizzi la console Amazon S3 per creare il tuo primo bucket di tabelle. Per conoscere altri metodi per creare un bucket di tabelle, consulta [Creazione di un bucket di tabelle](#).

Note

Per impostazione predefinita, la console Amazon S3 integra automaticamente i bucket di tabelle con AWS Glue Data Catalog, il che consente ai servizi di AWS analisi di rilevare e accedere automaticamente ai dati di S3 Tables. Se crei il tuo primo bucket di tabelle a livello di codice utilizzando AWS Command Line Interface (AWS CLI), AWS SDK o API REST, devi completare manualmente l'integrazione dei servizi di analisi. AWS Per ulteriori informazioni, consulta [Integrazione di Amazon S3 Tables con AWS servizi di analisi](#).

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare il bucket di tabelle.
3. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
4. Seleziona Crea bucket di tabelle.
5. In Configurazione generale, inserisci un nome per il bucket di tabelle.

Il nome del bucket di tabelle deve:

- Sii unico per te Account AWS nella regione attuale.
- Deve contenere da 3 a 63 caratteri
- È composto solo da lettere minuscole, numeri e trattini (.).
- Iniziare e finire con una lettera o un numero.

Una volta creato il bucket di tabelle, non è possibile modificarne il nome. Chi crea il Account AWS bucket della tabella ne è il proprietario. Per ulteriori informazioni sulla denominazione dei bucket di tabelle, consulta [Regole di denominazione dei bucket di tabelle](#).

6. Nella sezione Integrazione con servizi di AWS analisi, assicurati che la casella di controllo Abilita integrazione sia selezionata.

Se l'opzione Abilita integrazione è selezionata quando crei il primo bucket di tabelle utilizzando la console, Amazon S3 tenta di integrare il bucket di tabelle con i servizi di analisi. AWS Questa integrazione consente di utilizzare i servizi di AWS analisi per accedere a tutte le tabelle nella regione corrente. Per ulteriori informazioni, consulta [Integrazione di Amazon S3 Tables con AWS servizi di analisi](#).

7. Seleziona Crea bucket.

Fase 2: creare un namespace di tabelle e una tabella

In questa fase si crea un namespace nel bucket di tabelle e quindi si crea una nuova tabella nel namespace. È possibile creare un namespace di tabelle e una tabella utilizzando la console o la AWS CLI.

Important

Durante la creazione delle tabelle, è necessario utilizzare solo lettere minuscole nei nomi delle tabelle e nelle definizioni delle tabelle. Ad esempio, è necessario verificare che i nomi delle colonne siano tutti in minuscolo. Se il nome o la definizione della tabella contiene lettere maiuscole, la tabella non è supportata da AWS Lake Formation o da AWS Glue Data Catalog. In questo caso, la tabella non sarà visibile ai servizi di AWS analisi come Amazon Athena, anche se i bucket di tabelle sono integrati con i servizi di AWS analisi.

Se la definizione della tabella contiene lettere maiuscole, riceverai il seguente messaggio di errore quando esegui una SELECT query in Athena: «GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model. ValidationException: Risorsa federativa non supportata: nomi di tabella o colonna non validi.»

Utilizzo della console S3 e Amazon Athena

La procedura seguente utilizza la console di Amazon S3 per creare un namespace e una tabella con Amazon Athena.

Come creare un namespace e una tabella

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nella pagina Bucket di tabelle, scegli il bucket di tabelle in cui creare una tabella.
4. Nella pagina dei dettagli del bucket di tabelle, scegli Crea tabella con Athena.
5. Nella finestra di dialogo Crea tabella con Athena, scegli Crea un namespace, quindi inserisci un nome nel campo Nome del namespace. I nomi dei namespace devono essere composti da un numero di caratteri compreso tra 1 e 255 ed essere univoci all'interno del bucket di tabelle. I caratteri validi sono a-z, 0-9 e i caratteri di sottolineatura (_). I caratteri di sottolineatura non sono consentiti all'inizio dei nomi dei namespace.
6. Selezionare Crea namespace.
7. Scegli Crea tabella con Athena.
8. Si apre la console Amazon Athena e viene visualizzato l'editor di query Athena. L'editor di query è popolato con una query di esempio da utilizzare per creare una tabella. Modifica la query per specificare il nome della tabella e le colonne della tabella.
9. Una volta modificata la query, scegli Esegui per creare la tabella.

Se la creazione della tabella viene completata, il nome della nuova tabella viene visualizzato nell'elenco delle tabelle in Athena. Quando torni alla console Amazon S3, la nuova tabella viene visualizzata nell'elenco Tabelle nella pagina dei dettagli del bucket di tabelle, dopo aver aggiornato l'elenco.

Utilizzo di AWS CLI

Per utilizzare i seguenti comandi di AWS CLI esempio per creare uno spazio dei nomi nel bucket della tabella e quindi creare una nuova tabella con uno schema all'interno di tale namespace, sostituisci i valori con i tuoi. *user input placeholder*

Prerequisiti

- Collegare la policy [AmazonS3TablesFullAccess](#) all'identità IAM.
- Installa AWS CLI la versione 2.23.10 o successiva. Per ulteriori informazioni, consulta [Installazione o aggiornamento della versione più recente della AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface .

1. Crea un nuovo namespace nel bucket di tabelle eseguendo il comando seguente:

```
aws s3tables create-namespace \  
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
table-bucket \  
--namespace my_namespace
```

- Verifica che il namespace sia stato creato correttamente eseguendo il comando seguente:

```
aws s3tables list-namespaces \  
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
table-bucket
```

2. Crea una nuova tabella con uno schema di tabella eseguendo il seguente comando:

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

Per il file `mytabledefinition.json`, utilizza la seguente definizione di tabella di esempio:

```
{  
  "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
table-bucket",  
  "namespace": "my_namespace",  
  "name": "my_table",  
  "format": "ICEBERG",  
  "metadata": {  
    "iceberg": {  
      "schema": {  
        "fields": [  
          {"name": "id", "type": "int", "required": true},  
          {"name": "name", "type": "string"},  
          {"name": "value", "type": "int"}  
        ]  
      }  
    }  
  }  
}
```

```
}  
  }  
    }
```

Fase 3: Interroga i dati con SQL in Athena

È possibile eseguire query sulla tabella con SQL in Athena. Athena supporta le query Data Definition Language (DDL), Data Manipulation Language (DML) e Data Query Language (DQL) per Tabelle S3.

È possibile accedere alla query Athena dalla console Amazon S3 o tramite la console Amazon Athena.

Utilizzo della console S3 e Amazon Athena

La procedura seguente utilizza la console Amazon S3 per accedere all'editor di query Athena in modo da poter eseguire query su una tabella con Amazon Athena.

Come eseguire query su una tabella

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nella pagina Bucket di tabelle, scegli il bucket di tabelle contenente la tabella sui cui desideri eseguire la query.
4. Nella pagina dei dettagli del bucket di tabelle, scegli il pulsante di opzione accanto al nome della tabella su cui desideri eseguire una query.
5. Scegli Interroga tabella con Athena.
6. Si apre la console Amazon Athena e viene visualizzato l'editor di query Athena con una query SELECT di esempio caricata automaticamente. Modifica questa query in base alle esigenze del caso d'uso.
7. Per eseguire la query, scegli Run (Esegui).

Utilizzo della console Amazon Athena

Come eseguire query su una tabella

1. Apri la console Athena all'indirizzo <https://console.aws.amazon.com/athena/>.

2. Eseguire una query sulla tabella. Di seguito è riportata una query di esempio che è possibile modificare. Assicurarsi di sostituire *user input placeholders* con le proprie informazioni.

```
SELECT * FROM "s3tablescatalog/amzn-s3-demo-table-bucket"."my_namespace"."my_table"
LIMIT 10
```

3. Per eseguire la query, scegli Run (Esegui).

Secchi da tavolo

Il bucket di tabelle Amazon S3 è un tipo di bucket S3 che è possibile utilizzare per creare e archiviare tabelle come risorse S3. I bucket di tabelle vengono utilizzati per archiviare dati tabulari e metadati come oggetti da utilizzare nei carichi di lavoro di analisi. S3 esegue automaticamente la manutenzione nei bucket di tabelle per contribuire a ridurre i costi di archiviazione delle tabelle. Per ulteriori informazioni, consulta [Manutenzione di Tabelle S3](#).

Per interagire con le tabelle archiviate all'interno dei propri bucket di tabelle, è possibile integrare i bucket di tabelle con applicazioni di analisi che supportano [Apache Iceberg](#). I bucket di tabella si integrano con i servizi di AWS analisi tramite AWS Glue Data Catalog. Per ulteriori informazioni, consulta [Integrazione di Amazon S3 Tables con AWS servizi di analisi](#). È anche possibile interagire con le tabelle tramite motori di query open source che utilizzano Catalogo di Tabelle Amazon S3 per Apache Iceberg. Per ulteriori informazioni, consulta [Accesso alle tabelle utilizzando Amazon S3 Tables Iceberg REST endpoint](#).

Ogni bucket di tabelle ha un nome della risorsa Amazon (ARN) univoco e una policy di risorsa associati. Gli ARN dei bucket di tabelle presentano il formato seguente:

```
arn:aws:s3tables:Region:OwnerAccountID:bucket/bucket-name
```

Tutti i bucket di tabelle e le tabelle sono privati e non possono essere resi pubblici. L'accesso a queste risorse è possibile solo per gli utenti a cui è concesso esplicitamente l'accesso. Per concedere l'accesso, è possibile utilizzare le policy basate sulle risorse IAM per i bucket di tabelle e le tabelle e per le policy basate sull'identità IAM per utenti e ruoli.

Per impostazione predefinita, puoi creare fino a 10 bucket di tabella per Regione AWS in un Account AWS. Per richiedere un aumento della quota per i bucket di tabelle o le tabelle, contattare [Supporto](#).

Tipi di bucket di tabelle

Amazon S3 supporta i seguenti tipi di bucket di tabelle:

Customer-managed secchi da tavola

Customer-managed i bucket di tabelle sono risorse per l'archiviazione di tabelle Amazon S3 create e gestite dai clienti. Puoi creare questi bucket in modo esplicito, sceglierne i nomi e mantenere il pieno controllo sulle tabelle e sui namespace al loro interno. Per i bucket di tabelle gestiti dal cliente, puoi creare, eliminare, impostare una crittografia predefinita personalizzata o configurare le opzioni di manutenzione in base alle esigenze.

AWS bucket di tabelle gestiti

AWS i bucket di tabelle AWS gestiti sono risorse gestite che archiviano automaticamente le tabelle create dai AWS servizi, come le tabelle dell'inventario attivo e del journal create da S3 Metadata. Questi bucket forniscono una posizione centralizzata per tutte le tabelle generate dal sistema. Inoltre, seguono una convenzione di denominazione standard, utilizzano un namespace standard per tutte le tabelle e dispongono di configurazioni di manutenzione e crittografia predefinite che S3 modifica per conto dell'utente. Hai accesso in sola lettura per interrogare i dati, mentre AWS gestisce tutte le operazioni di creazione, aggiornamento e manutenzione delle tabelle. Per ulteriori informazioni, consulta [Lavorare con AWS bucket da tavolo gestiti](#).

Sono disponibili diversi tipi di bucket Amazon S3. Prima di creare un bucket, accertati di scegliere il tipo di bucket più adatto ai requisiti dell'applicazione e delle prestazioni. Per ulteriori informazioni sui vari tipi di bucket e sui casi d'uso appropriati per ogni tipo, consulta [Bucket](#).

Argomenti

- [Regole di denominazione di bucket di tabelle, tabelle e spazio dei nomi di Amazon S3](#)
- [Creazione di un bucket di tabelle](#)
- [Eliminazione di un bucket di tabelle](#)
- [Visualizzazione dei dettagli su un bucket di tabelle Amazon S3](#)
- [Gestione delle policy dei bucket di tabelle](#)
- [Lavorare con AWS bucket da tavolo gestiti](#)
- [Utilizzo dei tag con i bucket di tabelle S3](#)

Regole di denominazione di bucket di tabelle, tabelle e spazio dei nomi di Amazon S3

Quando crei un bucket di tabelle, scegli un nome per il bucket e Regione AWS il nome deve essere univoco per il tuo account nella regione scelta. Dopo aver creato un bucket di tabelle, non è possibile modificare il nome del bucket o la Regione. I nomi dei bucket di tabelle devono seguire regole di denominazione specifiche. Per ulteriori informazioni sulle regole di denominazione per i bucket di tabelle, le tabelle e gli spazi dei nomi al loro interno, consulta il seguente argomento.

Argomenti

- [Regole di denominazione dei bucket di tabelle](#)
- [Regole di denominazione per tabelle e spazi dei nomi](#)

Regole di denominazione dei bucket di tabelle

Quando si creano bucket di tabelle Amazon S3, specificare un nome per i bucket di tabelle. Come altri tipi di bucket, i bucket di tabelle non possono essere rinominati. A differenza di altri tipi di bucket, i table bucket non si trovano in un namespace globale, quindi ogni nome di bucket nel tuo account deve essere univoco solo all'interno della regione corrente. AWS

Per le regole di denominazione dei bucket per uso generico, consulta [Regole di denominazione dei bucket per uso generico](#). Per le regole di denominazione dei bucket di directory, consulta [Regole di denominazione dei bucket di directory](#).

Ai bucket di tabelle si applicano le seguenti regole di denominazione.

- I nomi dei bucket devono avere una lunghezza compresa tra 3 e 63 caratteri.
- I nomi dei bucket possono essere composti solo da lettere minuscole, numeri e trattini (.). -
- I nomi dei bucket devono iniziare e terminare con una lettera o un numero.
- I nomi dei bucket non devono contenere trattini bassi (_) o punti (.).
- I nomi dei bucket non devono iniziare con i seguenti prefissi riservati:
 - xn--
 - sthree-
 - amzn-s3-demo-
 - aws

- I nomi dei bucket non devono terminare con i seguenti suffissi riservati:
 - `-s3alias`
 - `--ol-s3`
 - `--x-s3`
 - `--table-s3`

Regole di denominazione per tabelle e spazi dei nomi

Le seguenti regole di denominazione si applicano alle tabelle e ai namespace all'interno dei bucket di tabelle.

- I nomi devono contenere un numero di caratteri compreso tra 1 e 255.
- I nomi possono essere composti solo da lettere minuscole, numeri e caratteri di sottolineatura (`_`).
- I nomi devono iniziare con una lettera o un numero.
- I nomi non devono contenere trattini (`-`) o punti (`.`).
- Un nome di tabella deve essere univoco all'interno di uno spazio dei nomi.
- Uno spazio dei nomi deve essere univoco all'interno di un bucket di tabelle.
- I nomi dei namespace non devono iniziare con il prefisso riservato `aws`.

Important

Durante la creazione delle tabelle, è necessario utilizzare solo lettere minuscole nei nomi delle tabelle e nelle definizioni delle tabelle. Ad esempio, è necessario verificare che i nomi delle colonne siano tutti in minuscolo. Se il nome o la definizione della tabella contiene lettere maiuscole, la tabella non è supportata da AWS Lake Formation o da AWS Glue Data Catalog. In questo caso, la tabella non sarà visibile ai servizi di AWS analisi come Amazon Athena, anche se i bucket di tabelle sono integrati con i servizi di AWS analisi.

Se la definizione della tabella contiene lettere maiuscole, riceverai il seguente messaggio di errore quando esegui una `SELECT` query in Athena: «`GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model. ValidationException: Risorsa federativa non supportata: nomi di tabella o colonna non validi.`»

Creazione di un bucket di tabelle

Il bucket di tabelle Amazon S3 è un tipo di bucket S3 che è possibile utilizzare per creare e archiviare tabelle come risorse S3. Per iniziare a utilizzare Tabelle S3, creare un bucket di tabelle in cui archiviare e gestire tabelle. Quando crei un bucket di tabella, scegli il nome del bucket e. Regione AWS Il nome del bucket di tabelle deve essere univoco per l'account nella Regione selezionata. Dopo aver creato un bucket di tabelle, non è possibile modificare il nome del bucket o la Regione. Per ulteriori informazioni sulla denominazione dei bucket di tabelle, consulta [Regole di denominazione di bucket di tabelle, tabelle e spazio dei nomi di Amazon S3](#).

Il nome della risorsa Amazon (ARN) per i bucket di tabelle ha il seguente formato:

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name
```

Per impostazione predefinita, è possibile creare fino a 10 bucket di tabelle per Regione in un Account AWS. Per richiedere un aumento della quota per i bucket di tabelle o le tabelle, contattare [Supporto](#).

Quando crei un bucket di tabelle, puoi specificare il tipo di crittografia che verrà utilizzato per crittografare le tabelle che crei in quel bucket. Per ulteriori informazioni sulle opzioni di crittografia del bucket, consulta [the section called “Encryption \(Crittografia\)”](#).

Prerequisiti per la creazione di bucket di tabelle

Per creare un bucket di tabelle, procedi come segue:

- Assicurati di disporre delle autorizzazioni AWS Identity and Access Management (IAM) per. `s3tables:CreateTableBucket`

Note

Se scegli SSE-KMS come tipo di crittografia predefinito, devi disporre delle autorizzazioni e delle autorizzazioni per `s3tables:PutTableBucketEncryption` la chiave scelta AWS KMS . `DescribeKey` Inoltre, la AWS KMS chiave utilizzata deve concedere a S3 Tables l'autorizzazione per eseguire la manutenzione automatica delle tabelle. Per ulteriori informazioni, consulta [Requisiti di autorizzazione per la crittografia delle tabelle S3 SSE-KMS](#).

Per creare un bucket di tabelle, puoi utilizzare la console Amazon S3, l'API REST di Amazon S3, AWS Command Line Interface (AWS CLI) o gli SDK. AWS

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare un bucket.
3. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
4. Scegli Crea bucket di tabelle per aprire la pagina Crea bucket di tabelle.
5. In Proprietà inserire un nome per il bucket di tabelle.

Il nome del bucket di tabelle deve:

- Essere univoco per l'account dell'utente nella Regione corrente.
- Deve contenere un numero di caratteri compreso tra 3 a 63.
- Essere costituito solo da lettere minuscole, numeri e trattini (-).
- Iniziare e finire con una lettera o un numero.

Una volta creato il bucket, non è possibile modificarne il nome. Chi crea Account AWS il bucket ne è il proprietario. Per ulteriori informazioni sulla denominazione dei bucket di tabelle, consulta [Regole di denominazione di bucket di tabelle, tabelle e spazio dei nomi di Amazon S3](#).

6. Se desideri integrare i tuoi bucket di tabelle con i servizi di AWS analisi, assicurati che **Abilita integrazione** sia selezionata in **Integrazione con i servizi di AWS analisi**.

Note

Quando crei il tuo primo bucket di tabelle utilizzando la console con l'opzione **Abilita integrazione** selezionata, Amazon S3 tenta di integrare automaticamente il bucket di tabelle con i servizi di analisi. AWS Questa integrazione consente di utilizzare i servizi di AWS analisi per interrogare tutte le tabelle nella regione corrente. Per ulteriori informazioni, consulta [Integrazione di Amazon S3 Tables con AWS servizi di analisi](#).

7. Per configurare la crittografia predefinita, in **Tipo di crittografia** scegli una delle seguenti opzioni:
 - Server-side crittografia con chiave gestita Amazon S3 () SSE-S3
 - Server-side crittografia con AWS Key Management Service chiave () SSE-KMS

Per ulteriori informazioni sulle opzioni di crittografia dei dati della tabella, consulta [Protezione dei dati delle tabelle S3 con la crittografia](#).

8. Seleziona Crea bucket.

Utilizzo di AWS CLI

Questo esempio mostra come creare un bucket di tabelle tramite AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables create-table-bucket \  
  --region us-east-2 \  
  --name amzn-s3-demo-bucket1
```

Per impostazione predefinita, i bucket di tabella S3 utilizzano SSE-S3 come impostazione di crittografia predefinita, tuttavia, è possibile utilizzare il `--encryption-configuration` parametro opzionale per specificare un tipo di crittografia diverso. Gli esempi seguenti mostrano come creare un bucket che utilizza la crittografia. SSE-KMS Per ulteriori informazioni sulle impostazioni di crittografia per i bucket di tabelle, consulta [Protezione dei dati delle tabelle S3 con la crittografia](#).

```
aws s3tables create-table-bucket \  
  --region us-east-2 \  
  --name amzn-s3-demo-bucket1 \  
  --encryption-configuration '{  
    "sseAlgorithm": "aws:kms",  
    "kmsKeyArn":  
    "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab" }'
```

Eliminazione di un bucket di tabelle

Puoi utilizzare le API o gli AWS SDK di Amazon S3 per eliminare un bucket di tabelle. AWS Command Line Interface Prima di eliminare un bucket di tabelle, è necessario eliminare tutti i namespace e tutte le tabelle all'interno del bucket.

Important

Quando elimini un bucket di tabelle, è importante tenere in considerazione quanto segue:

- L'eliminazione del bucket è permanente e non può essere annullata.
- Tutti i dati e tutte le configurazioni associati al bucket vengono definitivamente persi.

Utilizzo di AWS CLI

In questo esempio viene mostrato come eliminare un bucket di tabelle tramite AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables delete-table-bucket \  
  --region us-east-2 \  
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket1
```

Visualizzazione dei dettagli su un bucket di tabelle Amazon S3

È possibile visualizzare i dettagli generali di un bucket di Tabelle Amazon S3, ad esempio il proprietario e il tipo di bucket, nella console o in modo programmatico. Puoi visualizzare le impostazioni di crittografia predefinite e le impostazioni di manutenzione a livello di codice utilizzando l'API REST o gli SDK di S3 Tables. AWS CLI AWS

Visualizzazione dei dettagli del bucket di tabelle

Utilizzo di AWS CLI

In questo esempio viene mostrato come ottenere dettagli su un bucket di tabelle tramite AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables get-table-bucket --table-bucket-arn arn:aws:s3tables:us-  
east-1:111122223333:bucket/amzn-s3-demo-table-bucket
```

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Selezionare il bucket di tabelle.

4. Seleziona la scheda Proprietà.

Visualizzazione delle impostazioni di crittografia dei bucket di tabelle

Per ulteriori informazioni sulla crittografia dei bucket di tabelle, consulta [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket delle tabelle](#).

Utilizzo di AWS CLI

Questo esempio mostra come ottenere dettagli sulle impostazioni di crittografia per un bucket di tabelle tramite la AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables get-table-bucket-encryption --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket
```

Visualizzazione delle configurazioni di manutenzione dei bucket di tabelle

Per ulteriori informazioni sulle impostazioni di manutenzione, consulta [Manutenzione dei bucket di tabelle](#).

Utilizzo di AWS CLI

Questo esempio mostra come ottenere dettagli sulle impostazioni di configurazione della manutenzione per un bucket di tabelle tramite la AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables get-table-bucket-maintenance-configuration --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket
```

Gestione delle policy dei bucket di tabelle

Puoi aggiungere, eliminare, aggiornare e visualizzare le politiche dei bucket per i bucket di tabelle Amazon S3 utilizzando l'API REST di Amazon S3, AWS gli SDK e (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta i seguenti argomenti.

Per ulteriori informazioni, consulta i seguenti argomenti. Per ulteriori informazioni sulle azioni e sulle chiavi di condizione AWS Identity and Access Management (IAM) supportate per Tabelle Amazon S3, consulta [Gestione degli accessi per Tabelle S3](#). Per le policy del bucket di esempio per i bucket di tabelle, consulta [Resource-based politiche per S3 Tables](#).

 Note

La policy di bucket delle tabelle fornisce l'accesso alle tabelle archiviate nel bucket. Le policy di bucket delle tabelle non si applicano alle tabelle di proprietà di altri account.

Aggiunta di una policy del bucket di tabelle

Per aggiungere una policy bucket a un bucket di tabella, usa il seguente esempio. AWS CLI

Utilizzo di AWS CLI

Questo esempio mostra come creare un bucket di tabelle tramite AWS CLI. Per utilizzare il comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables put-table-bucket-policy \  
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket1 \  
  --resource-policy your-policy-JSON
```

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Seleziona Bucket di tabelle, quindi fai clic sul nome del bucket di tabelle a cui desideri aggiungere una policy.
4. Scegli la scheda Autorizzazioni.
5. In Policy di bucket della tabella, seleziona Modifica.
6. Nell'editor della policy, inserisci il file JSON della policy stessa.
7. (Facoltativo) Seleziona Esempi di policy per visualizzare esempi di policy da adattare alle tue esigenze.
8. Dopo aver inserito la policy, seleziona Salva modifiche.

Visualizzazione di una policy dei bucket di tabelle

Per visualizzare la policy di bucket associata a un bucket di tabelle, utilizza il seguente esempio della AWS CLI .

Utilizzo di AWS CLI

Questo esempio mostra come visualizzare la policy associata a un bucket di tabelle tramite la AWS CLI. Per utilizzare il comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables get-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Seleziona Bucket di tabelle, quindi fai clic sul nome del bucket di tabelle per il quale desideri visualizzare la policy.
4. Scegli la scheda Autorizzazioni.

Eliminazione di una policy del bucket di tabelle

Per eliminare una policy di bucket associata a un bucket di tabelle, utilizza il seguente esempio della AWS CLI .

Utilizzo di AWS CLI

In questo esempio viene mostrato come eliminare una policy del bucket di tabelle tramite AWS CLI. Per utilizzare il comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables delete-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Seleziona Bucket di tabelle, quindi fai clic sul nome del bucket di tabelle per il quale desideri eliminare una policy.
4. Scegli la scheda Autorizzazioni.

5. In Policy di bucket della tabella, seleziona Elimina.

Lavorare con AWS bucket da tavolo gestiti

AWS i bucket di tabelle gestiti sono bucket di tabelle Amazon S3 specializzati progettati per archiviare tabelle AWS gestite, come il diario dei metadati [S3](#) e le tabelle di inventario in tempo reale. A differenza dei bucket di tabelle gestiti dai clienti che puoi creare e gestire direttamente, i bucket di tabelle AWS gestiti vengono assegnati automaticamente quando configuri funzionalità che richiedono tabelle gestite. AWS AWS Quando vengono create, le tabelle gestite appartengono a un namespace predefinito basato sul nome del bucket di origine. Questo namespace predefinito non può essere modificato.

Ognuno Account AWS ha un bucket di tabelle AWS gestito per regione, seguendo la convenzione di denominazione. `aws-s3` Questo bucket funge da posizione centralizzata per tutte le tabelle gestite associate alle risorse dell'account nella Regione in uso.

La tabella seguente confronta i bucket di tabelle AWS gestiti con i bucket di tabella gestiti dal cliente.

Funzionalità	AWS bucket da tavolo gestiti	Customer-managed secchi da tavolo
Creazione	Creato automaticamente da Servizi AWS	Creati manualmente
Denominazione	Utilizzano una convenzione di denominazione standard (<code>aws-s3</code>)	I nomi vengono definiti dall'utente
Creazione di tabelle	È Servizi AWS possibile creare solo tabelle	Le tabelle possono essere create dall'utente
Controllo dei namespace	Non è possibile creare o eliminare namespace (tutte le tabelle appartengono a un namespace fisso)	I namespace possono essere creati ed eliminati dall'utente
Accesso	Read-only accesso	Accesso completo ad
Encryption (Crittografia)	È possibile modificare le impostazioni di crittografia predefinite (SSE-S3) solo se la tabella iniziale è stata crittografata con una chiave gestita	La crittografia predefinita a livello di bucket può essere impostata e modificata in qualsiasi momento dall'utente

Funzionalità	AWS bucket da tavolo gestiti	Customer-managed secchi da tavolo
	dal cliente AWS Key Management Service (AWS KMS)	
Maintenance (Manutenzione)	Gestito da Servizi AWS	La manutenzione automatizzata a livello di bucket può essere personalizzata dall'utente

Autorizzazioni con cui lavorare AWS bucket di tabelle gestiti e per interrogare le tabelle

Per utilizzare i bucket di tabelle AWS gestiti, sono necessarie le autorizzazioni per creare bucket e tabelle AWS gestiti e per specificare le impostazioni di crittografia per le tabelle gestite. AWS Sono inoltre necessarie le autorizzazioni per interrogare le tabelle nei bucket di tabelle gestiti AWS .

La seguente politica di esempio consente di creare un bucket di tabelle AWS gestito tramite una configurazione di metadati S3:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermissionsToWorkWithMetadataTables",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucketMetadataTableConfiguration",
        "s3tables:CreateTableBucket",
        "s3tables:CreateNamespace",
        "s3tables:CreateTable",
        "s3tables:GetTable",
        "s3tables:PutTablePolicy",
        "s3tables:PutTableEncryption",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:s3:::bucket/amzn-s3-demo-source-bucket",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/*",
        "arn:aws:kms:us-east-1:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"
      ]
    }
  ]
}
```

```

    }
  ]
}
```

La seguente politica di esempio consente di interrogare le tabelle nei AWS bucket di tabelle gestiti:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermissionsToQueryMetadataTables",
      "Effect": "Allow",
      "Action": [
        "s3tables:GetTable",
        "s3tables:GetTableData",
        "s3tables:GetTableMetadataLocation",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/*",
        "arn:aws:kms:us-east-1:111122223333:key/01234567-89ab-
cdef-0123-456789abcdef"
      ]
    }
  ]
}
```

Interrogazione di tabelle in AWS bucket di tabelle gestiti

È possibile interrogare le tabelle AWS gestite nei bucket di tabelle AWS gestite utilizzando metodi e motori di accesso supportati da S3 Tables. Di seguito sono riportati alcuni esempi di query.

Using standard SQL

L'esempio seguente mostra come interrogare le tabelle AWS gestite utilizzando la sintassi SQL standard:

```

SELECT *
FROM "s3tablescatalog/aws-s3"."b_amzn-s3-demo-source-bucket"."inventory"
LIMIT 10;
```

L'esempio seguente mostra come unire tabelle AWS gestite con tabelle personalizzate:

```
SELECT *
FROM "s3tablescatalog/aws-s3"."b_arn-s3-demo-source-bucket"."inventory" a
JOIN "s3tablescatalog/arn-s3-demo-table-bucket"."my_namespace"."my_table" b
ON a.key = b.key
LIMIT 10;
```

Using Spark

L'esempio seguente mostra come eseguire una query sulla tabella con Spark:

```
spark.sql("""
    SELECT *
    FROM ice_catalog.inventory a
    JOIN ice_catalog.my_table b
    ON a.key = b.key
    """).show(10, true)
```

L'esempio seguente mostra come unire la tabella AWS gestita con un'altra tabella:

```
SELECT *
FROM inventory a
JOIN my_table b
ON a.key = b.key
LIMIT 10;
```

Crittografia per AWS bucket di tabelle gestiti

Per impostazione predefinita, i bucket di tabelle AWS gestiti sono crittografati con crittografia lato server utilizzando le chiavi gestite di Amazon S3 (`aws:kms`). Dopo aver creato il bucket di tabelle AWS gestite, puoi utilizzarlo [PutTableBucketEncryption](#) per impostare l'impostazione di crittografia predefinita del bucket in modo che utilizzi la crittografia lato server con (`aws:kms`) keys (`aws:kms`). AWS Key Management Service AWS KMS SSE-KMS

Durante la creazione delle tabelle AWS gestite, puoi scegliere di crittografarle con SSE-KMS. Se scegli di utilizzare SSE-KMS, devi fornire una chiave KMS gestita dal cliente nella stessa regione del bucket di tabelle AWS gestito. È possibile impostare il tipo di crittografia per le tabelle AWS gestite solo durante la creazione della tabella. Dopo aver creato una tabella AWS gestita, non è possibile modificarne le impostazioni di crittografia.

Se desideri che il bucket di tabelle AWS gestite e le tabelle in esso archiviate utilizzino la stessa chiave KMS, assicurati di utilizzare la stessa chiave KMS che hai usato per crittografare le tabelle per crittografare il bucket di tabelle dopo che è stato creato. Dopo aver modificato le impostazioni di crittografia predefinite per il bucket di tabelle da utilizzare SSE-KMS, tali impostazioni di crittografia vengono utilizzate per tutte le tabelle future create nel bucket.

Utilizzo dei tag con i bucket di tabelle S3

Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso i bucket di tabelle Amazon S3. Puoi etichettare i bucket di tabelle S3 quando li crei o gestire i tag sui bucket di tabella esistenti. Per informazioni generali sui tag, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

Note

Non sono previsti costi aggiuntivi per l'utilizzo dei tag nei bucket di tabella oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Modi comuni per utilizzare i tag con i bucket di tabella

Usa i tag nei bucket delle tabelle S3 per:

Attribute-based controllo degli accessi (ABAC): ridimensiona le autorizzazioni di accesso e concedi l'accesso ai bucket di tabelle S3 in base ai relativi tag. Per ulteriori informazioni, consulta [Utilizzo dei tag per ABAC](#).

ABAC per bucket da tavolo S3

I bucket di tabelle Amazon S3 supportano il controllo degli accessi basato sugli attributi (ABAC) tramite tag. Utilizza le chiavi di condizione basate su tag nelle policy AWS aziendali, AWS Identity and Access Management (IAM) e S3 table bucket. ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle tue policy IAM, puoi controllare l'accesso ai bucket di tabelle S3 in base ai tag del bucket di tabella utilizzando la chiave di condizione o le chiavi [di s3tables:TableBucketTag/tag-key condizione](#) AWS globali:, o. `aws:ResourceTag/key-name` `aws:RequestTag/key-name` `aws:TagKeys`

leggi: ResourceTag/key-name

Usa questa chiave di condizione per confrontare la coppia chiave-valore del tag specificata nella policy con la coppia chiave-valore associata alla risorsa. Ad esempio, potresti richiedere che l'accesso a un bucket di tabella sia consentito solo se il bucket di tabella ha la chiave tag con il valore. Department Marketing

Questa chiave di condizione si applica a tutte le azioni del bucket di tabella eseguite utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI), le API S3 o gli AWS SDK, ad eccezione della richiesta API. CreateBucket

Per un esempio di policy, consulta [1.1 - policy del bucket di tabelle per limitare le operazioni sulle tabelle all'interno del bucket di tabelle utilizzando i tag](#).

Per ulteriori esempi di policy e ulteriori informazioni, consulta [Controlling access to resources nella Guida per AWS l'utente](#). AWS Identity and Access Management

Note

Per le azioni eseguite sulle tabelle, questa chiave di condizione agisce sui tag applicati alla tabella e non sui tag applicati al bucket della tabella contenente la tabella. Usa `s3tables:TableBucketTag/tag-key` invece se desideri che le tue politiche ABAC agiscano sui tag del bucket della tabella quando esegui le azioni sulla tabella.

leggi: RequestTag/key-name

Usa questa chiave di condizione per confrontare la coppia chiave-valore del tag passata nella richiesta con la coppia di tag specificata nella policy. Ad esempio, puoi verificare se la richiesta di etichettare un bucket di tabella include la chiave del tag Department e se ha il valore. Accounting

Questa chiave di condizione si applica quando le chiavi dei tag vengono passate in una richiesta di operazione TagResource o CreateTableBucket API o quando si tagga o si crea un bucket di tabella con tag utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI) o gli SDK. AWS

Per un esempio di policy, consulta [1.2 - Politica IAM per creare o modificare bucket di tabelle con tag specifici](#).

Per ulteriori esempi di policy e ulteriori informazioni, consulta [Controllare l'accesso durante le AWS richieste](#) nella Guida per l'utente. AWS Identity and Access Management

è stato: TagKeys

Usa questa chiave di condizione per confrontare le chiavi dei tag in una richiesta con le chiavi specificate nella policy per definire a quali chiavi di tag è consentito l'accesso. Ad esempio, per consentire l'etichettatura durante l'CreateTableBucketazione, è necessario creare una policy che consenta `s3tables:TagResource` sia le `s3tables:CreateTableBucket` azioni che. È quindi possibile utilizzare la chiave di `aws:TagKeys` condizione per imporre che nella richiesta vengano utilizzati solo tag specifici. `CreateTableBucket`

Questa chiave di condizione si applica quando le chiavi dei tag vengono passate in `unaTagResource`, `UntagResource`, o in operazioni `CreateTableBucket` API o quando si codifica, deselecta o si crea un bucket di tabella con tag utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI) o gli SDK. AWS

Per un esempio di policy, consulta [1.3 - Politica IAM per controllare la modifica dei tag sulle risorse esistenti mantenendo la governance dei tag](#).

Per ulteriori esempi di policy e ulteriori informazioni, consulta [Controlling access based on tag keys nella Guida per l'utente](#). AWS Identity and Access Management

s3tables: TableBucketTag/tag-key

Usa questa chiave di condizione per concedere autorizzazioni a dati specifici nei bucket di tabelle utilizzando i tag. Questa chiave di condizione agisce, in gran parte, sui tag assegnati al bucket di tabelle per tutte le azioni delle tabelle S3. Anche quando si crea una tabella con tag, questa chiave di condizione agisce sui tag applicati al bucket della tabella che contiene quella tabella. Le eccezioni sono:

- Quando si crea un bucket di tabella con tag, questa chiave di condizione agisce sui tag nella richiesta.

Per un esempio di policy, consulta [1.4 - Utilizzo della chiave s3tables: condition TableBucketTag](#).

Esempi di politiche ABAC per i bucket di tabelle

Vedi il seguente esempio di politiche ABAC per i bucket di tabelle Amazon S3.

Note

Se utilizzi Lake Formation per gestire l'accesso alle tue tabelle Amazon S3 e disponi di una policy basata sulle risorse IAM o S3 Tables che limita gli utenti IAM e i ruoli IAM in base ai tag

principali, devi allegare gli stessi tag principali al ruolo IAM utilizzato da Lake Formation per accedere ai tuoi dati Amazon S3 (ad esempio) e concedere a questo ruolo le autorizzazioni necessarie. `LakeFormationDataAccessRole` Ciò è necessario affinché la politica di controllo degli accessi basata su tag funzioni correttamente con l'integrazione dell'analisi di S3 Tables.

1.1 - policy del bucket di tabelle per limitare le operazioni sulle tabelle all'interno del bucket di tabelle utilizzando i tag

In questa policy del bucket della tabella, i principali IAM specificati (utenti e ruoli) possono eseguire l'operazione `GetTable` su qualsiasi tabella nel bucket della tabella solo se il valore del tag della tabella corrisponde al valore del `project` tag del principale. `project`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGetTable",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3tables:GetTable",
      "Resource": "arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}
```

1.2 - Politica IAM per creare o modificare bucket di tabelle con tag specifici

Note

Se utilizzi AWS Lake Formation per gestire l'accesso alle tue tabelle Amazon S3 e utilizzi ABAC con Amazon S3 Tables, assicurati di assegnare anche il ruolo IAM in base al quale Lake Formation assume l'accesso richiesto. Per ulteriori informazioni sulla configurazione del

ruolo IAM per Lake Formation, consulta [Prerequisiti per l'integrazione del catalogo di tabelle Amazon S3 con il Data Catalog e Lake Formation nella guida per gli sviluppatori](#). AWS Lake Formation

In questa policy IAM, gli utenti o i ruoli con questa policy possono creare bucket di tabelle S3 solo se etichettano il bucket di tabella con la chiave `project` e il valore del tag `Trinity` nella richiesta di creazione del bucket di tabella. Possono anche aggiungere o modificare tag su bucket di tabelle S3 esistenti, purché la `TagResource` richiesta includa la coppia chiave-valore del tag. `project:Trinity` Questa policy non concede autorizzazioni di lettura, scrittura o eliminazione sui bucket della tabella o sui relativi oggetti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateTableBucketWithTags",
      "Effect": "Allow",
      "Action": [
        "s3tables:CreateTableBucket",
        "s3tables:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
            "Trinity"
          ]
        }
      }
    }
  ]
}
```

1.3 - Politica IAM per controllare la modifica dei tag sulle risorse esistenti mantenendo la governance dei tag

In questa policy IAM, i principali IAM (utenti o ruoli) possono modificare i tag su un bucket di tabella solo se il valore del tag del bucket di tabella corrisponde al valore del `project` tag del principal. `project` Per questi bucket di `project` tabella sono consentiti solo i quattro tag `environmentowner`, e `cost-center` specificati nelle chiavi di `aws:TagKeys` condizione. Questo

aiuta a far rispettare la governance dei tag, previene modifiche non autorizzate ai tag e mantiene lo schema di tagging coerente nei bucket della tabella.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3tables:TagResource",
        "s3tables:UntagResource"
      ],
      "Resource": "arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-bucket",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",
            "owner",
            "cost-center"
          ]
        }
      }
    }
  ]
}
```

1.4 - Utilizzo della chiave s3tables: condition TableBucketTag

In questa policy IAM, l'istruzione condition consente l'accesso ai dati del bucket della tabella solo se il bucket della tabella ha la chiave Environment e il valore del tag. Production s3tables:TableBucketTag/<tag-key>Si differenzia dalla chiave di aws:ResourceTag/<tag-key> condizione perché, oltre a controllare l'accesso ai bucket di tabelle in base ai relativi tag, consente di controllare l'accesso alle tabelle in base ai tag presenti nel bucket di tabella principale.

```
{
  "Version": "2012-10-17",
```

```
"Statement": [  
  {  
    "Sid": "AllowAccessToSpecificTables",  
    "Effect": "Allow",  
    "Action": "*",  
    "Resource": "arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket/*",  
    "Condition": {  
      "StringEquals": {  
        "s3tables:TableBucketTag/Environment": "Production"  
      }  
    }  
  }  
]
```

Gestione dei tag per i bucket di tabelle

Puoi aggiungere o gestire tag per i bucket di tabelle S3 utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI), gli AWS SDK o utilizzando le API S3:, e. [TagResource](#) [UntagResource](#) [ListTagsForResource](#) Per ulteriori informazioni, consulta gli argomenti seguenti:

Argomenti

- [Creazione di bucket di tabelle con tag](#)
- [Aggiungere un tag a un bucket di tabella](#)
- [Visualizzazione dei bucket tags della tabella](#)
- [Eliminazione di un tag da un bucket della tabella](#)

Creazione di bucket di tabelle con tag

Puoi etichettare i bucket di tabelle Amazon S3 quando li crei. Non sono previsti costi aggiuntivi per l'utilizzo dei tag nei bucket di tabelle oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sull'etichettatura dei bucket di tabella, consulta. [Utilizzo dei tag con i bucket di tabelle S3](#)

Permissions

Per creare un bucket di tabella con tag, devi disporre delle seguenti autorizzazioni:

- s3tables:CreateTableBucket

- `s3tables:TagResource`

Risoluzione degli errori

Se riscontri un errore durante il tentativo di creare un bucket di tabella con tag, puoi fare quanto segue:

- Verifica di avere i requisiti [Permissions](#) per creare il bucket di tabella e applicarvi un tag.
- Controllare la policy dell'utente IAM per eventuali condizioni del controllo degli accessi basato su attributi (ABAC). La tua policy potrebbe richiedere di etichettare i bucket della tabella con solo chiavi e valori di tag specifici. Per ulteriori informazioni su ABAC ed esempi di policy ABAC per i table bucket, vedi [ABAC for S3 table bucket](#).

Fasi

Puoi creare un bucket di tabelle con tag applicati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 Tables e gli SDK. AWS

Utilizzo della console S3

Per creare un bucket di tabelle con tag utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Per creare un nuovo bucket da tavolo, scegli Crea bucket da tavolo.
4. Inserisci un nome per il bucket della tabella. Per ulteriori informazioni, consulta [Regole di denominazione di bucket di tabelle, tabelle e spazio dei nomi di Amazon S3](#).
5. Nella pagina Crea bucket di tabelle, c'è una sezione Tag.
6. Scegli Aggiungi nuovo tag per aprire l'editor di tag e inserisci una coppia chiave-valore di tag. La chiave di tag è obbligatoria, mentre il valore è facoltativo.
7. Per aggiungere un altro tag, scegli nuovamente Aggiungi nuovo tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
8. Specifica le opzioni rimanenti per il nuovo bucket di tabelle. Per ulteriori informazioni, consulta [Creazione di un bucket di tabelle](#).
9. Seleziona Crea bucket di tabelle.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 Tables per la creazione di un bucket di tabelle con tag, consulta la seguente sezione nel riferimento alle API di Amazon Simple Storage Service:

- [CreateTableBucket](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come creare un bucket di tabelle con tag utilizzando. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Quando si crea un bucket di tabelle è necessario fornire i dettagli di configurazione. Per ulteriori informazioni, consulta [Creazione di un bucket di tabelle](#). È inoltre necessario assegnare un nome al bucket di tabella con un nome che segua la convenzione di denominazione del bucket di tabella. Per ulteriori informazioni, consulta [Regole di denominazione di bucket di tabelle, tabelle e spazio dei nomi di Amazon S3](#).

Richiesta:

```
aws --region us-west-2 \  
s3tables create-table-bucket \  
--tags '{"Department":"Engineering"}' \  
--name amzn-s3-demo-table-bucket
```

Aggiungere un tag a un bucket di tabella

Puoi aggiungere tag ai bucket di tabelle Amazon S3 e modificare questi tag. Per ulteriori informazioni sull'etichettatura dei bucket di tabelle, consulta. [Utilizzo dei tag con i bucket di tabelle S3](#)

Permissions

Per aggiungere un tag a un bucket di tabella, devi disporre delle seguenti autorizzazioni:

- `s3tables:TagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di aggiungere un tag a un bucket di tabella, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per aggiungere un tag a un bucket di tabella.
- Se hai tentato di aggiungere una chiave tag che inizia con il prefisso AWS riservato `aws :`, modifica la chiave del tag e riprova.
- La chiave tag è obbligatoria. Inoltre, assicurati che la chiave del tag e il valore del tag non superino la lunghezza massima dei caratteri e non contengano caratteri soggetti a restrizioni. Per ulteriori informazioni, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

Fasi

Puoi aggiungere tag ai bucket di tabelle utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI), l'API REST di Amazon S3 Tables e gli SDK. AWS

Utilizzo della console S3

Per aggiungere tag a un bucket di tabelle utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Scegli il nome del bucket della tabella.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri la sezione Tag e scegli Aggiungi nuovo tag.
6. Viene visualizzata la pagina Aggiungi tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
7. Se si aggiunge un nuovo tag con lo stesso nome di chiave di un tag esistente, il valore del nuovo tag sovrascrive il valore del tag esistente.
8. In questa pagina è anche possibile modificare i valori dei tag esistenti.
9. Dopo aver aggiunto i tag, scegli Salva le modifiche.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'aggiunta di tag a un bucket di tabelle, consulta la seguente sezione nell'Amazon Simple Storage Service API Reference:

- [TagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come aggiungere tag a un bucket di tabella utilizzando il. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Richiesta:

```
aws --region us-west-2 \  
s3tables tag-resource \  
--resource-arn arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket \  
--tags '{"Department":"Engineering"}'
```

Visualizzazione dei bucket tags della tabella

Puoi visualizzare o elencare i tag applicati ai bucket di tabelle Amazon S3. Per ulteriori informazioni sull'etichettatura dei bucket di tabelle, consulta. [Utilizzo dei tag con i bucket di tabelle S3](#)

Permissions

Per visualizzare i tag applicati a un bucket di tabella, è necessario disporre delle seguenti autorizzazioni:

- `s3tables:ListTagsForResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di elencare o visualizzare i tag di un bucket di tabella, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per visualizzare i tag del bucket della tabella.

Fasi

Puoi visualizzare i tag applicati ai bucket di tabelle utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare i tag applicati a un bucket di tabelle utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Scegli il nome del bucket della tabella.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag per visualizzare tutti i tag applicati al bucket della tabella.
6. La sezione Tag mostra i User-defined tag per impostazione predefinita. Puoi selezionare la scheda dei tag AWS generati per visualizzare i tag applicati al bucket della tabella dai AWS servizi.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la visualizzazione dei tag applicati a un bucket di tabelle, consulta la seguente sezione nel riferimento alle API di Amazon Simple Storage Service:

- [ListTagsforResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come visualizzare i tag applicati a un bucket di tabella. Per utilizzare il comando, sostituiscili *user input placeholders* con le tue informazioni.

Richiesta:

```
aws --region us-west-2 \  
s3tables list-tags-for-resource \  
--resource-arn arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket/table/example_table
```

Risposta con tag:

```
{
```

```
"tags": {  
  "project": "Trinity",  
  "code": "123456"  
}
```

Risposta senza tag:

```
{  
  "Tags": []  
}
```

Eliminazione di un tag da un bucket della tabella

Puoi rimuovere i tag dai bucket di tabelle Amazon S3. Per ulteriori informazioni sull'etichettatura dei bucket di tabelle, consulta [Utilizzo dei tag con i bucket di tabelle S3](#)

Note

Se elimini un tag e in seguito scopri che è stato utilizzato per tenere traccia dei costi o per il controllo degli accessi, puoi aggiungere nuovamente il tag al bucket della tabella.

Permissions

Per eliminare un tag da un bucket di tabella, devi disporre della seguente autorizzazione:

- `s3tables:UntagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di eliminare un tag da un bucket di tabella, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per eliminare un tag da un bucket di tabella.

Fasi

Puoi eliminare i tag dai bucket di tabelle utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 Tables e gli SDK. AWS

Utilizzo della console S3

Per eliminare i tag da un bucket di tabelle utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Scegli il nome del bucket della tabella.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag e seleziona la casella di controllo accanto al tag o ai tag che desideri eliminare.
6. Scegliere Elimina.
7. Viene visualizzato il pop-up Elimina tag definiti dall'utente che chiede di confermare l'eliminazione del tag o dei tag selezionati.
8. Seleziona Elimina per confermare.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'eliminazione di tag da un bucket di tabelle, consulta la seguente sezione nell'Amazon Simple Storage Service API Reference:

- [UnTagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI nella Guida per l'utente](#). AWS Command Line Interface

Il seguente esempio CLI mostra come eliminare i tag da un bucket di tabella utilizzando il. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Richiesta:

```
aws --region us-west-2 \  
s3tables untag-resource \  
--resource-arn arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket \  
--tags-keys '["Department"]'
```

Manutenzione di Tabelle S3

Amazon S3 esegue automaticamente la manutenzione per migliorare le prestazioni delle tabelle nei bucket di tabelle S3. Eseguita a livello bucket di tabelle e di singola tabella, la manutenzione include quanto segue:

Manutenzione a livello di bucket di tabelle:

- Rimozione dei file senza riferimenti: ripulisce i file orfani per ottimizzare l'utilizzo e i costi dello storage.

Table-level manutenzione:

- Compattazione dei file: consolida i file di piccole dimensioni per migliorare le prestazioni delle query e ridurre i costi di archiviazione.
- Gestione delle snapshot: controlla la cronologia delle versioni della tabella e impedisce una crescita eccessiva dei metadati.

Queste opzioni sono attivate per impostazione predefinita. È possibile modificare o disattivare queste operazioni tramite i file di configurazione della manutenzione.

Oltre a queste opzioni, puoi anche abilitare e configurare le impostazioni di scadenza dei record per le tabelle. Con questa opzione, Amazon S3 rimuove automaticamente i record da una tabella quando i record scadono.

Argomenti

- [Stato dei processi di manutenzione di Tabelle S3](#)
- [Manutenzione dei bucket di tabelle](#)
- [Manutenzione delle tabelle](#)
- [Scadenza del record per le tabelle](#)
- [Considerazioni e limitazioni per i processi di manutenzione](#)

Stato dei processi di manutenzione di Tabelle S3

I processi di manutenzione di Tabelle S3 vengono eseguiti periodicamente per le tabelle o i bucket di Tabelle S3. È possibile eseguire query sullo stato di tali processi con l'API `GetTableMaintenanceJobStatus`.

Per conoscere lo stato dei lavori di manutenzione utilizzando AWS CLI

Nel seguente esempio lo stato dei processi di manutenzione viene ottenuto utilizzando l'API `GetTableMaintenanceJobStatus`.

```
aws s3tables get-table-maintenance-job-status \
  --table-bucket-arn="arn:aws:s3tables:arn:aws::111122223333:bucket/amzn-s3-demo-bucket1" \
  --namespace="mynamespace" \
  --name="testtable"
```

Per ulteriori informazioni, consulta [get-table-maintenance-job-status](#) nella documentazione di riferimento dei comandi della AWS CLI .

I processi di manutenzione di Tabelle S3 possono passare da uno dei quattro stati possibili all'altro:

- Successful
- Failed
- Disabled
- Not_Yet_Run

I processi con stato Non riuscito includeranno un messaggio di errore. Nell'elenco seguente sono riportati i possibili messaggi di errore.

- È stata rilevata un'eccezione di convalida Iceberg durante il tentativo di leggere la tabella. Assicurati che la tua tabella sia leggibile, che sia conforme alla specifica Iceberg e che contenga solo percorsi S3 che iniziano con il tuo alias di Tabelle S3.
- La gestione delle snapshot di Iceberg attualmente non supporta tag o riferimenti definiti dall'utente.
- La configurazione di manutenzione delle tabelle Iceberg non è compatibile con le proprietà delle tabelle "history.expire.max-snapshot-age-ms" e "history.expire.min-snapshots-to-keep".
- La gestione delle snapshot di Iceberg e la rimozione di file senza riferimenti non sono supportate quando la proprietà della tabella "gc.enabled" è false. Assicurati che questa proprietà non sia impostata o impostata esplicitamente su true.
- Impossibile effettuare il commit a causa di metadati non aggiornati. La manutenzione verrà ripetuta alla prossima occasione disponibile.

- Accesso insufficiente per eseguire la manutenzione delle tabelle. Assicurati che la chiave utilizzata per crittografare la tabella sia attiva, esista e disponga di una policy delle risorse che garantisca l'accesso al principale `maintenance.s3tables.amazonaws.com` del servizio S3.

Note

Per ulteriori informazioni sulle AWS KMS autorizzazioni per le tabelle S3, vedere. [Requisiti di autorizzazione per la crittografia delle tabelle S3 SSE-KMS](#)

- Errore interno

Manutenzione dei bucket di tabelle

Amazon S3 offre operazioni di manutenzione per migliorare la gestione e le prestazioni dei bucket di tabelle. La seguente opzione è abilitata per tutti i bucket di tabelle per impostazione predefinita. È possibile modificare o disabilitare questa opzione specificando un file di configurazione di manutenzione per il bucket di tabelle.

La modifica di questa configurazione richiede l'autorizzazione `s3tables:PutTableBucketMaintenanceConfiguration`.

Argomenti

- [Rimozione di file senza riferimenti](#)
- [Considerazioni e limitazioni](#)

Rimozione di file senza riferimenti

La rimozione di file senza riferimenti identifica ed elimina tutti gli oggetti a cui non fa riferimento alcuno snapshot delle tabelle. Nell'ambito della policy di rimozione dei file senza riferimenti, è possibile configurare due proprietà: `unreferencedDays` (3 giorni per impostazione predefinita) e `nonCurrentDays` (10 giorni per impostazione predefinita).

Qualsiasi oggetto senza riferimenti della tabella e precedente alla proprietà `unreferencedDays` viene contrassegnato da S3 come non corrente. S3 elimina gli oggetti non correnti dopo il numero di giorni specificato dalla proprietà `nonCurrentDays`.

 Note

L'eliminazione di oggetti non correnti è permanente, pertanto gli oggetti non possono essere recuperati.

Per visualizzare o recuperare oggetti contrassegnati come non correnti, è necessario contattare Supporto AWS. Per informazioni su come contattare Supporto AWS, consulta [Contatti AWS](#) o Documentazione. [Supporto AWS](#)

La rimozione di file senza riferimenti determina gli oggetti da eliminare dalla tabella con riferimento solo a quella tabella. Qualsiasi riferimento fatto a questi oggetti all'esterno della tabella non impedirà che la rimozione di file senza riferimenti elimini un oggetto.

La disabilitazione della rimozione di file senza riferimenti non influirà sui processi in corso. La nuova configurazione avrà effetto per il processo successivo dopo la modifica della configurazione. Per ulteriori informazioni, consulta i prezzi in [Prezzi di Amazon S3](#).

È possibile configurare la rimozione di file senza riferimenti solo a livello di bucket di tabelle. Questa configurazione verrà applicata a ogni tabella del bucket.

Per configurare la rimozione di file senza riferimenti utilizzando AWS CLI

Il seguente esempio imposterà `unreferencedDays` su 4 giorni e `nonCurrentDays` su 10 giorni utilizzando l'API `PutTableBucketMaintenanceConfiguration`.

```
aws s3tables put-table-bucket-maintenance-configuration \
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
  --type icebergUnreferencedFileRemoval \
  --value '{"status":"enabled","settings":{"icebergUnreferencedFileRemoval":
{"unreferencedDays":4,"nonCurrentDays":10}}}'
```

Per ulteriori informazioni, consulta [put-table-bucket-maintenance-configuration](#) nella documentazione di riferimento dei comandi della AWS CLI.

Considerazioni e limitazioni

Per ulteriori informazioni su limiti e considerazione aggiuntivi per la rimozione di file senza riferimenti, consulta [the section called “Considerazioni e limitazioni”](#).

Manutenzione delle tabelle

Tabelle S3 consente di usufruire di operazioni di manutenzione in grado di migliorare la gestione e le prestazioni delle singole tabelle. Le seguenti opzioni sono abilitate per impostazione predefinita per tutte le tabelle nei bucket di tabelle. È possibile modificarle o disattivarle specificando i file di configurazione della manutenzione per la tabella S3.

Per modificare questa configurazione sono necessarie le autorizzazioni `s3tables:GetTableMaintenanceConfiguration` e `s3tables:PutTableMaintenanceConfiguration`.

Note

È possibile tenere traccia delle operazioni di manutenzione automatizzata di S3 Tables sulle tabelle tramite CloudTrail i registri, per ulteriori informazioni, vedere. [CloudTrail eventi di gestione per la manutenzione di S3 Tables](#)

Argomenti

- [Compattazione](#)
- [Gestione degli snapshot](#)
- [Considerazioni e limitazioni](#)

Compattazione

La compattazione è configurata a livello di tabella e combina più oggetti più piccoli in un numero inferiore di oggetti più grandi per migliorare le prestazioni delle query Apache Iceberg. Per combinare gli oggetti, la compattazione applica anche gli effetti delle eliminazioni a livello di riga alla tabella.

La compattazione è abilitata per impostazione predefinita per tutte le tabelle, con una dimensione del file di destinazione predefinita di 512 MB oppure un valore personalizzato specificato compreso tra 64 MB e 512 MB. I file compattati vengono scritti come la snapshot più recente della tabella.

Note

La compattazione è supportata sui file di tipo Apache Parquet, Avro e ORC.

Strategie di compattazione

È possibile scegliere tra diverse strategie di compattazione che possono aumentare ulteriormente le prestazioni delle query a seconda dei modelli di query e dell'ordinamento delle tabelle.

Tabelle S3 supporta le seguenti strategie di compattazione per le tabelle:

- Auto (impostazione predefinita)
 - Amazon S3 seleziona la migliore strategia di compattazione in base all'ordinamento delle tabelle. Questa è la strategia di compattazione predefinita per tutte le tabelle.
 - Per le tabelle con un ordinamento definito nei metadati, auto applicherà automaticamente la compattazione `sort`.
 - Per le tabelle senza un ordinamento, auto per impostazione predefinita utilizzerà la compattazione `binpack`.
- Binpack
 - Combina file di piccole dimensioni in file più grandi, in genere con dimensioni superiori a 100 MB, applicando eventuali eliminazioni in sospeso. Questa è la strategia di compattazione predefinita per le tabelle non ordinate.
- Ordina
 - Organizza i dati in base a colonne specifiche che automaticamente vengono ordinate gerarchicamente durante la compattazione, migliorando le prestazioni delle query per le operazioni di filtro. Questa strategia è consigliata quando le query vengono spesso filtrate in base a colonne specifiche. Quando si utilizza questa strategia, Tabelle S3 applica automaticamente l'ordinamento gerarchico alle colonne quando `sort_order` è definito nelle proprietà della tabella.
- Z-order
 - Ottimizza l'organizzazione dei dati fondendo più attributi in un unico valore scalare che può essere utilizzato per l'ordinamento, consentendo query efficienti su più dimensioni. Questa strategia è consigliata quando è necessario eseguire query sui dati su più dimensioni contemporaneamente. Questa strategia richiede la definizione di un ordinamento nelle proprietà della tabella Iceberg utilizzando la proprietà della tabella `sort_order`.

La compattazione comporta costi aggiuntivi. Le strategie di compattazione `z-order` e `sort` possono comportare un costo maggiore rispetto a `binpack`. Per ulteriori informazioni, consulta i prezzi in [Prezzi di Amazon S3](#).

Esempi di compattazione

I seguenti esempi mostrano come configurare la compattazione delle tabelle.

Per configurare la dimensione del file di destinazione della compattazione utilizzando AWS CLI

La dimensione minima del file di compattazione di destinazione è 64 MB, la massima è 512 MB.

Il seguente esempio cambierà la dimensione del file di destinazione in 256 MB utilizzando l'API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
  bucket1 \
  --type icebergCompaction \
  --namespace mynamespace \
  --name testtable \
  --value='{"status":"enabled","settings":{"icebergCompaction":
  {"targetFileSizeMB":256}}}'
```

Per ulteriori informazioni, consulta [put-table-maintenance-configuration](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per configurare la strategia di compattazione utilizzando AWS CLI

L'esempio seguente cambia la strategia di compattazione in sort utilizzando l'API `PutTableMaintenanceConfiguration`. Quando si imposta la compattazione, è possibile scegliere tra le seguenti strategie di compattazione: auto, binpack, sort o z-order

Note

Per impostare la strategia di compattazione su sort o z-order sono necessari i seguenti prerequisiti:

- Un ordinamento definito nelle proprietà delle tabelle Iceberg.
- L'autorizzazione `s3tables:GetTableData`.

```
aws s3tables put-table-maintenance-configuration \
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
  table-bucket \
  --type icebergCompaction \
```

```
--namespace mynamespace \  
--name testtable \  
--value='{"status":"enabled","settings":{"icebergCompaction":  
{"strategy":"sort"}}}'
```

Per ulteriori informazioni, consulta [put-table-maintenance-configuration](#) nella documentazione di riferimento dei comandi della AWS CLI .

Per disattivare la compattazione utilizzando AWS CLI

Il seguente esempio disattiverà la compattazione utilizzando l'API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \  
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
table-bucket \  
--type icebergCompaction \  
--namespace mynamespace \  
--name testtable \  
--value='{"status":"disabled","settings":{"icebergCompaction":  
{"targetFileSizeMB":256}}}'
```

Per ulteriori informazioni, consulta [put-table-maintenance-configuration](#) nella documentazione di riferimento dei comandi della AWS CLI .

Gestione degli snapshot

La gestione degli snapshot determina il numero di snapshot attivi per la tabella. Si basa su `MinimumSnapshots` (1 per impostazione predefinita) e `MaximumSnapshotAge` (120 ore per impostazione predefinita). La gestione degli snapshot scade e rimuove gli snapshot delle tabelle in base a queste configurazioni.

Quando uno snapshot scade, Amazon S3 contrassegna come non correnti tutti gli oggetti a cui fa riferimento tale snapshot. Tali oggetti non correnti vengono eliminati dopo il numero di giorni specificato dalla proprietà `NoncurrentDays` nella policy di rimozione dei file senza riferimenti.

Note

L'eliminazione di oggetti non correnti è permanente, pertanto gli oggetti non possono essere recuperati.

Per visualizzare o recuperare oggetti contrassegnati come non correnti, è necessario contattare Supporto AWS. Per informazioni su come contattare Supporto AWS, consulta [Contatti AWS](#) o la [Supporto AWS Documentazione](#).

La gestione degli snapshot determina gli oggetti da eliminare dalla tabella che fanno riferimento solo a tale tabella. I riferimenti a questi oggetti esterni alla tabella non impediscono alla gestione degli snapshot di eliminare un oggetto.

Note

La gestione delle istantanee non supporta i valori di conservazione configurati come proprietà della Apache Iceberg tabella nel metadata .json file o tramite un comando ALTER TABLE SET TBLPROPERTIES SQL. Se sussiste una delle seguenti condizioni, la gestione delle istantanee fallirà per l'intera tabella e Amazon S3 non scadrà né rimuoverà alcuna istantanea:

- User-defined tag o rami: se nella tabella sono presenti tag o rami definiti dall'utente, la gestione delle istantanee avrà esito negativo per l'intera tabella. Ciò vale anche se il tag o il ramo ha un breve periodo di conservazione. Per ripristinare la scadenza automatica delle istantanee, rimuovi tutti i tag e i rami definiti dall'utente dalla tabella.
- Proprietà della tabella di conservazione delle istantanee Iceberg: se la `history.expire.min-snapshots-to-keep` proprietà `history.expire.max-snapshot-age-ms` or è impostata come proprietà della Apache Iceberg tabella, la gestione delle istantanee avrà esito negativo per l'intera tabella indipendentemente dal valore configurato. Per ripristinare la scadenza automatica delle istantanee, rimuovi queste proprietà:

```
ALTER TABLE mydb.mytable UNSET TBLPROPERTIES ('history.expire.max-snapshot-age-ms');  
ALTER TABLE mydb.mytable UNSET TBLPROPERTIES ('history.expire.min-snapshots-to-keep');
```

Per diagnosticare gli errori di gestione delle istantanee, utilizza l'GetTableMaintenanceJobStatusAPI o esegui il comando seguente. AWS CLI Se la gestione delle istantanee non è riuscita, la risposta include uno FAILED stato con un messaggio che descrive la causa dell'errore.

```
aws s3tables get-table-maintenance-job-status \
```

```
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-  
demo-table-bucket \  
--namespace my_namespace \  
--name my_table
```

È possibile configurare la gestione degli snapshot solo a livello di tabella. Per ulteriori informazioni, consulta i prezzi in [Prezzi di Amazon S3](#).

Esempi di gestione degli snapshot

I seguenti esempi mostrano come configurare la gestione degli snapshot delle tabelle.

Per configurare la gestione delle istantanee utilizzando AWS CLI

Il seguente esempio imposterà MinimumSnapshots su 10 e MaximumSnapshotAge su 2.500 ore utilizzando l'API PutTableMaintenanceConfiguration.

```
aws s3tables put-table-maintenance-configuration \  
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
table-bucket \  
--namespace my_namespace \  
--name my_table \  
--type icebergSnapshotManagement \  
--value '{"status":"enabled","settings":{"icebergSnapshotManagement":  
{"minSnapshotsToKeep":10,"maxSnapshotAgeHours":2500}}}'
```

Per disattivare la gestione delle istantanee utilizzando AWS CLI

Il seguente esempio disabilita la gestione degli snapshot utilizzando l'API PutTableMaintenanceConfiguration.

```
aws s3tables put-table-maintenance-configuration \  
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
table-bucket \  
--namespace my_namespace \  
--name my_table \  
--type icebergSnapshotManagement \  
--value '{"status":"disabled","settings":{"icebergSnapshotManagement":  
{"minSnapshotsToKeep":1,"maxSnapshotAgeHours":120}}}'
```

Per ulteriori informazioni, consulta [put-table-maintenance-configuration](#) nella documentazione di riferimento dei comandi della AWS CLI .

Considerazioni e limitazioni

Per ulteriori informazioni su considerazioni e limitazioni aggiuntive relative alla compattazione e alla gestione degli snapshot, consulta [the section called “Considerazioni e limitazioni”](#).

Note

Tabelle Amazon S3 applica la dimensione predefinita del gruppo di righe in formato Parquet di 128 MB.

Scadenza del record per le tabelle

Per impostazione predefinita, i record nelle tabelle S3 non scadono. Per ridurre al minimo i costi di archiviazione per le tabelle, puoi abilitare e configurare la scadenza dei record per le tabelle. Con questa opzione, Amazon S3 rimuove automaticamente i record da una tabella quando i record scadono.

Se abiliti la scadenza dei record per una tabella, specifichi il numero di giorni di conservazione dei record nella tabella prima della scadenza dei record. Può trattarsi di un numero qualsiasi di giorni compreso tra 1 giorno e 2.147.483.647 giorni. Ad esempio, per conservare i record della tabella per un anno, specifica i giorni. 365 I record vengono quindi conservati per 365 giorni. Dopo 365 giorni, i record scadono e Amazon S3 li rimuove automaticamente.

Puoi abilitare e configurare la scadenza dei record per le tabelle AWS gestite che memorizzano set di dati specifici provenienti da determinati Servizi AWS, attualmente Amazon S3 Storage Lens e Amazon Catalog. SageMaker Le opzioni di scadenza dei record non sono attualmente disponibili per altre tabelle AWS gestite. L'eccezione sono le tabelle del journal con metadati di Amazon S3. Le tabelle di journal utilizzano impostazioni di scadenza dei record distinte specificate a livello di servizio. Per informazioni sulla configurazione della scadenza dei record per questo tipo di tabella, vedere [Scadenza dei record della tabella del diario](#). Tieni presente che le opzioni di scadenza dei record non sono disponibili per le tabelle S3 che crei.

Dopo aver abilitato la scadenza dei record per una tabella, puoi disabilitarla in qualsiasi momento. Amazon S3 interrompe quindi la scadenza e rimuove i record dalla tabella.

Argomenti

- [Come funziona la scadenza dei record](#)
- [Configurazione della scadenza dei record per una tabella](#)
- [Monitoraggio della scadenza dei record per una tabella](#)
- [Considerazioni](#)

Come funziona la scadenza dei record

La scadenza dei record rimuove automaticamente i record da una tabella S3 quando i record sono più vecchi del numero di giorni specificato nelle impostazioni di scadenza dei record per la tabella. Per determinare quando scadono i record, Amazon S3 utilizza timestamp specifici nei record. La scelta della colonna timestamp deriva direttamente dallo schema della tabella per una tabella. Non è necessario specificare quale colonna di timestamp utilizzare. Le tabelle sono gestite da AWS e Amazon S3 sceglie automaticamente la colonna appropriata da utilizzare quando abiliti la scadenza dei record per una tabella.

Puoi abilitare e configurare le impostazioni di scadenza dei record per le tabelle AWS gestite che memorizzano metriche specifiche di Amazon S3 Storage Lens o metadati specifici di Amazon Catalog. SageMaker Le opzioni di scadenza dei record sono disponibili per le seguenti tabelle AWS gestite per tali servizi:

- Lente di archiviazione S3: `bucket_property_metrics`, `default_activity_metrics`, `default_storage_metric`, `expanded_prefixes_activity_metrics`, `expanded_prefixes_storage_metrics`. Per determinare quando scadono i record in queste tabelle, Amazon S3 utilizza il `report_time` campo nei record.
- SageMaker Catalogo Amazon —. ASSET Per determinare quando scadono i record in questa tabella, Amazon S3 utilizza il `snapshot_time` campo nei record.

Dopo aver abilitato la scadenza dei record per una tabella, Amazon S3 inizia a eseguire processi di scadenza dei record che eseguono le seguenti operazioni per la tabella:

1. Identifica i record più vecchi dell'impostazione di scadenza specificata.
2. Crea una nuova istantanea che escluda i riferimenti ai record scaduti.

La rimozione si basa anche sulla scadenza dell'istantanea e sulle impostazioni di rimozione dei file senza riferimenti nelle impostazioni di configurazione di manutenzione della tabella. Per ulteriori informazioni su queste impostazioni, vedere. [Manutenzione delle tabelle](#)

 Warning

Amazon S3 scade e rimuove i record entro 24-48 ore dopo che i record sono diventati idonei per la scadenza. I record della tabella vengono rimossi dall'ultima istantanea. I dati e l'archiviazione dei record vengono rimossi tramite le operazioni di manutenzione della tabella. I record della tabella non possono essere recuperati dopo la loro scadenza.

Configurazione della scadenza dei record per una tabella

Puoi abilitare, configurare e gestire in altro modo le impostazioni di scadenza dei record per una tabella S3 utilizzando la console Amazon S3, l'API REST di Amazon S3, AWS Command Line Interface (AWS CLI) o gli SDK. AWS

Prima di provare a eseguire queste attività per una tabella, assicurati di disporre delle seguenti autorizzazioni AWS Identity and Access Management (IAM):

- `s3tables:GetTableRecordExpirationConfiguration`— Questa azione consente di accedere alle impostazioni correnti di scadenza dei record per le tabelle.
- `s3tables:PutTableRecordExpirationConfiguration`— Questa azione consente di abilitare, configurare e disabilitare le impostazioni di scadenza dei record per le tabelle.
- `s3tables:GetTableRecordExpirationJobStatus`— Questa azione consente di monitorare lo stato delle operazioni di scadenza dei record (job) per le tabelle e di accedere alle metriche per le operazioni.

Le sezioni seguenti spiegano come abilitare, configurare e disabilitare le impostazioni di scadenza dei record per una tabella utilizzando la console Amazon S3 e il. AWS CLI Per eseguire queste attività con l'API REST di Amazon S3 o un AWS SDK, utilizza l'operazione.

[PutTableRecordExpirationConfiguration](#) Per ulteriori informazioni, consulta [Sviluppo con Amazon S3](#) nell'API Reference di Amazon Simple Storage Service.

Utilizzo della console S3

Per abilitare e configurare le impostazioni di scadenza dei record per una tabella S3 utilizzando la console, segui questi passaggi.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nella pagina Table buckets, scegli il bucket in cui è archiviata la tabella.
4. Nella scheda Tabelle, scegli la tabella.
5. Nella scheda Manutenzione, nella sezione Scadenza del record, scegli Modifica.
6. In Scadenza del record, scegli Abilita.
7. Per Giorni dopo i quali scadono i record, inserisci il numero di giorni di conservazione dei record nella tabella. Può essere qualsiasi numero intero compreso tra 1 e 2.147.483.647. Ad esempio, per conservare i record per un anno, inserisci. **365**

 Warning

Quando si determina il periodo di conservazione appropriato per i record nella tabella, si noti che i record non possono essere recuperati dopo la loro scadenza.

8. Scegli Save changes (Salva modifiche).

Per modificare successivamente il periodo di conservazione, ripeti i passaggi precedenti.

Per disattivare successivamente la scadenza dei record, ripetere i passaggi da 1 a 5. Quindi, per il passaggio 6, scegli Disabilita. Al termine, scegliere Save changes (Salva modifiche).

Utilizzo di AWS CLI

Per configurare e gestire le impostazioni di scadenza dei record per una tabella S3 utilizzando il comando AWS CLI, esegui il [put-table-record-expiration-configuration](#) comando.

Puoi iniziare creando un file JSON che contiene le impostazioni di scadenza dei record da applicare alla tabella. L'esempio seguente mostra il contenuto di un file JSON che consente la scadenza dei record per una tabella. Specifica inoltre un periodo di conservazione di 30 giorni per i record della tabella. In altre parole, specifica che i record della tabella devono scadere dopo 30 giorni.

```
{
  "status": "enabled",
  "settings": {
    "days": 30
  }
}
```

Per utilizzare l'esempio precedente, sostituiscili *user input placeholders* con le tue informazioni.

 Warning

Quando si determina il periodo di conservazione appropriato per i record nella tabella, si noti che i record non possono essere recuperati dopo la loro scadenza.

Per disattivare la scadenza dei record per una tabella, specificate `disabled` il `status` campo e omettete l'oggetto `settings` dal file. Ad esempio:

```
{
  "status": "disabled"
}
```

Dopo aver creato un file JSON con le impostazioni da applicare, esegui il `put-table-record-expiration-configuration` comando. Per il `table-arn` parametro, specifica l'Amazon Resource Name (ARN) della tabella. Per il `value` parametro, specifica il nome del file che memorizza le impostazioni.

Ad esempio, il comando seguente aggiorna le impostazioni di scadenza dei record per una tabella. Le impostazioni sono specificate in un file denominato *record-expiration-config.json*.

```
aws s3tables put-table-record-expiration-configuration \
  --table-arn arn:aws:s3tables:us-east-1:123456789012:bucket/amzn-s3-demo-table-
  bucket/table/amzn-s3-demo-table \
  --value file:///./record-expiration-config.json
```

Per utilizzare l'esempio precedente, sostituiscili *user input placeholders* con le tue informazioni.

Monitoraggio della scadenza dei record per una tabella

Per monitorare lo stato e i risultati delle operazioni di scadenza dei record per le tabelle S3, usa l'[GetTableRecordExpirationJobStatus](#) operazione o, se stai usando il AWS CLI, esegui il [get-table-record-expiration-job-status](#) comando. Nella richiesta, specifica l'Amazon Resource Name (ARN) della tabella.

Ad esempio, il AWS CLI comando seguente recupera lo stato delle operazioni di scadenza dei record per una tabella specifica in un bucket di tabelle. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables get-table-record-expiration-job-status \  
  --table-arn arn:aws:s3tables:us-east-1:123456789012:bucket/amzn-s3-demo-table-  
  bucket/table/amzn-s3-demo-table
```

Se la richiesta ha esito positivo, riceverai una risposta che fornisce dettagli come l'ultima volta che Amazon S3 ha eseguito le operazioni di scadenza dei record per la tabella e lo stato di tale esecuzione. Se l'esecuzione più recente ha avuto esito positivo, la risposta include anche le metriche di elaborazione, ad esempio il numero di file e record di dati rimossi e la dimensione totale dei dati rimossi. Se si sono verificati errori durante l'esecuzione più recente, la risposta include un messaggio di errore che descrive il motivo per cui l'esecuzione non è riuscita.

Considerazioni

Quando configuri e gestisci le impostazioni di scadenza dei record per le tabelle S3 AWS gestite, tieni presente quanto segue:

- La scadenza dei record è disponibile solo per alcune tabelle AWS gestite create da supported Servizi AWS, Amazon S3 Storage Lens e Amazon SageMaker Catalog. Inoltre, la scadenza dei record è disponibile solo per singole tabelle, non per interi bucket di tabelle.
- Per determinare quando scadono i record, Amazon S3 utilizza timestamp specifici nelle tabelle. Questi timestamp rappresentano quando i dati sono stati creati, non quando Amazon S3 ha inserito i record in una tabella. La colonna timestamp utilizzata dipende dal servizio che pubblica la tabella: per le metriche di S3 Storage Lens, il campo `e`, per i metadati di Amazon Catalog, il `report_time` campo. SageMaker `snapshot_time` Non puoi specificare quale campo utilizzare perché le tabelle sono gestite da AWS.
- Se si verificano ritardi nell'esportazione dei dati in una tabella, i record potrebbero diventare idonei alla scadenza prima del previsto. Per questo motivo, ti consigliamo di tenere conto dei potenziali ritardi nell'inserimento aggiungendo un buffer al periodo di conservazione nelle impostazioni di scadenza delle tabelle.
- I record scadono e vengono rimossi entro 24-48 ore dal momento in cui sono diventati idonei alla scadenza. Amazon S3 non ha una scadenza e rimuove i record immediatamente dopo che sono diventati idonei alla scadenza.
- I record non possono essere recuperati dopo la loro scadenza e la loro rimozione.

Considerazioni e limitazioni per i processi di manutenzione

Amazon S3 consente di usufruire di operazioni di manutenzione per migliorare le prestazioni delle tabelle o dei bucket delle tabelle S3. Tali opzioni comprendono la compattazione dei file, la gestione degli snapshot e la rimozione dei file senza riferimenti. Di seguito sono riportate le limitazioni e le considerazioni relative a queste opzioni di gestione.

Argomenti

- [Considerazioni sulla compattazione](#)
- [Considerazioni sulla gestione degli snapshot](#)
- [Considerazioni sulla rimozione di file senza riferimenti](#)
- [Limiti delle operazioni di manutenzione di tabelle S3 e bucket di tabelle e API correlate](#)

Considerazioni sulla compattazione

Alla compattazione si applicano le seguenti considerazioni. Per ulteriori informazioni sulla compattazione, consulta [the section called “Manutenzione delle tabelle”](#).

- La compattazione è supportata sui file di tipo Apache Parquet, Avro e ORC.
- Per impostazione predefinita, la compattazione scrive nuovi file in formato Apache Parquet. Per compattare invece i file in formato Avro o ORC, imposta la proprietà della tabella `write.format.default` su `avro` o `orc`.
- La compattazione non supporta i file di tipo Fixed.
- La compattazione non supporta i tipi di compressione: `brotli` e `lz4`.
- La compattazione avviene in base a una pianificazione automatica. Se desideri evitare gli addebiti associati alla compattazione, puoi disabilitarla manualmente per una tabella utilizzando l'operazione [PutTableMaintenanceConfiguration](#) API.

Note

Apache Iceberg utilizza un modello di concorrenza ottimistico insieme al rilevamento dei conflitti per arbitrare le transazioni di scrittura. Con una concorrenza ottimistica, le transazioni dell'utente e le transazioni di compattazione possono entrare in conflitto, causando la mancata riuscita delle transazioni. Se si verifica un conflitto, i processi di compattazione tenteranno nuovamente l'operazione in caso di errore. È consigliabile che le pipeline

implementino anche una logica di ripetizione per gestire le transazioni che non riescono a causa di operazioni in conflitto.

Considerazioni sulla gestione degli snapshot

Alla gestione degli snapshot si applicano le seguenti considerazioni. Per ulteriori informazioni sulla gestione degli snapshot, consulta [the section called “Manutenzione delle tabelle”](#).

- Gli snapshot verranno conservati solo quando entrambi i criteri saranno soddisfatti: il numero minimo di snapshot da conservare e il periodo di conservazione specificato.
- La gestione degli snapshot elimina i metadati degli snapshot scaduti da Apache Iceberg, evitando le query temporali per gli snapshot scaduti e, facoltativamente, eliminando i file di dati associati.
- La gestione degli snapshot non supporta i valori di conservazione configurati come proprietà della tabella Iceberg nel file `metadata.json` o tramite un comando SQL `ALTER TABLE SET TBLPROPERTIES`, inclusa la conservazione basata su ramo o tag. La gestione degli snapshot viene disattivata quando si configura una policy di conservazione basata su ramo o tag oppure quando si configura una policy di conservazione sul file `metadata.json` più lunga dei valori configurati tramite l'API `PutTableMaintenanceConfiguration`. In questi casi S3 non scadrà né rimuoverà gli snapshot e sarà necessario eliminare manualmente gli snapshot o rimuovere le proprietà dalla tabella Iceberg per evitare costi di archiviazione.

Considerazioni sulla rimozione di file senza riferimenti

Alla rimozione dei file senza riferimenti si applicano le seguenti considerazioni. Per ulteriori informazioni sulla rimozione di file senza riferimenti, consulta [the section called “Manutenzione dei bucket di tabelle”](#).

- La rimozione di file senza riferimenti elimina i file di dati e metadati a cui non fanno più riferimento i metadati Iceberg se la data di creazione è precedente al periodo di conservazione.

Limiti delle operazioni di manutenzione di tabelle S3 e bucket di tabelle e API correlate

Operazioni di manutenzione	Proprietà	Configurabile a livello di bucket di tabelle?	Configurabile a livello di tabella?	Valore predefinito	Valore minimo	Routine di manutenzione Iceberg correlata	Controllo dell'API di Tabelle S3
Compattazione	targetFileSizeMB	No	Sì	512 MB	64 MB	rewriteDataFiles	PutTableMaintenanceConfiguration
Gestione degli snapshot	minimumSnapshots	No	Sì	1	1	ExpireSnapshots retainLatest	PutTableMaintenanceConfiguration
Gestione degli snapshot	maximumSnapshotAge	No	Sì	120 ore	1 ora	ExpireSnapshots expireOlderThan	PutTableMaintenanceConfiguration
Rimozione di file senza riferimenti	unreferencedDays	Sì	No	3 giorni	1 giorno	deleteOrphanFiles	PutTableBucketMaintenanceConfiguration
Rimozione di file senza riferimenti	nonCurrentDays	Sì	No	10 giorni	1 giorno	N/A	PutTableBucketMaintenanceConfiguration

 Note

Tabelle Amazon S3 applica la dimensione predefinita del gruppo di righe in formato Parquet di 128 MB.

Ottimizzazione dei costi per tabelle con Intelligent-Tiering

È possibile ottimizzare automaticamente i costi di archiviazione per le tabelle utilizzando S3.

Intelligent-Tiering La classe di Intelligent-Tiering storage S3 Tables sposta automaticamente i dati al livello di accesso più conveniente quando i modelli di accesso cambiano. Quando si utilizza S3 Intelligent-Tiering, i dati a cui si accede meno frequentemente vengono automaticamente spostati su livelli a basso costo e trasferiti nuovamente al livello Frequent Access ogni volta che vi si accede nuovamente.

Tutti i dati vengono spostati tra i livelli senza costi di recupero, impatto sulle prestazioni o modifiche alla disponibilità. Inoltre, le operazioni di manutenzione delle tabelle, come la compattazione, sono ottimizzate in base ai modelli di accesso, elaborando solo i dati a cui si accede attivamente nel livello Frequent Access e riducendo i costi di manutenzione sui dati a cui si accede meno frequentemente nei livelli a basso costo.

Argomenti

- [Livelli di accesso alle tabelle S3 Intelligent-Tiering](#)
- [Auto-tiering comportamento con S3 Intelligent-Tiering](#)
- [Specificare S3 Intelligent-Tiering come classe di archiviazione](#)
- [Monitoraggio dell'utilizzo dello storage](#)

Livelli di accesso alle tabelle S3 Intelligent-Tiering

Quando la tabella è archiviata nella classe di Intelligent-Tiering storage S3, Amazon S3 monitora continuamente i modelli di accesso e sposta automaticamente i dati della tabella tra i livelli di accesso.

Il tiering avviene a livello di singolo file, quindi una singola tabella può avere file in diversi livelli in base ai modelli di accesso. I dati della tabella vengono spostati automaticamente su uno dei seguenti livelli di accesso in base ai modelli di accesso:

- **Accesso frequente:** il livello predefinito per tutti i file. I file di altri livelli tornano automaticamente al livello di accesso frequente quando vi si accede.
- **Accesso non frequente:** se non si accede a un file per 30 giorni consecutivi, questo passa al livello Accesso non frequente.
- **Accesso istantaneo all'archivio:** se non si accede a un file per 90 giorni consecutivi, si passa al livello Archive Instant Access.

Tutti i livelli offrono una latenza di millisecondi, prestazioni di throughput elevate e sono progettati per una disponibilità del 99,9% e una durata del 99,9%.

Auto-tiering comportamento con S3 Intelligent-Tiering

Le seguenti azioni costituiscono un accesso che sposta automaticamente i file dal livello Infrequent Access o dal livello Archive Instant Access al livello Frequent Access:

- Qualsiasi operazione di lettura o scrittura sui dati delle tabelle o sui file di metadati utilizzando `GetObject`, `PutObject` o azioni `CompleteMultipartUpload`
- `LoadTable` o `UpdateTable` azioni utilizzando [Iceberg REST API Operations](#)
- Operazioni di replica di S3 Tables

Le altre azioni non costituiscono un accesso che sposta automaticamente i file dal livello Infrequent Access o dal livello Archive Instant Access al livello Frequent Access.

Note

I file di dimensioni inferiori a 128 KB non sono idonei alla suddivisione automatica e rimangono nel livello Frequent Access. La compattazione può combinare questi file in un numero minore di oggetti più grandi e salvarli nuovamente nella tabella come nuova istantanea. I file appena compattati diventano idonei per il tiering automatico se il nuovo file ha una dimensione pari o superiore a 128 KB.

Comportamento di manutenzione della tabella

Le operazioni di manutenzione automatica delle tabelle eseguite da Amazon S3, come la gestione delle istantanee, la rimozione di file senza riferimenti e la scadenza dei record, continuano a essere eseguite sulle tabelle indipendentemente dal livello. La compattazione viene eseguita solo sui file del

livello Frequent Access, ottimizzando le prestazioni per i dati a cui si accede di frequente e riducendo i costi di manutenzione dei dati nei livelli a basso costo.

Le operazioni di manutenzione non influiscono sul livello di accesso dei file nella tabella. Le letture eseguite dalle operazioni di manutenzione non comportano la modifica dei livelli dei file. Tuttavia, se un'operazione di manutenzione, ad esempio la compattazione o la scadenza di un record, scrive un nuovo file, tale file viene creato nel livello di accesso frequente.

Note

Poiché la compattazione elabora solo i file del livello Frequent Access, le operazioni di eliminazione sui dati nei livelli a basso costo creano file di eliminazione che non vengono compattati automaticamente. Questi file di eliminazione diventano idonei alla compattazione quando si accede ai file di dati associati e tornano al livello di accesso frequente. Per le tabelle a cui non si accede frequentemente, puoi eseguire la compattazione manualmente utilizzando Amazon EMR per compattare questi file di eliminazione con i file di dati associati. Per ulteriori informazioni, consulta [Manutenzione delle tabelle mediante la compattazione](#). Puoi monitorare la crescita dei file nella tua tabella utilizzando le CloudWatch metriche di Amazon per determinare quando la compattazione manuale può essere utile.

Specificare S3 Intelligent-Tiering come classe di archiviazione

Per impostazione predefinita, tutte le tabelle vengono create nella classe di storage S3 Standard e non possono essere spostate in S3. Intelligent-Tiering Per utilizzare S3 Intelligent-Tiering, è necessario specificarlo al momento della creazione della tabella. Puoi anche impostare S3 Intelligent-Tiering come classe di archiviazione predefinita per il tuo bucket di tabelle per archiviare automaticamente tutte le nuove tabelle create lì nella classe di archiviazione Intelligent-Tiering S3.

Specificare S3 per i bucket di tabelle Intelligent-Tiering

È possibile specificare S3 Intelligent-Tiering come classe di archiviazione predefinita quando si crea un nuovo bucket di tabella utilizzando l'operazione `CreateTableBucket` con l'opzione `storage-class-configuration`.

Per verificare la classe di archiviazione predefinita su un bucket di tabella esistente, usa l'operazione `GetTableBucketStorageClass`. Per modificare la classe di archiviazione predefinita di un bucket di tabella esistente, usa l'operazione `PutTableBucketStorageClass`.

 Note

Quando modifichi la classe di archiviazione predefinita su un bucket di tabelle, tale impostazione si applica solo alle nuove tabelle create in quel bucket. La classe di archiviazione per le tabelle preesistenti non viene modificata.

Specificare S3 per le tabelle Intelligent-Tiering

È possibile specificare S3 Intelligent-Tiering come classe di archiviazione quando si crea una nuova tabella utilizzando l'`storage-class-configuration` intestazione con l'operazione `CreateTable`.

Se non si specifica una classe di archiviazione al momento della creazione della tabella, la tabella viene creata nella classe di archiviazione predefinita configurata nel bucket della tabella in quel momento. Una volta creata una tabella, non è possibile modificarne la classe di archiviazione.

Per verificare la classe di archiviazione predefinita su un bucket di tabella esistente, usa l'operazione `GetTableBucketStorageClass`.

Monitoraggio dell'utilizzo dello storage

Puoi visualizzare la suddivisione dell'utilizzo dello storage per livello di accesso nei report sui AWS costi e sull'utilizzo del tuo account. Per ulteriori informazioni, consulta [Creazione di report su costi e utilizzo](#) nella Guida per l'utente di AWS Data Exports.

I seguenti tipi di utilizzo sono disponibili nei report di fatturazione:

Tipo di utilizzo	Unità	Granularità (Granularità)	Description
<code>region-Tables-TimedStorage-INT-</code>	GB-Month	Giornaliero	Il numero di tali dati GB-months è stato archiviato nello storage S3 Intelligent-Tiering Frequent Access di S3 Intelligent-Tiering

Tipo di utilizzo	Unità	Granularità (Granularità)	Description
FA-ByteHrs			
<i>region</i> -Tables-TimedStorage-INT-IA-ByteHrs	GB-Month	Giornaliero	Il numero di tali dati GB-months è stato archiviato nello storage S3 Intelligent-Tiering Infrequent Access of S3 Intelligent-Tiering
<i>region</i> -Tables-TimedStorage-INT-AIA-ByteHrs	GB-Month	Giornaliero	Il numero di tali dati GB-months è stato archiviato nell' Intelligent-Tiering archivio S3 Instant Access dello storage S3 Intelligent-Tiering
<i>region</i> -Tables-Rrequests-INT-Tier1	Conteggio	Orario	Il numero o le PUT POST richieste sugli oggetti S3 Tables COPY Intelligent-Tiering

Tipo di utilizzo	Unità	Granularità (Granularità)	Description
<i>region</i> -Tables-Requests-INT-Tier2	Conteggio	Orario	Il numero GET e tutte le altre richieste non di livello 1 per gli oggetti S3 Tables Intelligent-Tiering

Spazi dei nomi per le tabelle

Le tabelle create all'interno del bucket di tabelle Amazon S3 vengono organizzate in raggruppamenti logici chiamati namespace. A differenza delle tabelle e dei bucket di tabelle S3, i namespace non sono risorse. I namespace sono costrutti che consentono di organizzare e gestire le tabelle in modo scalabile. Ad esempio, tutte le tabelle appartenenti al reparto delle risorse umane di un'azienda possono essere raggruppate in base al valore di namespace comune `hr`.

È possibile utilizzare le policy relative alle risorse dei bucket di tabelle per controllare l'accesso a namespace specifici. Per ulteriori informazioni, consulta [the section called "Policy Resource-based"](#).

Ai namespace di tabelle si applicano le seguenti regole:

- Ogni namespace deve essere univoco all'interno di un bucket di tabelle.
- È possibile creare 10.000 namespace per ogni bucket di tabelle.
- Ogni nome di tabella deve essere univoco all'interno di un namespace.
- Ogni tabella può avere un solo livello di namespace. Gli spazi dei nomi non possono essere nidificati.
- Ogni tabella appartiene a un singolo spazio dei nomi.
- È possibile spostare le tabelle tra spazi dei nomi.

I namespace delle tabelle sono denominati database in vari servizi e motori di interrogazione. AWS La tabella seguente mappa la terminologia utilizzata per i namespace di Tabelle S3 ad alcuni motori e servizi comuni.

Servizio o motore	Terminologia
AWS Lake Formation	Database
AWS Glue Data Catalog	Database
Athena	Database
Spark	Namespace

Argomenti

- [Creazione di un namespace](#)
- [Eliminare uno spazio dei nomi](#)

Creazione di un namespace

Il namespace di una tabella è un costrutto logico in base al quale raggruppare le tabelle in un bucket di tabelle Amazon S3. Ogni tabella appartiene a un singolo spazio dei nomi. Prima di creare una tabella in un bucket di tabelle, è necessario creare un namespace per raggruppare le tabelle. Puoi creare uno spazio dei nomi utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3, gli AWS SDK o i motori di query integrati.

Nomi degli spazi dei nomi

Per la denominazione degli spazi dei nomi si applicano le seguenti regole:

- I nomi devono contenere un numero di caratteri compreso tra 1 e 255.
- I nomi possono essere composti solo da lettere minuscole, numeri e trattini bassi (.). _ I caratteri di sottolineatura non sono consentiti all'inizio o alla fine dei nomi dei namespace.
- I nomi devono iniziare e terminare con una lettera o un numero.
- I nomi non devono contenere trattini (-) o punti (.).
- Uno spazio dei nomi deve essere univoco all'interno di un bucket di tabelle.
- I nomi dei namespace non devono iniziare con il prefisso riservato aws.

Per ulteriori informazioni sui nomi di namespace validi, consulta [Regole di denominazione per tabelle e spazi dei nomi](#).

Utilizzo della console S3 e Amazon Athena

La procedura seguente utilizza il flusso di lavoro Crea tabella con Athena per creare un namespace nella console Amazon S3. Se non si desidera utilizzare Amazon Athena per creare la tabella nel namespace, è possibile annullare il flusso di lavoro dopo aver creato il namespace.

Per creare uno spazio dei nomi

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nella pagina Bucket di tabelle, scegli il bucket in cui desideri creare un namespace.
4. Nella pagina dei dettagli del bucket, scegli Crea tabella con Athena.
5. Nella finestra di dialogo Crea tabella con Athena, scegli Crea un namespace, quindi seleziona Crea namespace.
6. Immetti un nome nel campo Nome del namespace. I nomi dei namespace devono essere composti da un numero di caratteri compreso tra 1 e 255 ed essere univoci all'interno del bucket di tabelle. I caratteri validi sono a-z, 0-9 e i caratteri di sottolineatura (_). I caratteri di sottolineatura non sono consentiti all'inizio o alla fine dei nomi dei namespace.
7. Selezionare Crea namespace.
8. Se desideri creare anche una tabella, scegli Crea tabella con Athena. Per ulteriori informazioni sulla creazione di una tabella con Athena, consulta [the section called "Utilizzo della console S3 e Amazon Athena"](#). Se non desideri creare una tabella in questo momento, scegli Annulla.

Utilizzo di AWS CLI

In questo esempio viene mostrato come creare lo spazio dei nomi di una tabella utilizzando AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables create-namespace \  
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket1 \  
  --namespace example_namespace
```


Utilizzo di un motore di query

È possibile creare uno spazio dei nomi in una sessione di Apache Spark connessa ai bucket delle tabelle Amazon S3.

Questo esempio mostra come creare una tabella utilizzando istruzioni CREATE in un motore di query integrato con Tabelle S3. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
spark.sql("CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

Eliminare uno spazio dei nomi

Prima di eliminare il namespace di una tabella da un bucket di tabelle Amazon S3, è necessario eliminare tutte le tabelle all'interno del namespace o spostarle in un altro namespace. Puoi eliminare uno spazio dei nomi utilizzando l'API REST di Amazon S3, gli AWS SDK, AWS Command Line Interface (AWS CLI) o i motori di query integrati.

Per informazioni sulle autorizzazioni richieste per la eliminare un namespace, consulta [DeleteNamespace](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di AWS CLI

Questo esempio mostra come eliminare lo spazio dei nomi di una tabella utilizzando AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables delete-namespace \  
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket1 \  
  --namespace example_namespace
```

Tabelle nei bucket di tabelle S3

Una tabella S3 rappresenta un set di dati strutturato composto dai dati della tabella sottostante e dai relativi metadati. Questi dati vengono archiviati all'interno di un bucket di tabelle come sottorisorsa. Tutte le tabelle in un bucket vengono archiviate nel formato di tabella [Apache Iceberg](#). Amazon S3 gestisce la manutenzione delle tabelle tramite la compattazione automatica dei file e la gestione degli snapshot. Per ulteriori informazioni, consulta [Manutenzione delle tabelle](#).

Per rendere le tabelle del tuo account accessibili dai servizi di AWS analisi, integra i bucket di tabelle Amazon S3 con AWS Glue Data Catalog. Questa integrazione consente a servizi di AWS analisi come Amazon Athena e Amazon Redshift di rilevare e accedere automaticamente ai dati delle tabelle.

Quando si crea una tabella, Amazon S3 genera automaticamente la relativa posizione nel warehouse. Si tratta di una posizione di S3 univoca in cui vengono archiviati gli oggetti associati alla tabella. Nell'esempio seguente viene illustrato il formato di una posizione del warehouse:

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

All'interno del bucket, le tabelle possono essere organizzate in raggruppamenti logici chiamati spazi dei nomi. Per ulteriori informazioni, consulta [Spazi dei nomi per le tabelle](#).

Le tabelle possono essere rinominate, tuttavia ognuna ha il proprio nome della risorsa Amazon (ARN) e ID univoci. Ogni tabella è collegata anche a una policy delle risorse. È possibile usare questa policy per gestire l'accesso alla tabella.

Gli ARN delle tabelle utilizzano il seguente formato:

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

Per impostazione predefinita, puoi creare fino a 10.000 tabelle in un table bucket. Per richiedere un aumento della quota per i bucket di tabelle o le tabelle, contattare [Supporto](#).

Nei bucket di tabelle di Amazon S3 sono supportati i seguenti tipi di tabelle:

Tabelle dei clienti

Le tabelle dei clienti sono tabelle su cui è possibile leggere e scrivere. È possibile recuperare i dati da queste tabelle utilizzando motori di query integrati. I dati delle tabelle possono essere inseriti, aggiornati o eliminati utilizzando le operazioni dell'API S3 o i motori di query integrati.

AWS tabelle

AWS le tabelle sono tabelle di sola lettura generate da e per Servizio AWS conto dell'utente. Tali tabelle sono gestite da Amazon S3 e non possono essere modificate da alcun principale IAM al di fuori di Amazon S3. È possibile recuperare informazioni da queste tabelle, ma non è possibile modificare i dati in esse contenuti. AWS le tabelle includono le tabelle di metadati S3, che contengono metadati acquisiti dagli oggetti all'interno di un bucket S3 generico. Per ulteriori informazioni, consulta [Individuazione dei dati con le tabelle di S3 Metadati](#).

Argomenti

- [Creazione di una tabella di Amazon S3](#)
- [Eliminazione di una tabella Amazon S3](#)
- [Visualizzazione dei dettagli su una tabella Amazon S3](#)
- [Gestione delle policy delle tabelle](#)
- [Utilizzo dei tag con le tabelle S3](#)

Creazione di una tabella di Amazon S3

Una tabella Amazon S3 è una sottomisura di un bucket di tabelle. Le tabelle sono archiviate nel formato Apache Iceberg in modo da poterle utilizzare con motori di query e altre applicazioni che supportano Apache Iceberg. Amazon S3 ottimizza continuamente le tabelle per ridurre i costi di archiviazione e migliorare le prestazioni delle query di analisi.

Quando si crea una tabella, Amazon S3 genera automaticamente la relativa posizione nel warehouse. La posizione del warehouse è una posizione S3 univoca in cui è possibile leggere e scrivere oggetti associati alla tabella. Nell'esempio seguente viene illustrato il formato di una posizione del warehouse:

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

Il nome della risorsa Amazon (ARN) per le tabelle ha il seguente formato:

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

Per impostazione predefinita, puoi creare fino a 10.000 tabelle in un bucket di tabelle. Per richiedere un aumento della quota per i bucket di tabelle o le tabelle, contattare [Supporto](#).

Puoi creare una tabella utilizzando la console Amazon S3, l'API REST di Amazon S3, AWS gli SDK AWS Command Line Interface (AWS CLI) o i motori di query collegati ai tuoi bucket di tabelle.

Quando si crea una tabella, è possibile specificare le relative impostazioni di crittografia, a meno che non si stia utilizzando Athena. Se non si specificano le impostazioni di crittografia, la tabella viene crittografata con le impostazioni predefinite per il bucket di tabelle. Per ulteriori informazioni, consulta [Specifica della crittografia per tabelle](#).

Prerequisiti per la creazione di tabelle

Per creare una tabella, è necessario procedere come segue:

- [Creare un bucket di tabelle](#).
- [Creare un namespace](#) nel bucket di tabelle.
- Assicurati di disporre delle autorizzazioni AWS Identity and Access Management (IAM) per e. `s3tables:CreateTable` `s3tables:PutTableData`

Note

Se utilizzi la SSE-KMS crittografia per la tua tabella, hai bisogno delle autorizzazioni e `DescribeKey` delle autorizzazioni per `s3tables:PutTableEncryption` la chiave scelta AWS KMS . Inoltre, la AWS KMS chiave utilizzata deve concedere a S3 Tables l'autorizzazione per eseguire la manutenzione automatica della tabella. Per ulteriori informazioni, consulta [Requisiti di autorizzazione per la crittografia delle tabelle S3 SSE-KMS](#)

Per ulteriori informazioni sui nomi di tabella validi, consulta [Regole di denominazione per tabelle e spazi dei nomi](#).

Important

Durante la creazione delle tabelle, è necessario utilizzare solo lettere minuscole nei nomi delle tabelle e nelle definizioni delle tabelle. Ad esempio, è necessario verificare che i nomi delle colonne siano tutti in minuscolo. Se il nome o la definizione della tabella contiene lettere maiuscole, la tabella non è supportata da AWS Lake Formation o da AWS Glue Data Catalog. In questo caso, la tabella non sarà visibile ai servizi di AWS analisi come Amazon Athena, anche se i bucket di tabelle sono integrati con i servizi di AWS analisi.

Se la definizione della tabella contiene lettere maiuscole, riceverai il seguente messaggio di errore quando esegui una SELECT query in Athena: «`GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model. ValidationException: Risorsa federativa non supportata: nomi di tabella o colonna non validi.`»

Utilizzo della console S3 e Amazon Athena

La procedura seguente utilizza la console di Amazon S3 per creare una tabella con Amazon Athena. Se non è ancora stato creato un namespace nel bucket di tabelle, è possibile farlo come parte di questo processo. Prima di eseguire i seguenti passaggi, assicurati di aver integrato i bucket di tabelle con i servizi di analisi AWS nella Regione in uso. Per ulteriori informazioni, consulta [the section called “Integrazione delle tabelle S3 con AWS i servizi di analisi”](#).

Note

Quando si crea una tabella utilizzando Athena, quella tabella eredita le impostazioni di crittografia predefinite dal bucket di tabelle. Per utilizzare un tipo di crittografia diverso, è necessario creare la tabella utilizzando un altro metodo.

Per creare una tabella

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nella pagina Bucket di tabelle, scegli il bucket in cui desideri creare una tabella.
4. Nella pagina dei dettagli del bucket, scegli Crea tabella con Athena.
5. Nella finestra di dialogo Crea tabella con Athena, effettua una delle seguenti operazioni:
 - Crea un nuovo namespace. Scegli Crea un namespace, quindi inserisci un nome nel campo Nome del namespace. I nomi dei namespace devono essere composti da un numero di caratteri compreso tra 1 e 255 ed essere univoci all'interno del bucket di tabelle. I caratteri validi sono a-z, 0-9 e i caratteri di sottolineatura (_). I caratteri di sottolineatura non sono consentiti all'inizio dei nomi dei namespace.
 - Selezionare Crea namespace.
 - Specifica un namespace esistente. Scegli Specifica un namespace esistente nel bucket di tabelle. Quindi seleziona Scegli tra namespace esistenti o Inserisci un nome per il namespace esistente. Se sono presenti più di 1.000 namespace nel bucket, è necessario inserire il nome del namespace se non compare nell'elenco.
6. Scegli Crea tabella con Athena.
7. Si apre la console Amazon Athena e viene visualizzato l'editor di query Athena. Il campo Catalogo deve essere compilato con s3tablescatalog/ seguito dal nome del bucket di tabelle, ad

esempio `s3tablescatalog/amzn-s3-demo-bucket`. Il campo Database deve essere compilato con il namespace creato o selezionato in precedenza.

Note

Se non vedi questi valori nei campi Catalogo e Database, assicurati di aver integrato il bucket di tabelle gestito con i servizi di analisi AWS nella Regione in uso. Per ulteriori informazioni, consulta [the section called “Integrazione delle tabelle S3 con AWS i servizi di analisi”](#).

8. L'editor di query è popolato con una query di esempio da utilizzare per creare una tabella. Modifica la query per specificare il nome della tabella e le colonne della tabella.
9. Una volta modificata la query, scegli Esegui per creare la tabella.

Note

- Se ricevi l'errore “Insufficient permissions to execute the query. Principal does not have any privilege on specified resource” quando provi a eseguire una query in Athena, assicurati di disporre delle necessarie autorizzazioni Lake Formation sulla tabella. Per ulteriori informazioni, consulta [the section called “Concessione dell'autorizzazione Lake Formation per una tabella o un database”](#).
- Se ricevi l'errore «Iceberg non può accedere alla risorsa richiesta» quando provi a eseguire una query in Athena, accedi alla AWS Lake Formation console e assicurati di aver concesso le autorizzazioni per il catalogo e il database (namespace) della tabella che hai creato. Non specificare una tabella quando fornisci queste autorizzazioni. Per ulteriori informazioni, consulta [the section called “Concessione dell'autorizzazione Lake Formation per una tabella o un database”](#).
- Se ricevi il seguente messaggio di errore quando esegui una SELECT query in Athena, questo messaggio è causato dalla presenza di lettere maiuscole nel nome della tabella o nei nomi delle colonne nella definizione della tabella: «GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model. ValidationException: Risorsa federativa non supportata: nomi di tabella o colonna non validi.» Verifica che i nomi delle tabelle e delle colonne siano tutti in minuscolo.

Se la creazione della tabella viene completata, il nome della nuova tabella viene visualizzato nell'elenco delle tabelle in Athena. Quando torni alla console Amazon S3, la nuova tabella viene visualizzata nell'elenco Tabelle nella pagina dei dettagli del bucket di tabelle, dopo aver aggiornato l'elenco.

Utilizzo di AWS CLI

Questo esempio mostra come creare una tabella con uno schema utilizzando AWS CLI e specificando i metadati della tabella con. JSON Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

Per il file `mytabledefinition.json`, utilizza la seguente definizione di tabella di esempio. Per creare una tabella partizionata, includi a nei metadati della tabella. `partitionSpec` Ogni campo di partizione fa riferimento a una colonna dello schema in base al suo valore `sourceId` e applica una trasformazione (ad esempio `identitybucket`, `truncate`, `year`, `monthday`, `hour`) per produrre il valore della partizione. Poiché i campi di partizione fanno riferimento alle colonne dello schema in base all'ID, è necessario assegnare un valore esplicito `id` a ciascun campo dello schema. L'esempio seguente assegna gli ID ai campi dello schema e partiziona la tabella in base alla `registration_date` colonna utilizzando la trasformazione. `day` Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
{
  "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket",
  "namespace": "your_namespace",
  "name": "example_table",
  "format": "ICEBERG",
  "metadata": {
    "iceberg": {
      "schema": {
        "fields": [
          {"id": 1, "name": "id", "type": "int", "required": true},
          {"id": 2, "name": "name", "type": "string"},
          {"id": 3, "name": "registration_date", "type": "timestamp"}
        ]
      },
      "partitionSpec": {
        "specId": 0,
        "fields": [
```

```

        {"sourceId": 3, "transform": "day", "name": "registration_day"}
      ]
    }
  }
}

```

Utilizzo di un motore di query

È possibile creare una tabella in un motore di query supportato collegato ai bucket di tabelle, ad esempio in una sessione Apache Spark su Amazon EMR.

L'esempio seguente mostra come creare una tabella con Spark utilizzando istruzioni CREATE e come aggiungere dati della tabella utilizzando istruzioni INSERT o leggendo i dati da un file esistente. Per creare una tabella partizionata, aggiungete una PARTITIONED BY clausola all'istruzione. CREATE È possibile partizionare direttamente in base a una o più colonne (partizionamento dell'identità) o applicando una trasformazione della partizione come bucket,,, o. truncate years months days hours L'esempio seguente partiziona la tabella per colonna utilizzando la registration_date trasformazione. days Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```

spark.sql(
" CREATE TABLE IF NOT EXISTS s3tablesbucket.example_namespace.`example_table` (
  id INT,
  name STRING,
  registration_date TIMESTAMP
)
USING iceberg
PARTITIONED BY (days(registration_date)) "
)

```

Dopo aver creato la tabella, è possibile caricare i dati nella tabella. Scegli tra i seguenti metodi:

- Aggiungere i dati nella tabella utilizzando l'istruzione INSERT.

```

spark.sql(
"""
  INSERT INTO s3tablesbucket.my_namespace.my_table
  VALUES
    (1, 'ABC', 100),
    (2, 'XYZ', 200)

```



```
""")
```

- Caricare un file di dati esistente.

1. Leggi i dati in Spark:

```
val data_file_location = "Path such as S3 URI to data file"
val data_file = spark.read.parquet(data_file_location)
```

2. Scrivi i dati in una Iceberg tabella:

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty(
  ("format-version", "2").createOrReplace())
```

Eliminazione di una tabella Amazon S3

Puoi eliminare una tabella utilizzando l'API REST di Amazon S3, AWS gli SDK, AWS Command Line Interface (AWS CLI) o utilizzando motori di query integrati.

Note

Tabelle S3 non supporta l'operazione DROP TABLE con `purge=false`. Alcune versioni di Apache Spark impostano sempre questo flag su `false` anche quando eseguono i comandi DROP TABLE PURGE. Per eliminare una tabella, puoi rieseguire DROP TABLE con `purge=true` oppure utilizzare l'operazione REST API [DeleteTable](#) di Tabelle S3.

Important

Quando elimini una tabella, è importante sapere quanto segue:

- L'eliminazione di una tabella un'azione permanente e non può essere annullata. Prima di eliminare una tabella, assicurati di aver eseguito il backup o la replica di tutti i dati importanti.
- Tutti i dati e le configurazioni associati alla tabella vengono rimossi definitivamente.

Utilizzo di AWS CLI

Questo esempio mostra come eliminare una tabella tramite AWS CLI. Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables delete-table \  
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
table-bucket \  
  --namespace example_namespace --name example_table
```

Utilizzo di un motore di query

Le tabelle possono essere eliminate da una sessione di Apache Spark connessa ai bucket di tabelle Amazon S3.

Questo esempio mostra come eliminare una tabella utilizzando il comando DROP TABLE PURGE. Per utilizzare il comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
spark.sql(  
  " DROP TABLE [IF EXISTS] s3tablesbucket.example_namespace.example_table PURGE")
```

Visualizzazione dei dettagli su una tabella Amazon S3

Puoi visualizzare i dettagli generali di una tabella in un bucket di tabelle, come informazioni sulla creazione, sul formato e sul tipo, tramite console o in modo programmatico. Puoi visualizzare le impostazioni di crittografia delle tabelle e le impostazioni di manutenzione a livello di codice utilizzando l'API REST o gli SDK di S3 Tables. AWS CLI AWS

Visualizzazione dei dettagli di una tabella

Utilizzo di AWS CLI

Questo esempio mostra come ottenere dettagli su una tabella tramite la AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables get-table --table-bucket-arn arn:aws:s3tables:us-  
east-1:111122223333:bucket/amzn-s3-demo-table-bucket --namespace my_namespace --  
name my-table
```

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Seleziona prima il bucket di tabelle, quindi la tabella.
4. Seleziona la scheda Proprietà.
5. (Facoltativo) Per informazioni sulla policy di autorizzazione allegata alla tabella, seleziona Autorizzazioni.

Visualizzazione in anteprima dei dati della tabella

Utilizzo della console S3

Puoi visualizzare in anteprima i dati della tabella direttamente dalla console Amazon S3 utilizzando la procedura seguente.

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nella pagina Bucket di tabelle, scegli il bucket contenente la tabella sui cui desideri eseguire la query.
4. Seleziona la tabella che desideri visualizzare in anteprima, quindi fai clic su Anteprima.

Note

L'anteprima mostra le prime 10 righe e fino a 25 colonne della tabella. Le tabelle di dimensioni superiori a 50 MB non possono essere visualizzate in anteprima.

Dettagli sulla crittografia

Per ulteriori informazioni sulla crittografia dei bucket di tabelle, consulta [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket delle tabelle](#).

Utilizzo di AWS CLI

Questo esempio mostra come ottenere dettagli sulle impostazioni di crittografia per una tabella tramite la AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables get-table-encryption --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket --namespace my-namespace --name my-table
```

Dettagli sulla manutenzione

Per ulteriori informazioni sulle impostazioni di manutenzione, consulta [Manutenzione dei bucket di tabelle](#).

Utilizzo di AWS CLI

Questo esempio mostra come ottenere dettagli sulle impostazioni di configurazione della manutenzione per una tabella tramite la AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables get-table-maintenance-configuration --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket --namespace my-namespace --name my-table
```

Gestione delle policy delle tabelle

Puoi aggiungere, eliminare, aggiornare e visualizzare le policy delle tabelle utilizzando la console Amazon S3, l'API REST di Amazon S3, l' AWS SDK e il. AWS CLI Per ulteriori informazioni, consulta i seguenti argomenti. Per ulteriori informazioni sulle azioni e sulle chiavi di condizione supportate AWS Identity and Access Management (IAM) per Amazon S3 Tables, consulta. [Gestione degli accessi per Tabelle S3](#) Per esempi di policy delle tabelle, consulta [Resource-based politiche per S3 Tables](#).

Aggiunta di una policy di tabella

Per aggiungere una policy di tabella a una tabella, puoi utilizzare l'API REST di Amazon S3, l' AWS SDK e il. AWS CLI

Utilizzo di AWS CLI

Questo esempio mostra come visualizzare la policy associata a una tabella utilizzando AWS CLI. Per utilizzare il comando, sostituisci il *user input placeholders* con le tue informazioni.

```
aws s3tables get-table-policy \  
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket1/table/tableID \  
  --namespace my-namespace \  
  --name my-table
```

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Seleziona Bucket di tabelle, poi scegli il bucket che contiene la tabella e infine seleziona la tabella.
4. Scegli la scheda Autorizzazioni.
5. In Policy della tabella, seleziona Modifica.
6. Nell'editor della policy, inserisci il file JSON della policy stessa.
7. (Facoltativo) Seleziona Esempi di policy per visualizzare esempi di policy da adattare alle tue esigenze.
8. Dopo aver inserito la policy, seleziona Salva modifiche.

Visualizzazione di una policy di tabella

Per visualizzare la policy del bucket allegata a una tabella, puoi utilizzare l'API REST di Amazon S3, l'AWS SDK e il AWS CLI

Utilizzo di AWS CLI

Questo esempio mostra come visualizzare la policy associata a una tabella utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3tables get-table-policy \  
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
table-bucket \  
  --namespace my-namespace \  
  --name my-table
```

```
--name my-table
```

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Seleziona Bucket di tabelle, poi scegli il bucket che contiene la tabella e infine seleziona la tabella.
4. Scegli la scheda Autorizzazioni.

Eliminazione di una policy di tabella

Per eliminare una policy allegata a una tabella, puoi utilizzare l'API REST di Amazon S3, l' AWS SDK e il AWS CLI

Utilizzo di AWS CLI

Questo esempio mostra come eliminare una policy di tabella utilizzando AWS CLI. Per utilizzare il comando, sostituisci il *user input placeholders* con le tue informazioni.

```
aws s3tables delete-table-policy \  
  --table-ARN arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-  
bucket \  
  --namespace your-namespace \  
  --name your-table
```

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Seleziona Bucket di tabelle, poi scegli il bucket che contiene la tabella e infine seleziona la tabella.
4. Scegli la scheda Autorizzazioni.
5. In Policy di bucket della tabella, seleziona Elimina.

Utilizzo dei tag con le tabelle S3

Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso le tabelle Amazon S3. Puoi etichettare le tabelle S3 quando le crei o gestire i tag sulle tabelle esistenti. Per informazioni generali sui tag, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

Note

Non sono previsti costi aggiuntivi per l'utilizzo dei tag sulle tabelle oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Modi comuni per utilizzare i tag con le tabelle

Usa i tag sulle tue tabelle S3 per:

1. Allocazione dei costi: tieni traccia dei costi di archiviazione in base ai tag della tabella. Gestione costi e fatturazione AWS Per ulteriori informazioni, consultare [Utilizzo dei tag per l'allocazione dei costi](#).
2. Attribute-based controllo degli accessi (ABAC): ridimensiona le autorizzazioni di accesso e concedi l'accesso alle tabelle S3 in base ai relativi tag. Per ulteriori informazioni, consulta [Utilizzo dei tag per ABAC](#).

Note

È possibile utilizzare gli stessi tag sia per l'allocazione dei costi che per il controllo degli accessi.

ABAC per tabelle S3

Le tabelle Amazon S3 supportano il controllo degli accessi basato sugli attributi (ABAC) tramite tag. Utilizza le chiavi di condizione basate su tag nelle policy delle tue AWS organizzazioni, AWS Identity and Access Management (IAM) e delle tabelle S3. ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle tue policy IAM, puoi controllare l'accesso alle tabelle S3 in base ai tag della tabella utilizzando la chiave di `s3tables:TableBucketTag/tag-key` condizione o le chiavi di condizione [AWS globali:aws:ResourceTag/key-name](#), `aws:RequestTag/key-name` o `aws:TagKeys`

era: `ResourceTag/key-name`

Usa questa chiave di condizione per confrontare la coppia chiave-valore del tag specificata nella policy con la coppia chiave-valore associata alla risorsa. Ad esempio, potresti richiedere che l'accesso a una tabella sia consentito solo se la tabella ha la chiave `Department` tag con il valore `Marketing`

Questa chiave di condizione si applica alle azioni sulla tabella eseguite utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI), le API S3 o gli SDK. AWS

Per un esempio di policy, consulta [1.1 - politica della tabella per limitare le operazioni sulla tabella utilizzando i tag](#).

Per ulteriori esempi di policy e ulteriori informazioni, consulta [Controlling access to AWS resources](#) nella Guida per l'utente. AWS Identity and Access Management

Note

Per le azioni eseguite sulle tabelle, questa chiave di condizione agisce sui tag applicati alla tabella e non sui tag applicati al bucket della tabella contenente la tabella. Usa `s3tables:TableBucketTag/tag-key` invece se desideri che le tue politiche ABAC agiscano sui tag del bucket della tabella quando esegui le azioni sulla tabella.

leggi: `RequestTag/key-name`

Usa questa chiave di condizione per confrontare la coppia chiave-valore del tag passata nella richiesta con la coppia di tag specificata nella policy. Ad esempio, puoi verificare se la richiesta di etichettare una tabella include la chiave del tag `Department` e se ha il valore `Accounting`

Questa chiave di condizione si applica quando le chiavi dei tag vengono passate in una richiesta di operazione `TagResource` o `CreateTable` API o quando si tagga o si crea una tabella con tag utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI) o gli SDK. AWS

Per un esempio di policy, consulta [1.2 - Politica IAM per creare o modificare tabelle con tag specifici](#).

Per ulteriori esempi di policy e ulteriori informazioni, consulta [Controllare l'accesso durante AWS le richieste](#) nella Guida per l'utente. AWS Identity and Access Management

è stato: TagKeys

Usa questa chiave di condizione per confrontare le chiavi dei tag in una richiesta con le chiavi specificate nella policy per definire a quali chiavi di tag è consentito l'accesso. Ad esempio, per consentire l'etichettatura durante l>CreateTableazione, è necessario creare una policy che consenta `s3tables:TagResource` sia le `s3tables:CreateTable` azioni che. È quindi possibile utilizzare la chiave di `aws:TagKeys` condizione per imporre che nella richiesta vengano utilizzati solo tag specifici. `CreateTable`

Questa chiave di condizione si applica quando le chiavi dei tag vengono passate in operazioni a `TagResource` `UntagResource`, o `CreateTable` API o quando si tagga, deseleziona o si crea una tabella con tag utilizzando l'interfaccia a riga di AWS comando (CLI) o gli SDK. AWS

Per un esempio di policy, consulta [1.3 - Politica IAM per controllare la modifica dei tag sulle risorse esistenti mantenendo la governance dei tag](#).

Per ulteriori politiche di esempio e ulteriori informazioni, vedere [Controllo dell'accesso in base alle chiavi](#) dei tag nella Guida per l'utente. AWS Identity and Access Management

`s3tables: TableBucketTag/tag-key`

Usa questa chiave di condizione per concedere autorizzazioni a dati specifici nei bucket di tabelle utilizzando i tag. Questa chiave di condizione agisce, in gran parte, sui tag assegnati al bucket di tabelle per tutte le azioni delle tabelle S3. Anche quando si crea una tabella con tag, questa chiave di condizione agisce sui tag applicati al bucket della tabella che contiene quella tabella. Le eccezioni sono:

- Quando si crea un bucket di tabella con tag, questa chiave di condizione agisce sui tag nella richiesta.

Per un esempio di policy, consulta [1.4 - Utilizzo della chiave `s3tables: condition TableBucketTag`](#).

Esempi di politiche ABAC per le tabelle

Vedi il seguente esempio di politiche ABAC per le tabelle Amazon S3.

 Note

Se disponi di una policy basata sulle risorse IAM o S3 Tables che limita gli utenti IAM e i ruoli IAM in base ai tag principali, devi allegare gli stessi tag principali al ruolo IAM utilizzato da Lake Formation per accedere ai tuoi dati Amazon S3 (ad esempio `LakeFormationDataAccessRole`) e concedere a questo ruolo le autorizzazioni necessarie. Ciò è necessario affinché la politica di controllo degli accessi basata su tag funzioni correttamente con l'integrazione analitica di S3 Tables.

1.1 - politica della tabella per limitare le operazioni sulla tabella utilizzando i tag

In questa politica della tabella, i principali IAM specificati (utenti e ruoli) possono eseguire l'operazione `GetTable` solo se il valore del `project` tag della tabella corrisponde al valore del `project` tag del principale.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGetTable",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3tables:GetTable",
      "Resource": "arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-bucket/my_example_table",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}
```

1.2 - Politica IAM per creare o modificare tabelle con tag specifici

In questa policy IAM, gli utenti o i ruoli con questa policy possono creare tabelle S3 solo se etichettano la tabella con la chiave `project` e il valore del tag `Trinity` nella richiesta di creazione

della tabella. Possono anche aggiungere o modificare tag su tabelle S3 esistenti purché la TagResource richiesta includa la coppia chiave-valore del tag. `project:Trinity` Questa policy non concede autorizzazioni di lettura, scrittura o eliminazione sulle tabelle o sui relativi oggetti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateTableWithTags",
      "Effect": "Allow",
      "Action": [
        "s3tables:CreateTable",
        "s3tables:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
            "Trinity"
          ]
        }
      }
    }
  ]
}
```

1.3 - Politica IAM per controllare la modifica dei tag sulle risorse esistenti mantenendo la governance dei tag

In questa policy IAM, i principali IAM (utenti o ruoli) possono modificare i tag su una tabella solo se il valore del `project` tag della tabella corrisponde al valore del tag del `project` principale. Per queste tabelle sono consentiti solo i quattro tag `project environmentowner`, e `cost-center` specificati nelle chiavi di `aws:TagKeys` condizione. Questo aiuta a far rispettare la governance dei tag, impedisce modifiche non autorizzate ai tag e mantiene lo schema di tagging coerente in tutte le tabelle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
```

```

    "Action": [
      "s3tables:TagResource",
      "s3tables:UntagResource"
    ],
    "Resource": "arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-
bucket/my_example_table",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "project",
          "environment",
          "owner",
          "cost-center"
        ]
      }
    }
  }
}

```

1.4 - Utilizzo della chiave s3tables: condition TableBucketTag

In questa policy IAM, l'istruzione condition consente l'accesso ai dati del bucket della tabella solo se il bucket della tabella ha la chiave Environment e il valore del tag. Production s3tables:TableBucketTag/<tag-key>Si differenzia dalla chiave di aws:ResourceTag/<tag-key> condizione perché, oltre a controllare l'accesso ai bucket di tabelle in base ai relativi tag, consente di controllare l'accesso alle tabelle in base ai tag presenti nel bucket di tabella principale.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToSpecificTables",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-
bucket/*",
      "Condition": {
        "StringEquals": {
          "s3tables:TableBucketTag/Environment": "Production"
        }
      }
    }
  ]
}

```

```
}  
  }  
    }  
  ]  
}
```

Gestione dei tag per le tabelle

Puoi aggiungere o gestire tag per le tabelle S3 utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI), AWS gli SDK o utilizzando le API S3:, e. [TagResource](#) [UntagResource](#) [ListTagsForResource](#) Per ulteriori informazioni, consulta:

Argomenti

- [Creazione di tabelle con tag](#)
- [Aggiungere un tag a una tabella](#)
- [Visualizzazione dei tag delle tabelle](#)
- [Eliminazione di un tag da una tabella](#)

Creazione di tabelle con tag

Puoi etichettare le tabelle Amazon S3 quando le crei. Non è previsto alcun costo aggiuntivo per l'utilizzo dei tag sulle tabelle oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sull'etichettatura delle tabelle, consulta. [Utilizzo dei tag con le tabelle S3](#)

Permissions

Per creare una tabella con tag, è necessario disporre delle seguenti autorizzazioni:

- `s3tables:CreateTable`
- `s3tables:TagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di creare una tabella con tag, è possibile effettuare le seguenti operazioni:

- Verificate di avere i requisiti [Permissions](#) per creare la tabella e applicarvi un tag.

- Controllare la policy dell'utente IAM per eventuali condizioni del controllo degli accessi basato su attributi (ABAC). La tua politica potrebbe richiedere di etichettare le tabelle con solo chiavi e valori di tag specifici. Per ulteriori informazioni sulle politiche ABAC e sulle tabelle di esempio ABAC, consulta [ABAC per le tabelle S3](#).

Fasi

Puoi creare una tabella con i tag applicati utilizzando AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 Tables e gli SDK. AWS

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 Tables per la creazione di una tabella con tag, consulta la seguente sezione nel riferimento alle API di Amazon Simple Storage Service:

- [CreateTable](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio CLI mostra come creare una tabella con tag utilizzando. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Quando si crea una tabella è necessario fornire i dettagli di configurazione. Per ulteriori informazioni, consulta [Creazione di una tabella di Amazon S3](#). È inoltre necessario denominare la tabella con un nome che segua la convenzione di denominazione della tabella. Per ulteriori informazioni, consulta [Regole di denominazione di bucket di tabelle, tabelle e spazio dei nomi di Amazon S3](#).

Richiesta:

```
aws --region us-west-2 \  
s3tables create-table \  
--endpoint https://ufwae60e2k.execute-api.us-west-2.amazonaws.com/personal/ \  
--table-bucket-arn arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket \  
--tags '{"Department":"Engineering"}' \  
--name my_table_abc \  
--namespace my_namesapce_123a \  
--format ICEBERG
```

Aggiungere un tag a una tabella

Puoi aggiungere tag alle tabelle Amazon S3 e modificare questi tag. Per ulteriori informazioni sull'etichettatura delle tabelle, consulta [Utilizzo dei tag con le tabelle S3](#)

Permissions

Per aggiungere un tag a una tabella, è necessario disporre delle seguenti autorizzazioni:

- `s3tables:TagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di aggiungere un tag a una tabella, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per aggiungere un tag a una tabella.
- Se hai tentato di aggiungere una chiave tag che inizia con il prefisso AWS riservato `aws :`, cambia la chiave del tag e riprova.
- La chiave tag è obbligatoria. Inoltre, assicurati che la chiave del tag e il valore del tag non superino la lunghezza massima dei caratteri e non contengano caratteri soggetti a restrizioni. Per ulteriori informazioni, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

Fasi

Puoi aggiungere tag alle tabelle utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI), l'API REST di Amazon S3 Tables e gli SDK. AWS

Utilizzo della console S3

Per aggiungere tag a una tabella utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Scegli il nome del bucket della tabella.
4. Scegli il nome della tabella.
5. Scegliere la scheda Properties (Proprietà).

6. Scorri la sezione Tag e scegli Aggiungi nuovo tag.
7. Viene visualizzata la pagina Aggiungi tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
8. Se si aggiunge un nuovo tag con lo stesso nome di chiave di un tag esistente, il valore del nuovo tag sovrascrive il valore del tag esistente.
9. In questa pagina è anche possibile modificare i valori dei tag esistenti.
10. Dopo aver aggiunto i tag, scegli Salva le modifiche.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'aggiunta di tag a una tabella, consulta la sezione seguente nell'Amazon Simple Storage Service API Reference:

- [TagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio CLI mostra come aggiungere tag a una tabella utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Richiesta:

```
aws --region us-west-2 \  
s3tables tag-resource \  
--resource-arn arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket/table/my_example_table \  
--tags '{"Department":"engineering"}'
```

Visualizzazione dei tag delle tabelle

Puoi visualizzare o elencare i tag applicati alle tabelle Amazon S3. Per ulteriori informazioni sui tag, consulta [Utilizzo dei tag con le tabelle S3](#).

Permissions

Per visualizzare i tag applicati a una tabella, è necessario disporre delle seguenti autorizzazioni:

- `s3tables:ListTagsForResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di elencare o visualizzare i tag di una tabella, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per visualizzare o elencare i tag della tabella.

Fasi

Puoi visualizzare i tag applicati alle tabelle utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e AWS gli SDK.

Utilizzo della console S3

Per visualizzare i tag applicati a una tabella utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Scegli il nome del bucket Table.
4. Scegli il nome della tabella all'interno del bucket Tabella.
5. Scegliere la scheda Properties (Proprietà).
6. Scorri fino alla sezione Tag per visualizzare tutti i tag applicati alla tabella.
7. La sezione Tag mostra i User-defined tag per impostazione predefinita. Puoi selezionare la scheda dei tag AWS generati per visualizzare i tag applicati alla tabella dai AWS servizi.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la visualizzazione dei tag applicati a una tabella, consulta la seguente sezione nell'Amazon Simple Storage Service API Reference:

- [ListTagsforResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio CLI mostra come visualizzare i tag applicati a una tabella. Per utilizzare il comando, sostituiscili *user input placeholders* con le tue informazioni.

Richiesta:

```
aws --region us-west-2 \  
s3tables list-tags-for-resource \  
--resource-arn arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket/table/my_example_table
```

Eliminazione di un tag da una tabella

Puoi rimuovere i tag dalle tabelle Amazon S3. Per ulteriori informazioni sull'etichettatura delle tabelle, consulta [Utilizzo dei tag con le tabelle S3](#)

Note

Se elimini un tag e in seguito scopri che è stato utilizzato per tenere traccia dei costi o per il controllo degli accessi, puoi aggiungere nuovamente il tag alla tabella.

Permissions

Per eliminare un tag da una tabella, è necessario disporre delle seguenti autorizzazioni:

- `s3tables:UntagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di eliminare un tag da una tabella, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per eliminare un tag da una tabella.

Fasi

Puoi eliminare i tag dalle tabelle utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 Tables e AWS gli SDK.

Utilizzo della console S3

Per eliminare i tag da una tabella utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Scegli il nome del bucket della tabella.
4. Scegli il nome della tabella.
5. Scegliere la scheda Properties (Proprietà).
6. Scorri fino alla sezione Tag e seleziona la casella di controllo accanto al tag o ai tag che desideri eliminare.
7. Scegliere Elimina.
8. Viene visualizzato il pop-up Elimina tag definiti dall'utente che chiede di confermare l'eliminazione del tag o dei tag selezionati.
9. Seleziona Elimina per confermare.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'eliminazione di tag da una tabella, consulta la seguente sezione nell'Amazon Simple Storage Service API Reference:

- [UnTagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come eliminare i tag da una tabella utilizzando. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Richiesta:

```
aws --region us-west-2 \  
s3tables untag-resource \  
--resource-arn arn:aws::s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-  
bucket/table/my_example_table \  
--tag-keys '["department"]'
```

Accesso ai dati delle tabelle

Esistono diversi modi per accedere alle tabelle nei bucket di tabelle di Amazon S3. Puoi integrare le tabelle con i servizi di AWS analisi utilizzando AWS Glue Data Catalog o accedere alle tabelle direttamente utilizzando l'iceberg RESTendpoint Amazon S3 Tables o Amazon S3 Tables Catalog per. Apache Iceberg Il metodo di accesso utilizzato dipende dalla configurazione del catalogo, dal modello di governance e dalle esigenze di controllo degli accessi. Di seguito è riportata una panoramica di questi metodi di accesso.

AWS Glue Data Catalog integration

Questo è il metodo di accesso consigliato per utilizzare le tabelle nei bucket di tabelle S3. Questa integrazione ti offre una visione unificata del tuo patrimonio di dati su più servizi di AWS analisi tramite. AWS Glue Data Catalog Dopo l'integrazione, puoi interrogare le tabelle utilizzando servizi come Athena e Amazon Redshift. L'accesso alle tabelle viene gestito utilizzando le autorizzazioni IAM. Per accedere alle tabelle utilizzando questa integrazione, l'identità IAM utilizzata richiede l'accesso alle risorse e alle azioni di S3 Tables, AWS Glue Data Catalog agli oggetti e al motore di query che stai utilizzando. Per ulteriori informazioni, consulta [Gestione degli accessi per Tabelle S3](#).

Accesso diretto

Utilizza questo metodo se devi lavorare con implementazioni di cataloghi AWS Partner Network (APN), implementazioni di cataloghi personalizzati o se devi eseguire solo read/write operazioni di base sulle tabelle all'interno di un singolo bucket di tabelle. L'accesso alle tabelle è gestito utilizzando le autorizzazioni IAM. Per accedere alle tabelle, l'identità IAM utilizzata richiede l'accesso alle risorse della tabella e alle azioni di S3 Tables. Per ulteriori informazioni, consulta [Gestione degli accessi per Tabelle S3](#).

L'accesso alle tabelle tramite AWS Glue Data Catalog integrazione

Puoi integrare i bucket di tabelle S3 AWS Glue Data Catalog per accedere alle tabelle da servizi di AWS analisi, come Amazon Athena, Amazon Redshift e Quick. L'integrazione li compila AWS Glue Data Catalog con le risorse della tua tabella e federa l'accesso a tali risorse. Per ulteriori informazioni sull'integrazione, consulta [Integrazione di Amazon S3 Tables con AWS servizi di analisi](#).

I seguenti servizi di AWS analisi possono accedere alle tabelle tramite questa integrazione:

- [Amazon Athena](#)

- [Amazon Redshift](#)
- [Amazon EMR](#)
- [di base](#)
- [Amazon Data Firehose](#)
- [AWS Glue ETL](#)
- [Interrogazione di tabelle S3 con Unified Studio SageMaker](#)

Accesso alle tabelle utilizzando AWS Glue Iceberg REST endpoint

Una volta integrati i bucket di tabelle S3 AWS Glue Data Catalog, puoi anche utilizzare l' AWS Glue Iceberg REST endpoint per connetterti alle tabelle S3 provenienti da motori di query di terze parti che supportano Iceberg. Per ulteriori informazioni, consulta [Accesso alle tabelle Amazon S3 utilizzando AWS Glue Iceberg REST endpoint](#).

È consigliabile utilizzare l'endpoint AWS Glue Iceberg REST per accedere alle tabelle da Spark, PyIceberg o altri client compatibili con Iceberg.

I seguenti client possono accedere alle tabelle direttamente tramite l'endpoint AWS Glue Iceberg REST:

- Qualsiasi client Iceberg, inclusi Spark, PyIceberg e altri.

Accesso diretto alle tabelle

È possibile accedere alle tabelle direttamente dai motori di query open source attraverso metodi che collegano le operazioni di gestione di Tabelle S3 alle applicazioni di analisi Apache Iceberg. Esistono due metodi di accesso diretto: l'endpoint Iceberg REST di Tabelle Amazon S3 o il Catalogo di Tabelle Amazon S3 per Apache Iceberg. L'endpoint REST è la scelta consigliata.

Ti consigliamo l'accesso diretto se accedi alle tabelle nelle implementazioni di catalogo autogestite o se devi eseguire solo read/write operazioni di base sulle tabelle in un singolo bucket di tabelle. Per altri scenari di accesso, consigliamo l'integrazione. AWS Glue Data Catalog

L'accesso diretto alle tabelle viene gestito tramite policy basate sull'identità IAM o policy basate sulle risorse collegate a tabelle e bucket di tabelle.

Accesso alle tabelle tramite Amazon S3 Tables Iceberg REST endpoint

È possibile utilizzare l'endpoint Iceberg REST di Tabelle Amazon S3 per accedere alle tabelle direttamente da qualsiasi client compatibile con Iceberg REST tramite endpoint HTTP. Per ulteriori informazioni, consulta [Accesso alle tabelle utilizzando Amazon S3 Tables Iceberg REST endpoint](#).

I seguenti servizi di AWS analisi e motori di query possono accedere alle tabelle direttamente utilizzando l'endpoint Amazon S3 TablesIceberg REST:

Motori di query supportati

- Qualsiasi client Iceberg, inclusi Spark, Pylceberg e altri.
- [Amazon EMR](#)
- [AWS Glue ETL](#)

Accesso diretto alle tabelle tramite Amazon S3 Tables Catalog per Apache Iceberg

È possibile accedere alle tabelle direttamente anche dai motori di query, ad esempio Apache Spark, utilizzando il catalogo client di Tabelle S3. Per ulteriori informazioni, consulta [Accesso alle tabelle Amazon S3 con Amazon S3 Tables Catalog per Apache Iceberg](#). Tuttavia, S3 consiglia di utilizzare l'endpoint Iceberg REST di Tabelle Amazon S3 per l'accesso diretto perché supporta più applicazioni, senza richiedere un linguaggio o un codice specifico del motore.

I seguenti motori di query possono accedere direttamente alle tabelle utilizzando il catalogo client:

- [Apache Spark](#)

Integrazione di Amazon S3 Tables con AWS panoramica dei servizi di analisi

Per rendere le tabelle del tuo account accessibili dai servizi di AWS analisi, integri i tuoi bucket di tabelle Amazon S3 con. AWS Glue Data Catalog Questa integrazione consente ai servizi di AWS analisi di scoprire e accedere automaticamente ai dati delle tabelle. È possibile utilizzare l'integrazione con le tabelle nei seguenti servizi:

- [Amazon Athena](#)
- [Amazon Redshift](#)

- [Amazon EMR](#)
- [di base](#)
- [Amazon Data Firehose](#)

Note

Questa integrazione utilizza AWS Glue e fornisce AWS Lake Formation servizi e potrebbe comportare costi di AWS Glue richiesta e archiviazione. Per ulteriori informazioni, consulta [AWS Glue Prezzi](#).

Vengono applicati costi aggiuntivi per l'esecuzione di query sulle tabelle S3. Per ulteriori informazioni, consulta le informazioni sui prezzi del motore di query in uso.

Funzionamento dell'integrazione

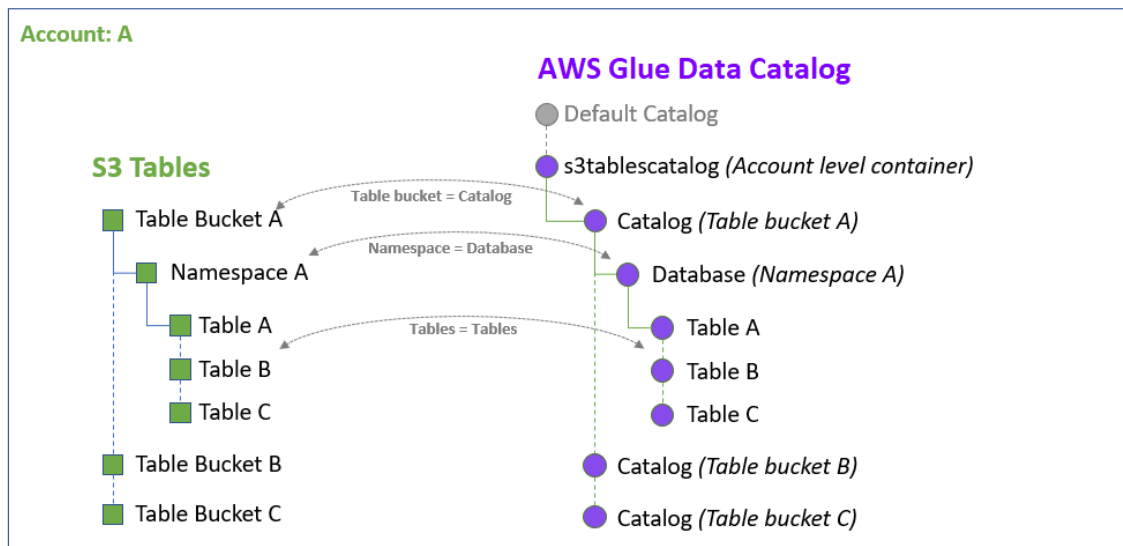
Quando integri S3 Tables con i servizi di AWS analisi, Amazon S3 aggiunge il catalogo `s3tablescatalog` denominato AWS Glue Data Catalog nella regione corrente. L'aggiunta `s3tablescatalog` di consente di popolare tutti i bucket di tabelle, i namespace e le tabelle nel catalogo dati.

Note

Queste azioni sono automatizzate tramite la console Amazon S3. Se esegui questa integrazione a livello di codice, devi eseguire queste azioni manualmente.

È possibile integrare i bucket di tabelle una volta per regione. AWS Una volta completata l'integrazione, tutti i bucket di tabelle, i namespace e le tabelle attuali e futuri vengono aggiunti a quelli presenti in quella regione. AWS Glue Data Catalog

L'illustrazione seguente mostra come il catalogo `s3tablescatalog` popola automaticamente i bucket di tabelle, i namespace e le tabelle nella Regione corrente come oggetti corrispondenti nel Catalogo dati. I bucket di tabelle vengono popolati come sottocataloghi. I namespace all'interno di un bucket di tabelle vengono popolati come database nei rispettivi sottocataloghi. Le tabelle vengono popolate come tabelle nei rispettivi database.



Dopo l'integrazione con Data Catalog, puoi creare Apache Iceberg tabelle in bucket di tabelle e accedervi tramite motori di AWS analisi come Amazon Athena, Amazon EMR e motori di analisi di terze parti.

Come funzionano le autorizzazioni

Ti consigliamo di integrare i bucket di tabelle con i servizi di AWS analisi in modo da poter lavorare con i dati delle tabelle tra i servizi che lo utilizzano come archivio di metadati. AWS Glue Data Catalog Una volta abilitata l'integrazione, puoi utilizzare le autorizzazioni AWS Identity and Access Management (IAM) per concedere l'accesso alle risorse di S3 Tables e agli oggetti del catalogo dati associati.

Assicurati di seguire i passaggi indicati in [Integrazione delle tabelle S3 con AWS i servizi di analisi](#) modo da disporre delle autorizzazioni appropriate per accedere alle risorse e alla tabella AWS Glue Data Catalog e per lavorare con AWS i servizi di analisi.

Regioni supportate

L'integrazione di S3 Tables con i servizi di AWS analisi utilizza AWS Glue Data Catalog i controlli di IAM-based accesso nelle seguenti regioni. In tutte le altre regioni, l'integrazione richiede AWS Lake Formation anche.

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (California settentrionale)

- Stati Uniti occidentali (Oregon)
- Africa (Città del Capo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Taipei)
- Asia Pacifico (Tokyo)
- Asia Pacifico (Seoul)
- Asia Pacifico (Osaka)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Hyderabad)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Malesia)
- Asia Pacifico (Nuova Zelanda)
- Asia Pacifico (Thailandia)
- Canada (Centrale)
- Canada occidentale (Calgary)
- Europa (Francoforte)
- Europa (Zurigo)
- Europa (Stoccolma)
- Europa (Milano)
- Europa (Spagna)
- Europa (Irlanda)
- Europa (Londra)
- Europa (Parigi)
- Israele (Tel Aviv)
- Messico (centrale)
- Sud America (San Paolo)

Fasi successive

- [Integrazione delle tabelle S3 con AWS i servizi di analisi](#)
- [Creare un namespace](#)
- [Creare una tabella](#)

Integrazione di Amazon S3 Tables con AWS servizi di analisi

Questo argomento illustra i prerequisiti e le procedure necessari per integrare i bucket di tabelle Amazon S3 con i servizi di analisi. AWS Per una panoramica di come funziona l'integrazione, consulta [Panoramica dell'integrazione di Tabelle S3](#).

Note

Questa integrazione utilizza AWS Glue Data Catalog e potrebbe comportare costi di AWS Glue richiesta e archiviazione. Per ulteriori informazioni, consulta [AWS Glue Prezzi](#). Si applicano prezzi aggiuntivi per l'esecuzione di query su S3 Tables. Per ulteriori informazioni, consulta le informazioni sui prezzi del motore di query in uso.

Prerequisiti per l'integrazione

I seguenti prerequisiti sono necessari per integrare i bucket di tabelle con i servizi di analisi: AWS

- [Creare un bucket di tabelle.](#)
- Aggiungi le seguenti AWS Glue autorizzazioni al tuo principale AWS Identity and Access Management (IAM):
 - `glue:CreateCatalog` necessario per creare un catalogo `s3tablescatalog` federato nel Data Catalog
 - `glue:PassConnection` concede al committente chiamante il diritto di delegare la creazione della `aws:s3tables` connessione al servizio Amazon S3.
- [Aggiornamento alla versione più recente di \(\). AWS Command Line InterfaceAWS CLI](#)

Important

Durante la creazione delle tabelle, è necessario utilizzare solo lettere minuscole nei nomi delle tabelle e nelle definizioni delle tabelle. Ad esempio, è necessario verificare che i nomi delle colonne siano tutti in minuscolo. Se il nome o la definizione della tabella contiene lettere maiuscole, la tabella non è supportata da AWS Lake Formation o da AWS Glue Data Catalog. In questo caso, la tabella non sarà visibile ai servizi di AWS analisi come Amazon Athena, anche se i bucket di tabelle sono integrati con i servizi di AWS analisi.

Se la definizione della tabella contiene lettere maiuscole, riceverai il seguente messaggio di errore quando esegui una SELECT query in Athena: «GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model. ValidationException: Risorsa federativa non supportata: nomi di tabella o colonna non validi.»

Integrazione di secchi da tavolo con AWS servizi di analisi

È possibile integrare i bucket di tabelle con Data Catalog e i servizi di AWS analisi utilizzando i controlli di accesso IAM per impostazione predefinita o, facoltativamente, utilizzare i controlli di accesso di Lake Formation.

Quando effettui l'integrazione utilizzando i controlli di accesso IAM, hai bisogno dei privilegi IAM per accedere ai bucket e alle tabelle di Amazon S3, agli oggetti del Data Catalog e al motore di query che stai utilizzando. Se scegli di effettuare l'integrazione utilizzando Lake Formation, sia i controlli di accesso IAM che le sovvenzioni Lake Formation determinano l'accesso alle risorse di Data Catalog. Fai riferimento alla [AWS Lake Formation Developer Guide](#) per saperne di più sull'integrazione con Lake Formation.

Le sezioni seguenti descrivono come utilizzare la console di gestione Amazon S3 o AWS CLI configurare l'integrazione con i controlli di accesso IAM.

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Seleziona Crea bucket di tabelle.

Viene visualizzata la pagina Create bucket di tabelle.

4. Inserisci un Nome del bucket di tabelle e assicurati che sia selezionata l'opzione Abilita integrazione.

5. Seleziona Crea bucket di tabelle. Amazon S3 tenterà di integrare automaticamente i bucket di tabelle in tale Regione.

Utilizzo di AWS CLI

Per integrare i bucket di tabelle con i controlli di accesso IAM utilizzando AWS CLI

I passaggi seguenti mostrano come utilizzare i bucket di tabella AWS CLI per integrare. Per utilizzare queste fasi, sostituisci *user input placeholders* con le informazioni appropriate.

1. Creare un bucket di tabelle.

```
aws s3tables create-table-bucket \  
--region us-east-1 \  
--name amzn-s3-demo-table-bucket
```

2. Creare un file denominato `catalog.json` contenente il catalogo seguente:

```
{  
  "Name": "s3tablescatalog",  
  "CatalogInput": {  
    "FederatedCatalog": {  
      "Identifier": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",  
      "ConnectionName": "aws:s3tables"  
    },  
    "CreateDatabaseDefaultPermissions": [  
      {  
        "Principal": {  
          "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"  
        },  
        "Permissions": ["ALL"]  
      }  
    ],  
    "CreateTableDefaultPermissions": [  
      {  
        "Principal": {  
          "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"  
        },  
        "Permissions": ["ALL"]  
      }  
    ],  
    "AllowFullTableExternalDataAccess": "True"  
  }  
}
```

```
}  
}
```

Creare il catalogo `s3tablescatalog` utilizzando il comando seguente. La creazione di questo catalogo lo compila AWS Glue Data Catalog con oggetti corrispondenti a bucket di tabelle, namespace e tabelle.

```
aws glue create-catalog \  
--region us-east-1 \  
--cli-input-json file://catalog.json
```

3. Verificate che il `s3tablescatalog` catalogo sia stato aggiunto utilizzando il seguente AWS Glue comando:

```
aws glue get-catalog --catalog-id s3tablescatalog
```

Migrazione al processo di integrazione aggiornato

Il processo di integrazione dei servizi di AWS analisi è stato aggiornato per utilizzare le autorizzazioni IAM per impostazione predefinita. Se hai già configurato l'integrazione, puoi continuare a utilizzare l'integrazione attuale. Tuttavia, se desideri modificare l'integrazione esistente per utilizzare invece le autorizzazioni IAM, consulta la Guida [per](#) AWS Lake Formation gli sviluppatori. Puoi anche rifare l'integrazione per eliminare la configurazione esistente AWS Glue Data Catalog AWS Lake Formation ed eseguire nuovamente l'integrazione. Ciò rimuoverà tutte le concessioni Lake Formation esistenti e le autorizzazioni di accesso associate a `s3tablescatalog`.

1. Apri la AWS Lake Formation console all'indirizzo <https://console.aws.amazon.com/lakeformation/>, e accedi come amministratore del data lake. Per ulteriori informazioni su come creare un amministratore del data lake, consulta [Creare un amministratore di data lake](#) nella Guida per gli sviluppatori di AWS Lake Formation.
2. Elimina il catalogo `s3tablescatalog` come segue:
 - Nel riquadro di navigazione a sinistra, seleziona Cataloghi.
 - Seleziona il pulsante di opzione accanto al catalogo `s3tablescatalog` nell'elenco Cataloghi. Dal menu Actions (Operazioni), scegli Delete (Elimina).
3. Annulla la registrazione della posizione dei dati per il catalogo `s3tablescatalog` come segue:

- Nel riquadro di navigazione a sinistra, vai alla sezione Amministrazione e scegli Posizioni del data lake.
 - Seleziona il pulsante di opzione accanto alla posizione del data lake `s3tablescatalog`, ad esempio `s3://tables:region:account-id:bucket/*`.
 - Nel menu Operazioni scegli Rimuovi.
 - Nella finestra di dialogo di conferma che viene visualizzata, scegli Rimuovi.
4. Ora che hai eliminato la posizione `s3tablescatalog` del catalogo e del data lake, puoi seguire i passaggi per [integrare i bucket di tabelle con i servizi di AWS analisi](#) utilizzando il processo di integrazione aggiornato.

Note

Se desideri lavorare con tabelle SSE-KMS crittografate nei servizi di AWS analisi integrati, il ruolo che utilizzi deve disporre dell'autorizzazione per utilizzare la tua AWS KMS chiave per le operazioni di crittografia. Per ulteriori informazioni, consulta [Concessione ai principali IAM delle autorizzazioni per lavorare con tabelle crittografate in modalità integrata AWS servizi di analisi](#).

Fasi successive

- [Creare un namespace](#).
- [Creare una tabella](#).

Accesso alle tabelle Amazon S3 utilizzando AWS Glue Iceberg REST endpoint

Una volta integrati i bucket di tabelle S3 con, AWS Glue Data Catalog puoi utilizzare l' AWS GlueIceberg RESTendpoint per connetterti alle tue tabelle S3 da Apache Iceberg client compatibili, come o. Pylceberg Spark L' AWS Glue Iceberg RESTendpoint implementa la specifica [Iceberg REST Catalog Open API](#) che fornisce un'interfaccia standardizzata per interagire con le tabelle. Iceberg Per accedere alle tabelle S3 utilizzando l'endpoint è necessario configurare le autorizzazioni tramite una combinazione di policy e concessioni IAM. AWS Lake Formation Le sezioni seguenti spiegano come configurare l'accesso, inclusa la creazione del ruolo IAM necessario, la definizione delle policy

richieste e la definizione delle autorizzazioni di Lake Formation per l'accesso sia a livello di database sia a livello di tabella.

Per una procedura dettagliata sull'utilizzo di Pylceberg, consulta [Accesso ai dati in Tabelle Amazon S3 utilizzando Pylceberg tramite l'endpoint AWS Glue Iceberg REST](#).

Prerequisiti

- [Integra i tuoi bucket di tabelle con i servizi di analisi AWS](#)
- [Creazione di un namespace di tabelle](#)
- [Accesso a un account amministratore di data Lake](#)

Creazione di un ruolo IAM per il client

Per accedere alle tabelle tramite gli AWS Glue endpoint, devi creare un ruolo IAM con autorizzazioni AWS Glue e azioni Lake Formation. Questa procedura spiega come creare questo ruolo e configurarne le autorizzazioni.

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione sinistro, scegli Policy.
3. Scegli Crea una policy e scegliere JSON nell'editor delle policy.
4. Aggiungi la seguente policy in linea che concede le autorizzazioni di accesso AWS Glue e le azioni di Lake Formation:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "glue:GetCatalog",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:CreateTable",
```

```

        "glue:UpdateTable"
    ],
    "Resource": [
        "arn:aws:glue:us-east-1:111122223333:catalog",
        "arn:aws:glue:us-east-1:111122223333:catalog/
s3tablescatalog",
        "arn:aws:glue:us-east-1:111122223333:catalog/s3tablescatalog/
amzn-s3-demo-table-bucket",
        "arn:aws:glue:us-east-1:111122223333:table/s3tablescatalog/
amzn-s3-demo-table-bucket/<namespace>/*",
        "arn:aws:glue:us-east-1:111122223333:database/
s3tablescatalog/amzn-s3-demo-table-bucket/<namespace>"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "lakeformation:GetDataAccess"
    ],
    "Resource": "*"
}
]
}

```

5. Dopo aver creato la policy, crea un ruolo IAM e scegli Policy di attendibilità personalizzata per Tipo di entità attendibile.
6. Inserisci quanto segue per la Policy di attendibilità personalizzata.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/Admin_role"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}

```



```
}
```

Definizione dell'accesso in Lake Formation

Lake Formation fornisce un controllo granulare degli accessi per le tabelle del data lake. Quando hai integrato il tuo bucket S3 con AWS Glue Data Catalog, le tue tabelle sono state automaticamente registrate come risorse in Lake Formation. Per accedere a queste tabelle, è necessario fornire autorizzazioni specifiche di Lake Formation all'identità IAM, oltre alle autorizzazioni relative alle relative policy IAM.

Le seguenti fasi spiegano come applicare i controlli degli accessi di Lake Formation per consentire al client Iceberg di connettersi alle tabelle. È necessario accedere come amministratore del data lake per applicare queste autorizzazioni.

Consenso per l'accesso ai dati delle tabelle dai motori esterni

In Lake Formation, è necessario abilitare l'accesso completo alle tabelle per consentire ai motori esterni di accedere ai dati. Ciò consente alle applicazioni di terze parti di ottenere credenziali temporanee da Lake Formation quando utilizzano un ruolo IAM con autorizzazioni complete sulla tabella richiesta.

Apri la console di Lake Formation all'indirizzo. <https://console.aws.amazon.com/lakeformation/>

1. Apri la console di Lake Formation all'indirizzo <https://console.aws.amazon.com/lakeformation/> e accedi come amministratore del data lake.
2. Nel riquadro di navigazione, scegliere Impostazioni di integrazione di applicazioni in Amministrazione.
3. Selezionare Consenti ai motori esterni di accedere ai dati nelle posizioni Amazon S3 con accesso completo alla tabella. Quindi scegli Save (Salva).

Concedere le autorizzazioni di Lake Formation sulle risorse delle tabelle

Quindi, concedi a Lake Formation le autorizzazioni per il ruolo IAM che hai creato per il tuo Iceberg-compatible cliente. Queste autorizzazioni consentono al ruolo di creare e gestire tabelle nel namespace. È necessario fornire sia le autorizzazioni a livello di database sia a livello di tabella. Per ulteriori informazioni, consulta [Concessione dell'autorizzazione Lake Formation per una tabella o un database](#).

Configurazione dell'ambiente per l'utilizzo dell'endpoint

Dopo aver impostato il ruolo IAM con le autorizzazioni necessarie per l'accesso alle tabelle, puoi utilizzarlo per eseguire Iceberg i client dal tuo computer locale configurandoli AWS CLI con il tuo ruolo, usando il seguente comando:

```
aws sts assume-role --role-arn "arn:aws:iam::<accountid>:role/<glue-irc-role>" --role-session-name <glue-irc-role>
```

Per accedere alle tabelle tramite l' AWS Glue RESTendpoint, è necessario inizializzare un catalogo nel client -compatible. Iceberg Questa inizializzazione richiede la specifica di proprietà personalizzate, tra cui le proprietà sigv4, l'URI dell'endpoint e la posizione del warehouse. Queste proprietà si specificano come segue:

- Proprietà Sigv4: Sigv4 deve essere abilitato, il nome della firma è glue
- Posizione del warehouse: è il bucket di tabelle, specificato nel formato `<accountid>:s3tablescatalog/<table-bucket-name>`
- URI dell'endpoint: consulta la guida di riferimento degli endpoint AWS Glue di servizio per l'endpoint specifico della regione

L'esempio seguente mostra come inizializzare un catalogo pylceberg.

```
rest_catalog = load_catalog(  
    s3tablescatalog,  
    **{  
        "type": "rest",  
        "warehouse": "<accountid>:s3tablescatalog/<table-bucket-name>",  
        "uri": "https://glue.<region>.amazonaws.com/iceberg",  
        "rest.sigv4-enabled": "true",  
        "rest.signing-name": "glue",  
        "rest.signing-region": region  
    }  
)
```

Per ulteriori informazioni sull'implementazione degli endpoint AWS GlueIceberg REST, consulta [Connessione al Catalogo dati utilizzando l'endpoint AWS GlueIceberg REST](#) nella Guida per l'utente di AWS Glue .

Accesso alle tabelle utilizzando Amazon S3 Tables Iceberg REST endpoint

È possibile collegare il client Iceberg REST all'endpoint Iceberg REST di Tabelle Amazon S3 ed effettuare chiamate REST API per creare, aggiornare o sottoporre a query le tabelle nei bucket di tabelle S3. L'endpoint implementa un set di Iceberg REST API standardizzate specificate nella specifica [Apache Iceberg REST Catalog Open API](#). L'endpoint funziona traducendo le operazioni Iceberg REST API nelle corrispondenti operazioni di Tabelle S3.

Note

L'Iceberg REST endpoint Amazon S3 Tables può essere utilizzato per accedere alle tabelle nelle implementazioni del catalogo AWS Partner Network (APN) o nelle implementazioni di cataloghi personalizzati. Può essere utilizzato anche se è necessario solo l' read/write accesso di base a un singolo bucket di tabelle. Per altri scenari di accesso, consigliamo di utilizzare l' AWS Glue Iceberg REST endpoint per connettersi alle tabelle, che fornisce una gestione unificata delle tabelle, una governance centralizzata e un controllo degli accessi granulare. Per ulteriori informazioni, consulta [Accesso alle tabelle Amazon S3 utilizzando AWS Glue Iceberg REST endpoint](#)

Configurazione dell'endpoint

Ci si connette all'endpoint Iceberg REST di Tabelle Amazon S3 utilizzando l'endpoint del servizio. Gli endpoint Iceberg REST di Tabelle S3 hanno il formato seguente:

```
https://s3tables.<REGION>.amazonaws.com/iceberg
```

Fai riferimento a per gli endpoint. [Tabelle S3 Regioni AWS ed endpoint](#) Region-specific

Proprietà della configurazione del catalogo

Quando si utilizza un client Iceberg per connettere un motore di analisi all'endpoint del servizio, è necessario specificare le seguenti proprietà di configurazione quando si inizializza il catalogo. Sostituiscili *placeholder values* con le informazioni relative alla tua regione e al bucket della tabella.

- L'endpoint specifico della Regione come l'URI dell'endpoint: `https://s3tables.<REGION>.amazonaws.com/iceberg`

- L'ARN del bucket di tabelle come posizione del warehouse:
`arn:aws:s3tables:<region>:<accountID>:bucket/<bucketname>`
- Proprietà Sigv4 per l'autenticazione. Il nome di firma SigV4 per le richieste degli endpoint del servizio è: `s3tables`

I seguenti esempi illustrano come configurare client diversi per utilizzare l'endpoint Iceberg REST di Tabelle Amazon S3.

Pylceberg

Per utilizzare l'endpoint Iceberg REST di Tabelle Amazon S3 con Pylceberg, specifica le seguenti proprietà di configurazione dell'applicazione:

```
rest_catalog = load_catalog(
    catalog_name,
    **{
        "type": "rest",
        "warehouse": "arn:aws:s3tables:<Region>:<accountID>:bucket/<bucketname>",
        "uri": "https://s3tables.<Region>.amazonaws.com/iceberg",
        "rest.sigv4-enabled": "true",
        "rest.signing-name": "s3tables",
        "rest.signing-region": "<Region>"
    }
)
```

Apache Spark

Per utilizzare l'Iceberg REST endpoint Amazon S3 Tables con Spark, specifica le seguenti proprietà di configurazione dell'applicazione, sostituendole *placeholder values* con le informazioni relative alla regione e al bucket di tabelle.

```
spark-shell \
  --packages "org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.4.1,software.amazon.awssdk:bundle:2.20.160,software.amazon.awssdk:url-
connection-client:2.20.160" \
  --master "local[*]" \
  --conf
"spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions"
\
  --conf "spark.sql.defaultCatalog=spark_catalog" \
  --conf "spark.sql.catalog.spark_catalog=org.apache.iceberg.spark.SparkCatalog" \
```

```
--conf "spark.sql.catalog.spark_catalog.type=rest" \
--conf "spark.sql.catalog.spark_catalog.uri=https://
s3tables.<Region>.amazonaws.com/iceberg" \
--conf
"spark.sql.catalog.spark_catalog.warehouse=arn:aws:s3tables:<Region>:<accountID>:bucket/
<bucketname>" \
--conf "spark.sql.catalog.spark_catalog.rest.sigv4-enabled=true" \
--conf "spark.sql.catalog.spark_catalog.rest.signing-name=s3tables" \
--conf "spark.sql.catalog.spark_catalog.rest.signing-region=<Region>" \
--conf "spark.sql.catalog.spark_catalog.io-
impl=org.apache.iceberg.aws.s3.S3FileIO" \
--conf
"spark.hadoop.fs.s3a.aws.credentials.provider=org.apache.hadoop.fs.s3a.SimpleAWSCredentialsProvider" \
--conf "spark.sql.catalog.spark_catalog.rest-metrics-reporting-enabled=false"
```

Autenticazione e autorizzazione dell'accesso all'endpoint

Le richieste API agli endpoint del servizio S3 Tables vengono autenticate utilizzando AWS Signature Version 4 (Sigv4). Vedi [AWS Signature Version 4 per le richieste API per saperne di più](#) su Sigv4. AWS

Il nome di firma SigV4 per le richieste degli endpoint Iceberg REST di Tabelle Amazon S3 è: s3tables

Le richieste all'endpoint Iceberg REST di Tabelle Amazon S3 sono autorizzate utilizzando azioni IAM s3tables che corrispondono alle operazioni REST API. Queste autorizzazioni possono essere definite in policy basate su identità IAM o in policy basate su risorse collegate a tabelle e bucket di tabelle. Per ulteriori informazioni, consulta [Gestione degli accessi per Tabelle S3](#).

È possibile monitorare le richieste effettuate alle tabelle tramite l'endpoint REST con AWS CloudTrail. Le richieste verranno registrate nei log come azioni IAM S3 corrispondenti. Ad esempio, un'API LoadTable genererà un evento di gestione per l'operazione GetTableMetadataLocation e un evento di dati per l'operazione GetTableData. Per ulteriori informazioni, consulta [Registrazione con AWS CloudTrail per tabelle S3](#).

Prefisso e parametri di percorso

Le API del catalogo Iceberg REST hanno un prefisso in formato libero negli URL delle richieste. Ad esempio, la chiamata API ListNamespaces utilizza il formato URL GET/v1/{prefix}/

namespaces. Per Tabelle S3, il {prefix} del percorso REST è sempre l'ARN del bucket di tabelle con codifica URL.

Ad esempio, per il seguente ARN di bucket di tabelle: `arn:aws:s3tables:us-east-1:111122223333:bucket/bucketname` il prefisso sarebbe: `arn%3Aaws%3As3tables%3Aus-east-1%3A111122223333%3Abucket%2Fbucketname`

Parametro del percorso namespace

I namespace in un percorso API del catalogo Iceberg REST possono avere più livelli. Tuttavia, Tabelle S3 supporta solo namespace con un singolo livello. Per accedere a un namespace in una gerarchia di cataloghi con più livelli, è possibile connettersi a un catalogo con più livelli sopra il namespace per fare riferimento al namespace. Ciò consente a qualsiasi motore di query che supporti la notazione in tre parti `catalog.namespace.table` di accedere agli oggetti nella gerarchia del catalogo di Tabelle S3 senza problemi di compatibilità rispetto all'utilizzo del namespace multilivello.

Supportata Iceberg REST operazioni API

La tabella seguente contiene le Iceberg REST API supportate e il modo in cui corrispondono alle azioni di Tabelle S3.

Operazione Iceberg REST	Percorso REST	Azione IAM di Tabelle S3	CloudTrail EventName
<code>getConfig</code>	<code>GET /v1/config</code>	<code>s3tables: GetTableBucket</code>	<code>s3tables: GetTableBucket</code>
<code>listNamespaces</code>	<code>GET /v1/{prefix}/namespaces</code>	<code>s3tables: ListNamespaces</code>	<code>s3tables: ListNamespaces</code>
<code>createNamespace</code>	<code>POST /v1/{prefix}/namespaces</code>	<code>s3tables: CreateNamespace</code>	<code>s3tables: CreateNamespace</code>
<code>loadNamespaceMetadata</code>	<code>GET /v1/{prefix}/namespaces/{namespace}</code>	<code>s3tables: GetNamespace</code>	<code>s3tables: GetNamespace</code>

Operazione Iceberg REST	Percorso REST	Azione IAM di Tabelle S3	CloudTrail EventName
dropNamespace	DELETE /v1/{prefix}/namespaces/{namespace}	s3tables: DeleteNamespace	s3tables: DeleteNamespace
listTables	GET /v1/{prefix}/namespaces/{namespace}/tables	s3tables: ListTables	s3tables: ListTables
createTable	POST /v1/{prefix}/namespaces/{namespace}/tables	s3tables: CreateTable, s3tables: PutTableData	s3tables: CreateTable, s3tables: PutObject
loadTable	GET /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables: GetTableMetadataLocation, s3tables: GetTableData	s3tables: GetTableMetadataLocation, s3tables: GetObject
updateTable	POST /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables: UpdateTableMetadataLocation, s3tables: PutTableData, s3tables: GetTableData	s3tables: UpdateTableMetadataLocation, s3tables: PutObject, s3tables: GetObject

Operazione Iceberg REST	Percorso REST	Azione IAM di Tabelle S3	CloudTrail EventName
dropTable	DELETE /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables: DeleteTable	s3tables: DeleteTable
renameTable	POST /v1/{prefix}/tables/rename	s3tables: RenameTable	s3tables: RenameTable
tableExists	HEAD /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables: GetTable	s3tables: GetTable
namespaceExists	HEAD /v1/{prefix}/namespaces/{namespace}	s3tables: GetNamespace	s3tables: GetNamespace

Considerazioni e limitazioni

Di seguito sono riportate le considerazioni e le limitazioni relative all'utilizzo dell'endpoint Iceberg REST di Tabelle Amazon S3.

Considerazioni

- **CreateTable** Comportamento dell'API: `stage-create` l'opzione non è supportata per questa operazione e genera un `400 Bad Request` errore. Ciò significa che non è possibile creare una tabella dai risultati della query utilizzando `CREATE TABLE AS SELECT (CTAS)`.
- **DeleteTable** Comportamento dell'API: puoi eliminare solo le tabelle con l'eliminazione abilitata. L'eliminazione di tabelle con `purge=false` non è supportata e genera un errore `400 Bad Request`. Alcune versioni di Spark impostano sempre questo flag su `false` anche quando

e eseguono i comandi `DROP TABLE PURGE`. Puoi provare `DROP TABLE PURGE` o utilizzare l'[DeleteTable](#) operazione S3 Tables per eliminare una tabella.

- L'endpoint supporta solo le operazioni standard sui metadati delle tabelle. Per la manutenzione delle tabelle, come la gestione e la compattazione di snapshot, utilizza le operazioni API di manutenzione di Tabelle S3. Per ulteriori informazioni, consulta [Manutenzione di Tabelle S3](#).

Limitazioni

- I namespace multilivello non sono supportati.
- OAuth-based l'autenticazione non è supportata.
- Solo la proprietà `owner` è supportata per i namespace.
- View-related Le API definite nella specifica [Apache Iceberg REST Open API non](#) sono supportate.
- L'esecuzione di operazioni su una tabella con un metadata .json file di oltre 50 MB non è supportata e restituirà un `400 Bad Request` errore. Per controllare la dimensione dei file metadata .json, utilizza le operazioni di manutenzione delle tabelle. Per ulteriori informazioni, consulta [Manutenzione di Tabelle S3](#).

Accesso alle tabelle Amazon S3 con Amazon S3 Tables Catalog per Apache Iceberg

È possibile accedere a Tabelle S3 dai motori di query open source come Apache Spark utilizzando il catalogo di Tabelle Amazon S3 per il catalogo client Apache Iceberg. Amazon S3 Tables Catalog for Apache Iceberg è una libreria open source ospitata da Labs. AWS Traduce le operazioni di Apache Iceberg in motori di query (come l'individuazione di tabelle, l'aggiornamento dei metadati e l'aggiunta o la rimozione di tabelle) in operazioni API di Tabelle S3.

Il catalogo di Tabelle Amazon S3 per Apache Iceberg è distribuito come un file Maven JAR chiamato `s3-tables-catalog-for-iceberg.jar`. È possibile creare il file JAR del catalogo cliente dal [repository AWS Labs GitHub](#) o scaricarlo direttamente da [Maven](#). Quando ti connetti alle tabelle, il file JAR del catalogo client viene utilizzato come dipendenza nel momento in cui viene inizializzata una sessione Spark per Apache Iceberg.

Utilizzo del catalogo Amazon S3 Tables per Apache Iceberg con Apache Spark

È possibile utilizzare catalogo di Tabelle Amazon S3 per il catalogo client Apache Iceberg al fine di connettersi alle tabelle da applicazioni open source quando si inizializza una sessione Spark. Nella

configurazione della sessione, devi specificare le dipendenze di Iceberg e di Amazon S3, nonché creare un catalogo personalizzato che utilizza il bucket della tabella come warehouse di metadati.

Prerequisiti

- Un'identità IAM con accesso al bucket della tabella e alle azioni di Tabelle S3. Per ulteriori informazioni, consulta [Gestione degli accessi per Tabelle S3](#).

Per inizializzare un Spark sessione utilizzando il catalogo Amazon S3 Tables per Apache Iceberg

- Inizializzare Spark utilizzando il seguente comando. Per utilizzare il comando, sostituisci il comando `replace the Amazon S3 Tables Catalog for Apache Iceberg` *version number* con la versione più recente del [AWS Labs GitHub repository](#) e quello *table bucket ARN* con il tuo table bucket ARN.

```
spark-shell \  
--packages org.apache.iceberg:iceberg-spark-  
runtime-3.5_2.12:1.6.1,software.amazon.s3tables:s3-tables-catalog-for-iceberg-  
runtime:0.1.4 \  
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \  
--conf spark.sql.catalog.s3tablesbucket.catalog-  
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \  
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-  
east-1:111122223333:bucket/amzn-s3-demo-table-bucket \  
--conf  
spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

Interrogazione di tabelle S3 con Spark SQL

Utilizzando Spark, è possibile eseguire operazioni DQL, DML e DDL sulle tabelle S3. Quando esegui una query sulle tabelle, devi utilizzare il nome completo della tabella, incluso il nome del catalogo della sessione, seguendo questo schema:

CatalogName.NamespaceName.TableName

Le seguenti query di esempio mostrano alcuni modi in cui è possibile interagire con le tabelle S3. Per utilizzare queste query di esempio nel tuo motore di query, sostituisci *user input placeholder* i valori con i tuoi.

Per interrogare le tabelle con Spark

- Creare un namespace

```
spark.sql(" CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

- Creare una tabella

```
spark.sql(" CREATE TABLE IF NOT EXISTS s3tablesbucket.my_namespace.my_table`  
( id INT, name STRING, value INT ) USING iceberg ")
```

- Eseguire una query su una tabella

```
spark.sql(" SELECT * FROM s3tablesbucket.my_namespace.my_table` ").show()
```

- Inserire i dati in una tabella

```
spark.sql(  
    ""  
    INSERT INTO s3tablesbucket.my_namespace.my_table  
    VALUES  
        (1, 'ABC', 100),  
        (2, 'XYZ', 200)  
    ""
```

- Caricare un file di dati esistente in una tabella

1. Leggere i dati in Spark.

```
val data_file_location = "Path such as S3 URI to data file"  
val data_file = spark.read.parquet(data_file_location)
```

2. Scrivere i dati in una tabella Iceberg.

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty  
("format-version", "2").createOrReplace()
```

Esecuzione di query sulle tabelle Amazon S3 con Athena

Amazon Athena è un servizio di query interattivo che semplifica l'analisi dei dati direttamente in Amazon S3 utilizzando SQL standard. Per ulteriori informazioni, consulta [Che cos'è Amazon Athena?](#) nella Guida per l'utente di Amazon Athena.

Dopo aver integrato i bucket di tabelle con i servizi di AWS analisi, puoi eseguire query Data Definition Language (DDL), Data Manipulation Language (DML) e Data Query Language (DQL) sulle tabelle S3 utilizzando Athena. Per ulteriori informazioni su come eseguire query sulle tabelle di un bucket di tabelle, consulta [Registrazione i cataloghi di bucket di tabelle S3](#) nella Guida per l'utente di Amazon Athena.

Puoi eseguire query in Athena anche dalla console Amazon S3.

Important

Durante la creazione delle tabelle, è necessario utilizzare solo lettere minuscole nei nomi delle tabelle e nelle definizioni delle tabelle. Ad esempio, è necessario verificare che i nomi delle colonne siano tutti in minuscolo. Se il nome o la definizione della tabella contiene lettere maiuscole, la tabella non è supportata da o da AWS Lake Formation AWS Glue Data Catalog. In questo caso, la tabella non sarà visibile ai servizi di AWS analisi come Amazon Athena, anche se i bucket di tabelle sono integrati con i servizi di AWS analisi.

Se la definizione della tabella contiene lettere maiuscole, riceverai il seguente messaggio di errore quando esegui una SELECT query in Athena: «`GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Risorsa federativa non supportata: nomi di tabella o colonna non validi.`»

Utilizzo della console S3 e Amazon Athena

La procedura seguente utilizza la console Amazon S3 per accedere all'editor di query Athena in modo da poter eseguire query su una tabella con Amazon Athena.

Note

Prima di eseguire i seguenti passaggi, assicurati di aver integrato i bucket di tabelle con i servizi di analisi AWS nella Regione in uso. Per ulteriori informazioni, consulta [the section called "Integrazione delle tabelle S3 con AWS i servizi di analisi"](#).

Come eseguire query su una tabella

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nella pagina Bucket di tabelle, scegli il bucket contenente la tabella sui cui desideri eseguire la query.
4. Nella pagina dei dettagli del bucket, scegli il pulsante di opzione accanto al nome della tabella su cui desideri eseguire una query.
5. Scegli Interroga tabella con Athena.
6. Si apre la console Amazon Athena e viene visualizzato l'editor di query Athena con una query SELECT di esempio caricata automaticamente. Modifica questa query in base alle esigenze del caso d'uso.

Nell'editor di query, il campo Catalogo deve essere compilato con `s3tablescatalog/` seguito dal nome del bucket di tabelle, ad esempio `s3tablescatalog/amzn-s3-demo-bucket`. Il campo Database deve essere compilato con il namespace in cui è archiviata la tabella.

Note

Se non vedi questi valori nei campi Catalogo e Database, assicurati di aver integrato il bucket di tabelle gestito con i servizi di analisi AWS nella Regione in uso. Per ulteriori informazioni, consulta [the section called “Integrazione delle tabelle S3 con AWS i servizi di analisi”](#).

7. Per eseguire la query, scegli Run (Esegui).

Note

- Se ricevi l'errore “Insufficient permissions to execute the query. Principal does not have any privilege on specified resource” quando provi a eseguire una query in Athena, assicurati di disporre delle necessarie autorizzazioni Lake Formation sulla tabella. Per ulteriori informazioni, consulta [the section called “Concessione dell'autorizzazione Lake Formation per una tabella o un database”](#).
- Se ricevi l'errore «Iceberg non può accedere alla risorsa richiesta» quando provi a eseguire la query, accedi alla AWS Lake Formation console e assicurati di aver

concesso le autorizzazioni per la tabella, il bucket catalog e il database (namespace) che hai creato. Non specificare una tabella quando fornisci queste autorizzazioni. Per ulteriori informazioni, consulta [the section called “Concessione dell'autorizzazione Lake Formation per una tabella o un database”](#).

- Se ricevi il seguente messaggio di errore quando esegui una SELECT query in Athena, questo messaggio è causato dalla presenza di lettere maiuscole nel nome della tabella o nei nomi delle colonne nella definizione della tabella: «GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Risorsa federativa non supportata: nomi di tabella o colonna non validi.» Verifica che i nomi delle tabelle e delle colonne siano tutti in minuscolo.

Accesso alle tabelle Amazon S3 con Amazon Redshift

Amazon Redshift è un servizio di data warehouse rapido, gestito e scalabile a livello di petabyte in grado analizzare correttamente i dati in modo semplice e conveniente utilizzando tutti gli strumenti di business intelligence già presenti. Redshift Serverless consente di accedere ai dati e analizzarli senza tutte le configurazioni di un data warehouse con provisioning. Per ulteriori informazioni, consulta [Introduzione ai data warehouse serverless](#) nella Guida introduttiva di Amazon Redshift.

Esecuzione di query su Tabelle Amazon S3 in Amazon Redshift

Prerequisiti

- [Integrare i bucket di tabelle con i servizi di analisi di AWS](#).
 - [Creare un namespace](#).
 - [Creare una tabella](#).
- [Gestione dell'accesso a una tabella o a un database con Lake Formation](#).

Dopo aver completato i prerequisiti, è possibile iniziare a utilizzare Amazon Redshift per eseguire query sulle tabelle in uno dei seguenti modi:

- [Utilizzando Editor di query V2 Amazon Redshift](#)
- [Eseguendo la connessione a un data warehouse Amazon Redshift tramite gli strumenti del client SQL](#)

- [Utilizzando l'API dati di Amazon Redshift](#)

Accesso alle tabelle Amazon S3 con Amazon EMR

Amazon EMR (precedentemente chiamata Amazon Elastic MapReduce) è una piattaforma cluster gestita che semplifica l'esecuzione di framework di big data, come Apache Hadoop e, su Apache Spark, AWS per elaborare e analizzare grandi quantità di dati. Utilizzando questi framework e i relativi progetti open source, è possibile elaborare i dati per scopi di analisi e carichi di lavoro di business intelligence. Amazon EMR consente inoltre di trasformare e spostare grandi quantità di dati da e verso altri AWS archivi di dati e database.

È possibile usare i cluster Apache Iceberg in Amazon EMR con le tabelle S3 connettendosi ai bucket di tabelle in una sessione di Spark. Per connetterti ai bucket di tabelle in Amazon EMR, puoi utilizzare l'integrazione dei servizi di AWS analisi tramite AWS Glue Data Catalog il catalogo open source Amazon S3 Tables Catalog for client. Apache Iceberg

Note

Tabelle S3 è supportato su [Amazon EMR versione 7.5](#) o successiva.

Connessione ai bucket di tabelle S3 con Spark su Amazon EMR Iceberg cluster

In questa procedura, è possibile impostare un cluster Amazon EMR configurato per Apache Iceberg e avviare una sessione di Spark che si connette ai bucket di tabelle. Puoi configurarlo utilizzando l'integrazione dei servizi di AWS analisi tramite AWS Glue, oppure puoi utilizzare il catalogo open source Amazon S3 Tables Catalog for Apache Iceberg Client. Per ulteriori informazioni sul catalogo del client, consulta [Accesso alle tabelle utilizzando Amazon S3 Tables Iceberg REST endpoint](#).

Scegli il metodo di utilizzo delle tabelle con Amazon EMR tra le seguenti opzioni.

Amazon S3 Tables Catalog for Apache Iceberg

I seguenti prerequisiti sono necessari per eseguire query sulle tabelle con Spark su Amazon EMR utilizzando il Catalogo di Tabelle Amazon S3 per Apache Iceberg.

Per la versione più recente del catalogo client JAR, consulta il repository [GitHub s3-tables-catalog](#).

Prerequisiti

- Associare la policy AmazonS3TablesFullAccess al ruolo IAM utilizzato per Amazon EMR.

Per configurare un cluster Amazon EMR per interrogare le tabelle con Spark

1. Crea un cluster con la seguente configurazione. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws emr create-cluster --release-label emr-7.5.0 \  
--applications Name=Spark \  
--configurations file://configurations.json \  
--region us-east-1 \  
--name My_Spark_Iceberg_Cluster \  
--log-uri s3://amzn-s3-demo-bucket/ \  
--instance-type m5.xlarge \  
--instance-count 2 \  
--service-role EMR_DefaultRole \  
--ec2-attributes \  
  
InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

configurations.json:

```
[{  
  "Classification":"iceberg-defaults",  
  "Properties":{"iceberg.enabled":"true"}  
}]
```

2. [Connettersi al nodo principale di Spark tramite SSH.](#)
3. Per inizializzare una sessione di Spark per Iceberg che si connette al proprio bucket di tabelle, inserire il seguente comando. Sostituisci *user input placeholders* con l'ARN del bucket di tabelle.

```
spark-shell \  
--packages software.amazon.s3tables:s3-tables-catalog-for-iceberg-runtime:0.1.8 \  
\  
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \  
--conf spark.sql.catalog.s3tablesbucket.catalog-  
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \  

```



```
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-  
east-1:111122223333:bucket/amzn-s3-demo-bucket1 \  
--conf spark.sql.defaultCatalog=s3tablesbucket \  
--conf  
spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

4. Eseguire query sulle tabelle con Spark SQL. Per query di esempio, consulta [the section called “Interrogazione di tabelle S3 con Spark SQL”](#).

AWS analytics services integration

I seguenti prerequisiti sono necessari per interrogare le tabelle con Spark Amazon EMR utilizzando l'integrazione dei servizi di AWS analisi.

Prerequisiti

- [Integra i tuoi bucket di tabelle con i servizi di analisi AWS](#).
- Crea il ruolo di servizio predefinito per Amazon EMR (EMR_DefaultRole_V2). Per i dettagli, consulta [Ruolo di servizio per Amazon EMR \(ruolo EMR\)](#).
- Crea il profilo dell'istanza Amazon EC2 per Amazon EMR (EMR_EC2_DefaultRole). Per i dettagli, consulta [Ruolo di servizio per istanze EC2 del cluster \(profilo dell'istanza EC2\)](#).
- Collega la policy AmazonS3TablesFullAccess a EMR_EC2_DefaultRole.

Per configurare un cluster Amazon EMR con cui interrogare le tabelle Spark

1. Crea un cluster con la seguente configurazione. Per utilizzare questo esempio, sostituisci i valori *user input placeholder* con le informazioni appropriate.

```
aws emr create-cluster --release-label emr-7.5.0 \  
--applications Name=Spark \  
--configurations file://configurations.json \  
--region us-east-1 \  
--name My_Spark_Iceberg_Cluster \  
--log-uri s3://amzn-s3-demo-bucket/ \  
--instance-type m5.xlarge \  
--instance-count 2 \  
--service-role EMR_DefaultRole \  
--ec2-attributes \  

```

```
InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

configurations.json:

```
[{  
  "Classification":"iceberg-defaults",  
  "Properties":{"iceberg.enabled":"true"}  
}]
```

2. [Connettersi al nodo principale di Spark tramite SSH.](#)
3. Inserire il seguente comando per inizializzare una sessione di Spark per Iceberg che si connette alle proprie tabelle. Sostituisci *user input placeholders* per la Regione, l'ID dell'account e il nome del bucket di tabelle con le informazioni appropriate.

```
spark-shell \  
--conf  
  spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions  
\  
--conf spark.sql.defaultCatalog=s3tables \  
--conf spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog \  
--conf spark.sql.catalog.s3tables.catalog-  
impl=org.apache.iceberg.aws.glue.GlueCatalog \  
--conf spark.sql.catalog.s3tables.client.region=us-east-1 \  
--conf spark.sql.catalog.s3tables.glue.id=111122223333:s3tablescatalog/amzn-s3-  
demo-table-bucket
```

4. Eseguire query sulle tabelle con Spark SQL. Per query di esempio, consulta [the section called "Interrogazione di tabelle S3 con Spark SQL"](#).

Note

Se si utilizza il comando `DROP TABLE PURGE` con Amazon EMR:

- Amazon EMR versione 7.5

Imposta la configurazione di Spark su `spark.sql.catalog.your-catalog-name.cache-enabled` per `false`. Se questa configurazione è impostata su `true`, eseguire il comando in una nuova sessione o applicazione in modo che la cache della tabella non venga attivata.

- Versioni di Amazon EMR successive alla 7.5

DROP TABLE non è supportato. È possibile utilizzare la REST API DeleteTable di Tabelle S3 per eliminare una tabella.

Visualizzazione dei dati delle tabelle con Quick

Quick è un servizio di analisi aziendale veloce per creare visualizzazioni, eseguire analisi ad hoc e ottenere rapidamente informazioni aziendali dai tuoi dati. Quick rileva facilmente le fonti di AWS dati, consente alle organizzazioni di scalare fino a centinaia di migliaia di utenti e offre prestazioni di query rapide e reattive utilizzando il Quick Super-fast, Parallel In-Memory, Calculation Engine (SPICE). Per ulteriori informazioni, consulta [What is Quick?](#) nella Guida rapida per l'utente.

Dopo aver [integrato i bucket di tabelle con i servizi di AWS analisi](#), puoi creare set di dati dalle tabelle e utilizzarli in Quick usando SPICE o interrogazioni SQL dirette dal tuo motore di query. Quick supporta Athena come fonte di dati per le tabelle S3.

Configura le autorizzazioni per Quick to access alle tabelle

Prima di lavorare con i dati delle tabelle S3 in Quick, devi concedere le autorizzazioni al ruolo di servizio Quick e alle autorizzazioni utente di Quick admin sulle tabelle a cui desideri accedere. Inoltre, se lo utilizzi AWS Lake Formation, devi anche concedere le autorizzazioni di Lake Formation all'utente amministratore di Quick per le tabelle a cui desideri accedere.

Concedi le autorizzazioni al ruolo di servizio Quick

Quando configuri Quick per la prima volta nel tuo account, AWS crea un ruolo di servizio che consente a Quick di accedere alle origini dati di altri AWS servizi, come Athena o Amazon Redshift. Il nome del ruolo predefinito è `aws-quicksight-service-role-v0`.

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Scegli Ruoli e seleziona il ruolo del servizio Quick. Il nome predefinito è `aws-quicksight-service-role-v0`
3. Scegli Aggiungi autorizzazioni, quindi seleziona Crea policy inline.
4. Seleziona JSON per aprire l'editor di policy JSON, quindi aggiungi la seguente policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "glue:GetCatalog",
      "Resource": "*"
    }
  ]
}
```

5. Scegli Successivo, inserisci un Nome policy e seleziona Crea policy.

Per configurare le autorizzazioni di Lake Formation per l'utente amministratore di Quick

1. Esegui il AWS CLI comando seguente per trovare l'ARN del tuo utente amministratore Quick.

```
aws quicksight list-users --aws-account-id 111122223333 --namespace default --
region region
```

2. Fornisci le autorizzazioni di Lake Formation a questo ARN. Per informazioni dettagliate, vedi [Gestione dell'accesso a una tabella o a un database con Lake Formation](#).

Utilizzo dei dati della tabella in Quick

È possibile connettersi ai dati delle tabelle utilizzando Athena come origine dati.

Prerequisiti

- [Integrare i bucket di tabelle con i servizi di analisi di AWS](#).
- [Creare un namespace](#).
- [Creare una tabella](#).
- [Configura le autorizzazioni per Quick to access alle tabelle](#).
- [Iscriviti a Quick](#).

1. Accedi al tuo account Quick all'indirizzo <https://quicksight.aws.amazon.com/>
2. Nella dashboard, scegli Nuova analisi.
3. Scegli Nuovo set di dati.
4. Seleziona Athena.
5. Inserisci un Nome dell'origine dati e scegli Crea origine dati.
6. Scegliere Usa SQL personalizzato. Non è possibile selezionare la tabella dal riquadro Scegli la tua tabella.
7. Inserisci una query SQL Athena che acquisisca le colonne da visualizzare, quindi scegli Conferma query. Ad esempio, utilizza la seguente query per selezionare tutte le colonne:

```
SELECT * FROM "s3tablescatalog/table-bucket-name".namespace.table-name
```

8. Scegli Visualizza per analizzare i dati e iniziare a creare le dashboard. Per ulteriori informazioni, consulta [Visualizzazione dei dati in Quick](#) ed [Esplorazione delle dashboard interattive in Quick](#)

Streaming di dati alle tabelle con Amazon Data Firehose

Amazon Data Firehose è un servizio completamente gestito per la distribuzione di dati in [streaming in tempo reale](#) verso destinazioni come Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk, Apache Iceberg tabelle ed endpoint HTTP personalizzati o endpoint HTTP di proprietà di fornitori di servizi di terze parti supportati. Con Amazon Data Firehose, non è necessario scrivere applicazioni o gestire risorse. È sufficiente configurare i produttori di dati perché inviino i dati a Firehose, che li distribuirà automaticamente alla destinazione specificata. È anche possibile configurare Firehose per trasformare i dati prima di distribuirli. Per ulteriori informazioni su Amazon Data Firehose, consultare [Cos'è Amazon Data Firehose?](#)

Completare queste fasi per configurare lo streaming Firehose nelle tabelle dei bucket di tabelle S3:

1. [Integrare i bucket di tabelle con i servizi di analisi di AWS.](#)
2. Configurare Firehose per fornire dati nelle tabelle S3. A tale scopo, [crei un ruolo di servizio AWS Identity and Access Management \(IAM\) che consenta a Firehose di accedere alle tue tabelle.](#)
3. Fornire al ruolo di servizio Firehose autorizzazioni esplicite per la tabella o il namespace di tabelle. Per ulteriori informazioni, consulta [Concedere le autorizzazioni](#) necessarie.
4. [Creare un flusso Firehose che indirizza i dati alla tabella.](#)

Creazione di un ruolo per Firehose per l'uso delle tabelle S3 come destinazione

Firehose necessita di un ruolo [di servizio IAM](#) con autorizzazioni specifiche per accedere alle AWS Glue tabelle e scrivere dati nelle tabelle S3. È necessario fornire questo ruolo IAM quando si crea un flusso Firehose.

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione a sinistra, seleziona Policy.
3. Scegli Crea una policy e scegliere JSON nell'editor delle policy.
4. Aggiungere la seguente policy in linea che concede le autorizzazioni a tutti i database e alle tabelle del catalogo dei dati. Se lo si desidera, è possibile concedere le autorizzazioni solo a tabelle e database specifici. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3TableAccessViaGlueFederation",
      "Effect": "Allow",
      "Action": [
        "glue:GetTable",
        "glue:GetDatabase",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:us-east-1:111122223333:catalog/s3tablescatalog/*",
        "arn:aws:glue:us-east-1:111122223333:catalog/s3tablescatalog",
        "arn:aws:glue:us-east-1:111122223333:catalog",
        "arn:aws:glue:us-east-1:111122223333:database/*",
        "arn:aws:glue:us-east-1:111122223333:table/*/*"
      ]
    },
    {
      "Sid": "S3DeliveryErrorBucketPermission",
      "Effect": "Allow",

```

```

        "Action": [
            "s3:AbortMultipartUpload",
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:ListBucketMultipartUploads",
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::error delivery bucket",
            "arn:aws:s3:::error delivery bucket/*"
        ]
    },
    {
        "Sid": "RequiredWhenUsingKinesisDataStreamsAsSource",
        "Effect": "Allow",
        "Action": [
            "kinesis:DescribeStream",
            "kinesis:GetShardIterator",
            "kinesis:GetRecords",
            "kinesis:ListShards"
        ],
        "Resource": "arn:aws:kinesis:us-east-1:111122223333:stream/stream-name"
    },
    {
        "Sid": "RequiredWhenDoingMetadataReadsANDDataAndMetadataWriteViaLakeformation",
        "Effect": "Allow",
        "Action": [
            "lakeformation:GetDataAccess"
        ],
        "Resource": "*"
    },
    {
        "Sid": "RequiredWhenUsingKMSEncryptionForS3ErrorBucketDelivery",
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": [
            "arn:aws:kms:us-east-1:111122223333:key/KMS-key-id"
        ]
    }

```

```

        "Condition": {
            "StringEquals": {
                "kms:ViaService": "s3.us-east-1.amazonaws.com"
            },
            "StringLike": {
                "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::error
delivery bucket/prefix*"
            }
        }
    },
    {
        "Sid": "LoggingInCloudWatch",
        "Effect": "Allow",
        "Action": [
            "logs:PutLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:us-east-1:111122223333:log-group:log-group-
name:log-stream:log-stream-name"
        ]
    },
    {
        "Sid": "RequiredWhenAttachingLambdaToFirehose",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction",
            "lambda:GetFunctionConfiguration"
        ],
        "Resource": [
            "arn:aws:lambda:us-east-1:111122223333:function:func-
tion-version"
        ]
    }
]
}

```

Questa policy contiene istruzioni che consentono l'accesso a Kinesis Data Streams, invocando le funzioni Lambda e l'accesso alle chiavi AWS KMS. Se non si utilizza nessuna di queste risorse, è possibile rimuovere le rispettive istruzioni.

Se la registrazione degli errori è abilitata, Firehose invia anche gli errori di consegna dei dati al gruppo di log e ai flussi. CloudWatch Per questo motivo, è necessario configurare i nomi del

gruppo di log e del flusso di log. Per i nomi dei gruppi di log e dei flussi di log, consulta [Monitor Amazon Data Firehose Using Logs. CloudWatch](#)

5. Dopo aver creato la policy, creare un ruolo IAM con il servizio AWS come il Tipo di entità attendibile.
6. Per Servizio o caso d'uso scegli Kinesis. Per Caso d'uso scegli Kinesis Firehose.
7. Scegli Successivo, quindi seleziona la policy creata in precedenza.
8. Assegnare un nome al proprio ruolo. Verifica i dettagli del ruolo e scegli Crea ruolo. Il ruolo avrà la seguente policy di attendibilità.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Principal": {
        "Service": [
          "firehose.amazonaws.com"
        ]
      }
    }
  ]
}
```

Creazione di un flusso Firehose alle tabelle S3

La seguente procedura mostra come creare un flusso Firehose per fornire dati alle tabelle S3 utilizzando la console. I seguenti prerequisiti sono necessari per configurare un flusso Firehose alle tabelle S3.

Prerequisiti

- [Integrare i bucket di tabelle con i servizi di analisi di AWS.](#)
- [Creare un namespace.](#)

- [Creare una tabella.](#)
- Creare il [ruolo per Firehose per accedere alle tabelle S3.](#)
- [Concedi le autorizzazioni necessarie](#) al ruolo del servizio Firehose che hai creato per accedere alle tabelle.

Per fornire informazioni di instradamento a Firehose quando si configura un flusso, si utilizza il namespace come il nome del database e il nome di una tabella in tale namespace. È possibile utilizzare questi valori nella sezione Chiave unica di una configurazione del flusso Firehose per instradare i dati a una singola tabella. È inoltre possibile utilizzare questi valori per eseguire l'instradamento a una tabella utilizzando le espressioni di query JSON. Per ulteriori informazioni, consulta [Instradare i record in entrata a una singola tabella Iceberg.](#)

Per configurare un flusso su tabelle S3 (console)

1. Apri la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegli Crea un flusso Firehose.
3. Per Origine scegli una delle seguenti origini:
 - Flusso di dati Amazon Kinesis
 - MSK Amazon
 - PUT diretto
4. Per Destinazione scegliere Tabelle Apache Iceberg.
5. Immettere un nome per il flusso Firehose.
6. Configurare le impostazioni dell'origine.
7. Per le impostazioni di destinazione, scegli Account corrente per lo streaming sulle tabelle del tuo account o Cross-account per le tabelle di un altro account.
 - Per le tabelle dell'Account corrente, selezionare il catalogo Tabelle S3 dal menu a discesa Catalogo.
 - Per le tabelle in a Cross-account, inserisci l'ARN del catalogo su cui desideri eseguire lo streaming in un altro account.
8. Configurare i nomi di database e tabelle utilizzando la Configurazione della chiave unica, le espressioni JSONQuery o una funzione Lambda. Per ulteriori informazioni, consultare [Instradare i record in entrata a una singola tabella Iceberg](#) e [Instradare i record in entrata a diverse tabelle Iceberg](#) nella Guida per gli sviluppatori di Amazon Data Firehose.

9. In Impostazioni di backup specificare un bucket di backup S3.
10. Per Ruoli IAM esistenti in Impostazioni avanzate, seleziona il ruolo IAM creato per Firehose.
11. Scegli Crea un flusso Firehose.

Per ulteriori informazioni sulle altre impostazioni che è possibile configurare per un flusso, consultare [Configurare il flusso Firehose](#) nella Guida per gli sviluppatori di Amazon Data Firehose.

Esecuzione di processi ETL su tabelle Amazon S3 con AWS Glue

AWS Glue è un servizio di integrazione dei dati senza server che consente agli utenti di analisi di scoprire, preparare, spostare e integrare facilmente i dati da più fonti. Puoi utilizzare i AWS Glue job per eseguire pipeline di estrazione, trasformazione e caricamento (ETL) per caricare i dati nei tuoi data lake. Per ulteriori informazioni su AWS Glue, vedi [Che cos'è? AWS Glue](#) nella Guida per AWS Glue gli sviluppatori.

Un AWS Glue job incapsula uno script che si connette ai dati di origine, li elabora e poi li scrive nella destinazione dei dati. Di solito un processo esegue script di estrazione, trasformazione e caricamento (ETL). I processi possono eseguire script progettati per gli ambienti di runtime di Apache Spark. È possibile monitorare le esecuzioni dei processi per comprendere i parametri di runtime come esito positivo, durata e ora di inizio.

Puoi utilizzare i AWS Glue job per elaborare i dati nelle tabelle S3 connettendoti alle tabelle tramite l'integrazione con i servizi di AWS analisi oppure collegarti direttamente utilizzando l'Iceberg REST endpoint Amazon S3 Tables o il catalogo Amazon S3 Tables per Apache Iceberg. Questa guida illustra i passaggi di base per iniziare a utilizzare AWS Glue S3 Tables, tra cui:

Argomenti

- [Fase 1: prerequisiti](#)
- [Fase 2: creazione di uno script per il collegamento ai bucket della tabella](#)
- [Fase 3: creare un AWS Glue lavoro che interroga le tabelle](#)

Scegliete il metodo di accesso in base ai requisiti specifici del vostro lavoro AWS Glue ETL:

- AWS integrazione dei servizi di analisi (consigliata): consigliata quando hai bisogno di una gestione centralizzata dei metadati su più servizi di AWS analisi, devi sfruttare le autorizzazioni esistenti del AWS Glue Data Catalog e, facoltativamente, Lake Formation o stai creando pipeline ETL di produzione che si integrano con altri servizi come Athena o Amazon EMR. AWS

- Iceberg RESTEndpoint Amazon S3 Tables: consigliato quando è necessario connettersi a tabelle S3 da motori di query di terze parti che supportano Apache Iceberg, creare applicazioni ETL personalizzate che richiedono l'accesso diretto all'API REST o quando è necessario il controllo sulle operazioni di catalogo senza dipendenze da AWS Glue Data Catalog.
- Catalogo di Tabelle Amazon S3 per Apache Iceberg: da utilizzare solo per applicazioni legacy o scenari di programmazione specifici che richiedono la libreria client Java. Questo metodo non è consigliato per nuove implementazioni di processi AWS Glue ETL a causa della gestione e della complessità aggiuntive delle dipendenze. JAR

Note

Il servizio Tabelle Amazon S3 è supportato su [AWS Glue versione 5.0 o successiva](#).

Fase 1: prerequisiti

Prima di poter interrogare le tabelle di un AWS Glue job, è necessario configurare un ruolo IAM da AWS Glue utilizzare per eseguire il job. Scegli il metodo di accesso per visualizzare i prerequisiti specifici relativi a quel metodo.

AWS analytics services integration (Recommended)

Prerequisiti necessari per utilizzare l'integrazione AWS analitica di S3 Tables per eseguire AWS Glue i job.

- [Integrare i bucket di tabelle con i servizi di analisi di AWS](#).
- [Crea un ruolo IAM per. AWS Glue](#)
 - Collegare la policy gestita AmazonS3TablesFullAccess al ruolo.
 - Collegare la policy gestita AmazonS3FullAccess al ruolo.

Amazon S3 Tables Iceberg REST endpoint

Prerequisiti per utilizzare l'Iceberg RESTendpoint Amazon S3 Tables per eseguire AWS Glue processi ETL.

- [Crea un ruolo IAM per. AWS Glue](#)
 - Collegare la policy gestita AmazonS3TablesFullAccess al ruolo.

- Collegare la policy gestita AmazonS3FullAccess al ruolo.

Amazon S3 Tables Catalog for Apache Iceberg

I prerequisiti utilizzano il catalogo Amazon S3 Tables per Apache Iceberg eseguire processi AWS Glue ETL.

- [Crea un ruolo IAM per. AWS Glue](#)
 - Collegare la policy gestita AmazonS3TablesFullAccess al ruolo.
 - Collegare la policy gestita AmazonS3FullAccess al ruolo.
 - Per utilizzare il catalogo di Tabelle Amazon S3 per Apache Iceberg, è necessario scaricare il catalogo client JAR e caricarlo in un bucket S3.

Scaricamento del catalogo BARATTOLO

1. Individua la versione più recente su [Maven Central](#). Puoi scaricare il file JAR da Maven Central tramite il browser oppure utilizzando il seguente comando. Assicurati di sostituirlo *version number* con la versione più recente.

```
wget https://repo1.maven.org/maven2/software/amazon/s3tables/s3-  
tables-catalog-for-iceberg-runtime/0.1.5/s3-tables-catalog-for-iceberg-  
runtime-0.1.5.jar
```

2. Carica il file JAR scaricato in un bucket S3 accessibile dal tuo ruolo IAM di AWS Glue . È possibile utilizzare il seguente AWS CLI comando per caricare il file JAR. Assicurati di sostituire la versione *version number* con la più recente e la *bucket name* e *path* con la tua.

```
aws s3 cp s3-tables-catalog-for-iceberg-runtime-0.1.5.jar s3://amzn-s3-demo-  
bucket/jars/
```

Fase 2: creazione di uno script per il collegamento ai bucket della tabella

Per accedere ai dati della tabella quando esegui un processo AWS Glue ETL, configuri una Spark sessione Apache Iceberg che si connette al bucket della tabella S3. Puoi modificare uno script esistente per collegarti al bucket della tabella o creare un nuovo script. Per ulteriori informazioni sulla

creazione di AWS Glue script, consulta [Tutorial: Scrivere uno script AWS Glue](#) per Spark nella Guida per gli sviluppatori. AWS Glue

Puoi configurare la sessione per connetterti ai bucket della tabella utilizzando uno dei seguenti metodi di accesso di Tabelle Amazon S3:

- Integrazione dei servizi di AWS analisi S3 Tables (consigliata)
- Endpoint Iceberg REST di Tabelle Amazon S3
- Catalogo di Tabelle Amazon S3 per Apache Iceberg

Scegli tra i seguenti metodi di accesso per visualizzare le istruzioni e gli esempi di configurazione.

AWS analytics services integration (Recommended)

Come prerequisito per interrogare le tabelle AWS Glue utilizzando l'integrazione dei servizi di AWS analisi, è necessario [integrare i bucket di tabelle con Spark i servizi di analisi AWS](#)

Puoi configurare la connessione al tuo table bucket tramite una Spark sessione in un job o con AWS Glue Studio magics in una sessione interattiva. Per utilizzare gli esempi seguenti, sostituisci il bucket *placeholder values* con le informazioni relative al tuo table bucket.

Usare uno script PySpark

Usa il seguente frammento di codice in PySpark uno script per configurare un AWS Glue job da connettere al tuo table bucket utilizzando l'integrazione.

```
spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.jars.packages", "org.apache.iceberg:iceberg-spark-
runtime-3.4_2.12:1.4.2") \
    .config("spark.sql.extensions",
"org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tables") \
    .config("spark.sql.catalog.s3tables",
"org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
"org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
"111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-
bucket/warehouse/") \
```

```
.getOrCreate()
```

Utilizzo di una sessione AWS Glue interattiva

Se utilizzi una sessione notebook interattiva con AWS Glue 5.0, specifica le stesse configurazioni usando il comando magic `%%configure` in una cella prima dell'esecuzione del codice.

```
%%configure
{"conf":
  "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
  --conf spark.sql.defaultCatalog=s3tables --conf
  spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog --conf
  spark.sql.catalog.s3tables.catalog-impl=org.apache.iceberg.aws.glue.GlueCatalog
  --conf spark.sql.catalog.s3tables.glue.id=111122223333:s3tablescatalog/amzn-s3-
demo-table-bucket --conf spark.sql.catalog.s3tables.warehouse=s3://amzn-s3-demo-
table-bucket/warehouse/"}
```

Amazon S3 Tables Iceberg REST endpoint

Puoi configurare la connessione al tuo table bucket tramite una Spark sessione in un job o con AWS Glue Studio magics in una sessione interattiva. Per utilizzare gli esempi seguenti, sostituisci il bucket *placeholder values* con le informazioni relative al tuo table bucket.

Usare uno script PySpark

Utilizzate il seguente frammento di codice in PySpark uno script per configurare un AWS Glue job per connettersi al bucket della tabella utilizzando l'endpoint.

```
spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.jars.packages", "org.apache.iceberg:iceberg-spark-
runtime-3.4_2.12:1.4.2") \
    .config("spark.sql.extensions",
    "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
    "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
    "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
```

```
.config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
.config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
.config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
.config('spark.sql.catalog.s3_rest_catalog.io-impl', 'org.apache.iceberg.aws.s3.S3FileIO') \
.config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-enabled', 'false') \
.getOrCreate()
```

Utilizzo di una sessione AWS Glue interattiva

Se utilizzate una sessione interattiva del notebook con AWS Glue 5.0, specificate le stesse configurazioni utilizzando la `%%configure` magia in una cella prima dell'esecuzione del codice. Sostituisci i valori segnaposto con le informazioni relative al bucket della tabella.

```
%%configure
{"conf":
  "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
  --conf spark.sql.defaultCatalog=s3_rest_catalog --conf
  spark.sql.catalog.s3_rest_catalog=org.apache.iceberg.spark.SparkCatalog
  --conf spark.sql.catalog.s3_rest_catalog.type=rest --conf
  spark.sql.catalog.s3_rest_catalog.uri=https://s3tables.Region.amazonaws.com/
  iceberg --conf
  spark.sql.catalog.s3_rest_catalog.warehouse=arn:aws:s3tables:Region:111122223333:bucket/
  amzn-s3-demo-table-bucket --conf spark.sql.catalog.s3_rest_catalog.rest.sigv4-
  enabled=true --conf spark.sql.catalog.s3_rest_catalog.rest.signing-name=s3tables
  --conf spark.sql.catalog.s3_rest_catalog.rest.signing-region=Region --conf
  spark.sql.catalog.s3_rest_catalog.io-impl=org.apache.iceberg.aws.s3.S3FileIO --
  conf spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-enabled=false"}

```

Amazon S3 Tables Catalog for Apache Iceberg

Come prerequisito per la connessione alle tabelle utilizzando il catalogo di Tabelle Amazon S3 per Apache Iceberg, devi innanzitutto scaricare il file jar del catalogo più recente e caricarlo in un bucket S3. Quindi, quando crei il processo, devi aggiungere il percorso al file JAR del catalogo client come parametro speciale. Per ulteriori informazioni sui parametri dei job in AWS Glue, consultate [Special Parameters used in AWS Glue jobs](#) nella AWS Glue Developer Guide.

Puoi configurare la connessione al tuo table bucket tramite una Spark sessione in un job o con AWS Glue Studio magics in una sessione interattiva. Per utilizzare gli esempi seguenti, sostituisci il bucket *placeholder values* con le informazioni relative al tuo table bucket.

Utilizzo di uno script PySpark

Usa il seguente frammento di codice in PySpark uno script per configurare un AWS Glue job per connettersi al tuo bucket di tabelle usando il JAR. Sostituisci i valori segnaposto con le informazioni relative al bucket della tabella.

```
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.jars.packages", "org.apache.iceberg:iceberg-spark-
runtime-3.4_2.12:1.4.2") \
    .config("spark.sql.extensions",
"org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
"org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
"software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
"arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()
```

Utilizzo di una sessione AWS Glue interattiva

Se stai usando una sessione interattiva del notebook con AWS Glue 5.0, specifica le stesse configurazioni usando la %%configure magia in una cella prima dell'esecuzione del codice. Sostituisci i valori segnaposto con le informazioni relative al bucket della tabella.

```
%%configure
{"conf":
  "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
--conf spark.sql.defaultCatalog=s3tablesbucket --conf
spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog --conf
spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:Region:111122223333:bucket/
amzn-s3-demo-table-bucket", "extra-jars": "s3://amzn-s3-demo-bucket/jars/s3-
tables-catalog-for-iceberg-runtime-0.1.5.jar"}
```

Script di esempio

I seguenti PySpark script di esempio possono essere usati per testare l'interrogazione di tabelle S3 con un job. AWS Glue. Questi script si connettono al bucket della tabella ed eseguono query per

creare un nuovo namespace, creare una tabella di esempio, inserire dati nella tabella e restituire i dati della tabella. Per utilizzare gli script, sostituiscili *placeholder values* con le informazioni relative al tuo bucket di tabelle.

Scegli tra i seguenti script in base al tuo metodo di accesso a Tabelle S3.

S3 Tables integration with AWS analytics services

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.jars.packages", "org.apache.iceberg:iceberg-spark-  
runtime-3.4_2.12:1.4.2") \
    .config("spark.sql.extensions",  
"org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tables") \
    .config("spark.sql.catalog.s3tables", "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",  
"org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",  
"111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-bucket/  
bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

namespace = "new_namespace"
table = "new_table"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
        id INT,
        name STRING,
        value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
```

```

        (1, 'ABC', 100),
        (2, 'XYZ', 200)
    """)

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()

```

Amazon S3 Tables Iceberg REST endpoint

```

from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.jars.packages", "org.apache.iceberg:iceberg-spark-
runtime-3.4_2.12:1.4.2") \
    .config("spark.sql.extensions",
"org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
"org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
"arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl', 'org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled', 'false') \
    .getOrCreate()

namespace = "s3_tables_rest_namespace"
table = "new_table_s3_rest"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
        id INT,
        name STRING,

```

```

        value INT
    )
    """)

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
        (1, 'ABC', 100),
        (2, 'XYZ', 200)
    """)

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()

```

Amazon S3 Tables Catalog for Apache Iceberg

```

from pyspark.sql import SparkSession

#Spark session configurations
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.jars.packages", "org.apache.iceberg:iceberg-spark-
runtime-3.4_2.12:1.4.2") \
    .config("spark.sql.extensions",
"org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
"org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
"software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
"arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

#Script
namespace = "new_namespace"
table = "new_table"

spark.sql(f"CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.{namespace}")
spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (

```

```
        id INT,  
        name STRING,  
        value INT  
    )  
""")  
  
spark.sql(f"""  
    INSERT INTO {namespace}.{table}  
    VALUES  
        (1, 'ABC', 100),  
        (2, 'XYZ', 200)  
""")  
  
spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Fase 3: creare un AWS Glue lavoro che interroga le tabelle

Le seguenti procedure mostrano come configurare i AWS Glue job che si connettono ai bucket di tabelle S3. Puoi farlo usando AWS CLI o usando la console con l'editor di AWS Glue Studio script. Per ulteriori informazioni, consulta [Creazione di processi in AWS Glue](#) nella Guida per l'utente di AWS Glue .

Utilizzo AWS Glue Studio editor di script

La procedura seguente mostra come utilizzare l'editor di AWS Glue Studio script per creare un job ETL che interroga le tabelle S3.

Prerequisiti

- [Fase 1: prerequisiti](#)
- [Fase 2: creazione di uno script per il collegamento ai bucket della tabella](#)

1. Apri la console all' AWS Glue indirizzo. <https://console.aws.amazon.com/glue/>
2. Nel riquadro di navigazione, seleziona Processi ETL.
3. Seleziona Editor di script, quindi scegli Carica script e carica lo script PySpark che hai creato per interrogare le tabelle S3.
4. Seleziona la scheda Dettagli del processo e inserisci quanto segue per Proprietà di base.
 - In Nome, inserisci un nome per il processo.

- In Ruolo IAM, seleziona il ruolo creato per AWS Glue.
5. (Facoltativo) Se utilizzi il catalogo di Tabelle Amazon S3 per Apache Iceberg come metodo di accesso, espandi Proprietà avanzate e per il percorso dei file JAR dipendenti inserisci l'URI S3 del file jar del catalogo client che hai caricato in un bucket S3 come prerequisito. Ad esempio, `s3://amzn-s3-demo-bucket1/jars0.1.5/s3-tables-catalog-for-iceberg-runtime- .jar`
 6. Seleziona Salva per creare il processo.
 7. Seleziona Esegui per avviare il processo e verifica lo stato del processo stesso nella scheda Esecuzioni.

Utilizzo di AWS CLI

La procedura seguente mostra come utilizzare per creare un job ETL che interroga le tabelle S3. AWS CLI Per utilizzare i comandi, sostituiscili *placeholder values* con i tuoi.

Prerequisiti

- [Fase 1: prerequisiti](#)
- [Fase 2: creazione di uno script per il collegamento ai bucket della tabella](#) e relativo caricamento in un bucket S3.

1. Crea un AWS Glue lavoro.

```
aws glue create-job \  
--name etl-tables-job \  
--role arn:aws:iam::111122223333:role/AWSGlueServiceRole \  
--command '{  
    "Name": "glueetl",  
    "ScriptLocation": "s3://amzn-s3-demo-bucket1/scripts/glue-etl-query.py",  
    "PythonVersion": "3"  
}' \  
--default-arguments '{  
    "--job-language": "python",  
    "--class": "GlueApp"  
}' \  
--glue-version "5.0"
```

 Note

(Facoltativo) Se utilizzi il catalogo di Tabelle Amazon S3 per Apache Iceberg come metodo di accesso, aggiungi il file JAR del catalogo client a `--default-arguments` utilizzando il parametro `--extra-jars`. Sostituisci il parametro *input placeholders* con il tuo quando aggiungi il parametro.

```
"--extra-jars": "s3://amzn-s3-demo-bucket/jar-path/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar"
```

2. Avvia il processo.

```
aws glue start-job-run \  
--job-name etl-tables-job
```

3. Per verificare lo stato del processo, copia l'ID di esecuzione dal comando precedente e inseriscilo nel comando seguente.

```
aws glue get-job-run --job-name etl-tables-job \  
--run-id jr_ec9a8a302e71f8483060f87b6c309601ea9ee9c1ffc2db56706dfcceb3d0e1ad
```

Guida introduttiva all'interrogazione di tabelle S3 con Amazon Unified Studio SageMaker

Amazon SageMaker Unified Studio è un servizio di analisi completo che ti consente di interrogare e ricavare informazioni dai tuoi dati utilizzando SQL, linguaggio naturale e notebook interattivi. Supporta la collaborazione in team e i flussi di lavoro di analisi tra repository di AWS dati e fonti di terze parti all'interno di un'interfaccia unificata. SageMaker Unified Studio si integra direttamente con S3 Tables, fornendo una transizione senza interruzioni dallo storage dei dati all'analisi all'interno della console Amazon S3.

Puoi integrare S3 Tables con SageMaker Unified Studio tramite la console Amazon S3 o la console Unified Studio. SageMaker

Per la configurazione tramite la console SageMaker Unified Studio, consulta la documentazione di Unified Studio. [SageMaker](#)

Requisiti per l'interrogazione delle tabelle S3 con Unified Studio SageMaker

L'utilizzo di SageMaker Unified Studio con tabelle S3 richiede quanto segue:

- I tuoi bucket di tabelle sono stati integrati con i servizi di AWS analisi nella regione corrente. Per ulteriori informazioni, consulta [Integrazione delle tabelle S3 con AWS i servizi di analisi](#).
- Stai utilizzando un ruolo IAM con autorizzazioni per creare e visualizzare risorse in SageMaker Unified Studio. Per ulteriori informazioni, consulta [Configurazione dei IAM-based domini in SageMaker Unified Studio](#).
- Hai un SageMaker dominio e un progetto. Per ulteriori informazioni, consulta [Domains](#) nella SageMaker Unified Studio Administrator Guide e [Projects](#) nella SageMaker Unified Studio User Guide.

Se non hai già eseguito queste azioni o creato queste risorse, S3 Tables può completare automaticamente questa configurazione per te in modo da poter iniziare a eseguire query con Unified Studio. SageMaker

Guida introduttiva all'interrogazione di tabelle S3 con Unified Studio SageMaker

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nella pagina Bucket di tabelle, scegli il bucket contenente la tabella sui cui desideri eseguire la query.
4. Nella pagina dei dettagli del bucket, seleziona la tabella su cui desideri interrogare.
5. Seleziona Query.
6. Quindi, scegli Tabella delle interrogazioni in SageMaker Unified Studio.
 - a. Se hai già configurato SageMaker Unified Studio per le tue tabelle, la console di SageMaker Unified Studio si apre nell'editor di query con una query di esempio SELECT caricata per te. Modifica questa query in base alle esigenze del caso d'uso.
 - b. Se non hai già configurato SageMaker Unified Studio for S3 Tables, viene visualizzata una pagina di configurazione con un solo passaggio per abilitare l'integrazione con i servizi di AWS analisi, che integra le tue tabelle con servizi come Unified Studio. SageMaker Questo passaggio verrà eseguito automaticamente, quindi verrai reindirizzato a una pagina nella console SageMaker Unified Studio con le seguenti opzioni per configurare il tuo account per l'interrogazione di S3 Tables:

- i. In Configurazione come amministratore, viene selezionato il ruolo IAM federato corrente. Se il tuo ruolo attuale non dispone già delle autorizzazioni richieste, dovrai [configurare un IAM-based dominio in SageMaker Unified Studio](#) e assegnare le autorizzazioni al tuo ruolo in modo da poter accedere a Unified Studio. SageMaker
- ii. In Dati di progetto e controllo amministrativo, seleziona Auto-create un nuovo ruolo con le autorizzazioni richieste per creare automaticamente un ruolo con le autorizzazioni richieste oppure seleziona Usa un ruolo esistente e scegli un ruolo. Se il ruolo scelto non dispone già delle autorizzazioni richieste, dovrai [configurare un IAM-based dominio in SageMaker Unified Studio](#) e assegnare le autorizzazioni al tuo ruolo di amministratore di esecuzione in modo da poter accedere ai dati in Unified Studio. SageMaker
- iii. In Crittografia dei dati, seleziona Usa AWS la chiave AWS proprietaria per assegnare e gestire una chiave per te o Scegli una AWS AWS KMS chiave diversa (avanzata) per utilizzare una chiave esistente o per crearne una nuova.
- iv. Seleziona Configura SageMaker Unified Studio.
- v. Successivamente, la console di SageMaker Unified Studio si apre all'editor di query con una SELECT query di esempio caricata per te. Modifica questa query in base alle esigenze del caso d'uso.

Nell'editor di query, il campo Catalogo deve essere compilato con `s3tablescatalog/` seguito dal nome del bucket di tabella, ad esempio, `s3tablescatalog/amzn-s3-demo-table-bucket` Il campo Database viene compilato con lo spazio dei nomi in cui è archiviata la tabella.

Streaming di tabelle con Amazon MSK

Le tabelle di streaming sono Apache Iceberg tabelle nei bucket di tabelle su cui Amazon Managed Streaming for Apache Kafka (Amazon MSK) scrive continuamente. A differenza delle tabelle che crei e su cui scrivi direttamente, una tabella di streaming viene creata e popolata da Amazon MSK. I broker Amazon MSK Express forniscono i record di un Kafka argomento come file di Apache Parquet dati e li salvano nella tabella, rendendo i dati disponibili per l'interrogazione entro pochi minuti dalla produzione. Una singola tabella di streaming è scalabile fino a un throughput di consegna di Amazon MSK fino a 10 GBps senza scalabilità manuale.

Poiché Amazon MSK è il proprietario delle scritture, una tabella di streaming è di sola lettura. Hai pieno accesso in lettura da qualsiasi motore Iceberg compatibile e controlli la manutenzione delle tabelle e l'accesso in lettura allo stesso modo delle altre tabelle nel tuo table bucket.

Puoi creare una tabella di streaming configurando un canale di distribuzione Amazon MSK anziché chiamando `CreateTable`. Amazon MSK crea la tabella alla prima consegna. Per informazioni su come configurare il canale, inclusi l'argomento di origine, l'aggiornamento dei dati, la coda per le lettere morte e AWS Glue lo Schema Registry, consulta la distribuzione dei dati di [Amazon MSK](#) nella *Amazon Managed Streaming for Apache Kafka Developer Guide*.

Cosa puoi e cosa non puoi fare con le tabelle di streaming

Con una tabella di streaming, puoi fare quanto segue:

- Interroga la tabella con Amazon Athena, Amazon Redshift, Amazon EMR o qualsiasi altro motore di query Iceberg compatibile. Apache Spark
- Concedi l'accesso in lettura con policy AWS Identity and Access Management (IAM), policy table bucket e. AWS Lake Formation
- Configura i processi di manutenzione automatici di S3 Tables: compattazione, scadenza delle istantanee e rimozione dei file senza riferimenti.
- Configura la scadenza dei record nella colonna delle `timestamptz` partizioni per eliminare automaticamente i record più vecchi del periodo di conservazione specificato.
- Elimina la tabella con `DeleteTable`. Dopo aver eliminato la tabella, la consegna di Amazon MSK non riesce. Per riprendere la consegna, ricrea il canale Amazon MSK.

Con una tabella di streaming, non puoi fare quanto segue:

- Scrivi direttamente sulla tabella (`INSERT`, `UPDATEMERGE`, `COPY INTO`, o Iceberg scrive dai tuoi motori).
- Modificate lo schema, le specifiche di partizione, l'ordinamento o le proprietà della tabella.
- Elimina singole righe al di fuori del processo di scadenza del record.
- Riempi i record prodotti Kafka sull'argomento prima dell'attivazione del canale Amazon MSK.

Autorizzazioni per interrogare le tabelle di streaming

L'accesso in lettura a una tabella di streaming funziona come per qualsiasi altra tabella Amazon S3. Lo concedi con politiche IAM, policy table bucket e. AWS Lake Formation La seguente policy di

esempio consente di interrogare una tabella di streaming. Se la tabella è crittografata con una AWS KMS chiave, la seconda istruzione concede l'`kms:Decrypt` autorizzazione su tale chiave.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermissionsToQueryStreamingTables",
      "Effect": "Allow",
      "Action": [
        "s3tables:GetTable",
        "s3tables:GetTableData",
        "s3tables:GetTableMetadataLocation"
      ],
      "Resource": [
        "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket/
table/*"
      ]
    },
    {
      "Sid": "PermissionsToDecryptTableData",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/01234567-89ab-
cdef-0123-456789abcdef"
      ]
    }
  ]
}
```

Le autorizzazioni necessarie ad Amazon MSK per creare la tabella e scrivervi appartengono al ruolo del servizio Amazon MSK. Per queste autorizzazioni, consulta le autorizzazioni [IAM per la distribuzione dei dati Amazon MSK](#) nella Amazon Managed Streaming for Apache Kafka Developer Guide. Se il bucket di tabella si trova in un cluster Amazon MSK diverso, il proprietario del bucket deve allegare una policy sul bucket di tabella che Account AWS conceda al ruolo del servizio Amazon MSK le azioni necessarie. Per ulteriori informazioni, consulta [Gestione delle policy dei bucket di tabelle](#).

Lavorare con Apache Iceberg V3

Apache Iceberg Version 3 (V3) è l'ultima versione della specifica del formato tabellare Apache Iceberg, che introduce funzionalità avanzate per la creazione di data lake su scala petabyte con prestazioni migliorate e costi operativi ridotti. La V3 risolve i problemi di prestazioni più comuni riscontrati con la versione 2 (V2), in particolare per quanto riguarda gli aggiornamenti in batch e le eliminazioni della conformità.

AWS fornisce supporto per i vettori di eliminazione, la derivazione delle righe e il tipo di dati delle varianti come definito nella specifica Apache Iceberg Version 3 (V3). Puoi utilizzare queste funzionalità con Apache Spark su [Amazon EMR](#), Glue ETL, [Amazon SageMaker Unified Studio Notebooks e le tabelle Apache Iceberg in AWS Glue Data Catalog](#), [includere le tabelle](#) Amazon S3. [AWS https://aws.amazon.com/s3/features/tables/](#) Il tipo di dati della variante è specifico per le tabelle S3.

Caratteristiche principali di V3

Vettori di cancellazione

Sostituisce i file di eliminazione posizionale di V2 con un efficiente formato binario archiviato come file Puffin. Ciò elimina l'amplificazione della scrittura dovuta agli aggiornamenti in batch casuali e alle eliminazioni conformi al GDPR, riducendo in modo significativo il sovraccarico legato al mantenimento di dati aggiornati. Le organizzazioni che elaborano aggiornamenti ad alta frequenza vedranno miglioramenti immediati nelle prestazioni di scrittura e costi di archiviazione ridotti grazie a un minor numero di file di piccole dimensioni.

Row-lineage

Consente un monitoraggio preciso delle modifiche a livello di riga. I sistemi downstream possono elaborare le modifiche in modo incrementale, velocizzando le pipeline di dati e riducendo i costi di calcolo per i flussi di lavoro CDC (Change Data Capture). Questa funzionalità integrata elimina la necessità di implementazioni personalizzate per il monitoraggio delle modifiche.

Tipo di dati variante

Con il tipo di dati variante, puoi scrivere dati semistrutturati come JSON direttamente nelle tabelle Iceberg senza definire in anticipo uno schema fisso. I motori compatibili con V3 suddividono i dati semistrutturati in colonne nascoste mentre li scrivi, generando statistiche sulle colonne Parquet che i motori di query utilizzano per ottimizzazioni come l'eliminazione dei file. Ciò riduce i dati scansionati dalle query analitiche. S3 Tables fornisce una manutenzione continua delle tabelle per

le colonne delle varianti, inclusa la compattazione, in modo da poter consolidare i dati provenienti da fonti semistrutturate in file più grandi che i motori Iceberg possono leggere in modo efficiente.

Compatibilità delle versioni

La V3 mantiene la retrocompatibilità con le tabelle V2. AWS i servizi supportano contemporaneamente le tabelle V2 e V3, consentendoti di:

- Esegui query su entrambe le tabelle V2 e V3
- Aggiorna le tabelle V2 esistenti a V3 senza riscrittura dei dati
- Esegui query sui viaggi nel tempo che comprendono istantanee V2 e V3
- Usa l'evoluzione dello schema e il partizionamento nascosto tra le versioni delle tabelle

Important

La V3 è un aggiornamento unidirezionale. Una volta aggiornata una tabella da V2 a V3, non può essere ripristinata alla V2 tramite operazioni standard.

Guida introduttiva alla V3

Prerequisiti

Prima di lavorare con le tabelle V3, assicurati di avere:

- Un AWS account con le autorizzazioni IAM appropriate
- Accesso a uno o più servizi di AWS analisi (EMR, Glue, Amazon SageMaker Unified Studio Notebooks o S3 Tables)
- Un bucket S3 per l'archiviazione di dati e metadati delle tabelle
- Un table bucket per iniziare a usare S3 Tables o un bucket S3 generico se stai creando la tua infrastruttura Iceberg
- AWS Catalogo Glue configurato

Creazione di tabelle V3

Creazione di nuove tabelle V3

Per creare una nuova tabella Iceberg V3, imposta la proprietà `format-version table` su 3.

Usando Spark SQL:

```
CREATE TABLE IF NOT EXISTS myns.orders_v3 (  
  order_id bigint,  
  customer_id string,  
  order_date date,  
  total_amount decimal(10,2),  
  status string,  
  created_at timestamp  
)  
USING iceberg  
TBLPROPERTIES (  
  'format-version' = '3'  
)
```

Aggiornamento delle tabelle da V2 a V3

È possibile aggiornare le tabelle V2 esistenti alla V3 atomicamente senza riscrivere i dati.

Usando Spark SQL:

```
ALTER TABLE myns.existing_table  
SET TBLPROPERTIES ('format-version' = '3')
```

Important

La V3 è un aggiornamento unidirezionale. Una volta aggiornata una tabella da V2 a V3, non può essere ripristinata alla V2 tramite operazioni standard.

Cosa succede durante l'aggiornamento:

- Una nuova istantanea dei metadati viene creata atomicamente
- I file di dati Parquet esistenti vengono riutilizzati
- Row-lineage i campi vengono aggiunti ai metadati della tabella
- La prossima compattazione rimuoverà i vecchi file di eliminazione V2
- Le nuove modifiche utilizzeranno i file Deletion Vector di V3
- L'aggiornamento non esegue un backfill cronologico dei record di tracciamento delle modifiche alla derivazione delle righe

Abilitazione dei vettori di cancellazione

Per sfruttare i vettori di eliminazione per aggiornamenti, eliminazioni e fusioni, configura la modalità di scrittura.

Usare Spark SQL:

```
ALTER TABLE myns.orders_v3
SET TBLPROPERTIES ('format-version' = '3',
                  'write.delete.mode' = 'merge-on-read',
                  'write.update.mode' = 'merge-on-read',
                  'write.merge.mode' = 'merge-on-read'
                  )
```

Queste impostazioni assicurano che le operazioni di aggiornamento, eliminazione e unione creino file vettoriali di cancellazione invece di riscrivere interi file di dati.

Utilizzo Row-lineage del monitoraggio delle modifiche

V3 aggiunge automaticamente campi di metadati relativi alla derivazione delle righe per tenere traccia delle modifiche.

Usando Spark SQL:

```
# Query with parameter value provided
last_processed_sequence = 47
```

```
SELECT
    id,
    data,
    _row_id,
    _last_updated_sequence_number
FROM myns.orders_v3
WHERE _last_updated_sequence_number > :last_processed_sequence
```

Il campo `_row_id` identifica in modo univoco ogni riga, mentre `_last_updated_sequence_number` tiene traccia dell'ultima modifica della riga. Usa questi campi per:

- Identifica le righe modificate per l'elaborazione incrementale
- Tieni traccia della derivazione dei dati per la conformità
- Ottimizza le pipeline CDC
- Riduci i costi di elaborazione elaborando solo le modifiche

Utilizzo del tipo di dati della variante

Important

Il tipo di dati della variante è disponibile solo in AWS regioni specifiche. Per l'elenco completo delle regioni supportate, consulta [the section called “Disponibilità”](#).

Con il tipo di dati variante, puoi scrivere dati semistrutturati come JSON direttamente nelle tue tabelle Iceberg senza definire in anticipo uno schema fisso. È possibile scrivere dati più velocemente ottenendo allo stesso tempo prestazioni efficienti delle query analitiche. I motori compatibili con Iceberg V3 suddividono i dati semistrutturati in colonne nascoste mentre li scrivi. Queste colonne nascoste generano statistiche sulle colonne Parquet che i motori di query utilizzano per ottimizzazioni come l'eliminazione dei file.

Creazione di una tabella con una colonna variante utilizzando Spark SQL:

```
CREATE TABLE IF NOT EXISTS myns.events (
    event_id bigint,
    event_timestamp timestamp,
    source string,
```



```
    event_data VARIANT
  )
  USING iceberg
  TBLPROPERTIES (
    'format-version' = '3'
  )
```

Inserimento di dati semistrutturati nella colonna variante:

```
INSERT INTO myns.events VALUES (
  1,
  current_timestamp(),
  'web-app',
  PARSE_JSON('{ "user_id": "u-1234", "action": "page_view", "page": "/products",
    "duration_ms": 350 }')
);

INSERT INTO myns.events VALUES (
  2,
  current_timestamp(),
  'mobile-app',
  PARSE_JSON('{ "user_id": "u-5678", "action": "purchase", "items": [ { "sku": "A100",
    "qty": 2 } ], "total": 49.99 }')
);
```

Con S3 Tables, la manutenzione delle tabelle per le colonne delle varianti, inclusa la compattazione, viene eseguita automaticamente. La compattazione consolida i dati provenienti da fonti semistrutturate da file di piccole dimensioni in file più grandi che i motori Iceberg possono leggere in modo più efficiente, migliorando le prestazioni delle query nel tempo.

Le migliori pratiche per la versione V3

Quando usare V3

Prendi in considerazione l'aggiornamento o l'avvio con V3 quando:

- Si eseguono aggiornamenti o eliminazioni in batch frequenti
- Devi soddisfare i requisiti del GDPR o di conformità all'eliminazione

- I tuoi carichi di lavoro comportano interruzioni ad alta frequenza
- Sono necessari flussi di lavoro CDC efficienti
- Desiderate ridurre i costi di archiviazione dovuti a file di piccole dimensioni
- Hai bisogno di migliori funzionalità di tracciamento delle modifiche

Ottimizzazione delle prestazioni di scrittura

- Abilita i vettori di cancellazione per carichi di lavoro ad alto contenuto di aggiornamenti:

```
SET TBLPROPERTIES (  
  'write.delete.mode' = 'merge-on-read',  
  'write.update.mode' = 'merge-on-read',  
  'write.merge.mode' = 'merge-on-read'  
)
```

- Configura le dimensioni appropriate dei file:

```
SET TBLPROPERTIES (  
  'write.target-file-size-bytes' = '536870912' -- 512 MB  
)
```

Ottimizzazione delle prestazioni di lettura

- Sfrutta la derivazione delle righe per l'elaborazione incrementale
- Usa il viaggio nel tempo per accedere ai dati storici senza copiarli
- Abilita la raccolta di statistiche per una migliore pianificazione delle query

Strategia di migrazione

Durante la migrazione da V2 a V3:

- Esegui prima il test in modalità non di produzione: convalida del processo di aggiornamento e delle prestazioni

- Aggiornamento durante i periodi di bassa attività: riduzione al minimo dell'impatto sulle operazioni simultanee
- Monitoraggio delle prestazioni iniziali: monitoraggio delle metriche dopo l'aggiornamento
- Esegui la compattazione: consolida i file eliminati dopo l'aggiornamento
- Aggiorna la documentazione: riflette le funzionalità di V3 nella documentazione del team

Considerazioni sulla compatibilità

- Versioni del motore: assicurati che tutti i motori che accedono alla tabella supportino V3
- Third-party strumenti - Verifica la compatibilità con V3 prima dell'aggiornamento
- Strategia di backup: verifica le procedure di ripristino basate su istantanee
- Monitoraggio: aggiorna le dashboard di monitoraggio per le metriche V3-specific

Considerazioni sulla compattazione

Per impostazione predefinita, Compaction scrive file varianti di Parquet tritati. I lettori meno recenti che non supportano la distruzione potrebbero non riuscire a leggere i file compressi. È possibile disattivare la distruzione impostando la proprietà della tabella.

```
write.variant.shredding.enabled=false
```

Risoluzione dei problemi

Problemi comuni

Errore: «la versione del formato 3 non è supportata»

- Controlla il catalogo del tuo motore di ricerca per verificare la compatibilità con Iceberg V3.
- Assicurati di utilizzare le versioni più recenti del AWS servizio.
- Verifica che la versione del tuo motore supporti la versione V3

Il supporto V3 per i AWS servizi Amazon è il seguente:

Servizio	Supporto V3	Supporto per le varianti V3
EMR Spark	Versione 7.12+	Versione 8.0+

Servizio	Supporto V3	Supporto per le varianti V3
AWS Colla ETL	Sì	No
Notebook Amazon SageMaker Unified Studio	Sì	No
AWS Glue: API REST Iceberg, manutenzione delle tabelle	Sì	No
Tabelle Amazon S3: API REST Iceberg, manutenzi one delle tabelle	Sì	Sì*
Amazon Athena (Trino)	No	No

*Disponibilità parziale nella regione

Degrado delle prestazioni dopo l'aggiornamento

- Verificare che non vi siano errori di compattazione. Per maggiori dettagli, consulta [Registrazione e monitoraggio per le tabelle](#) S3.
- Controlla se i vettori di cancellazione sono abilitati. Assicuratevi che siano impostate le seguenti proprietà:

```
SET TBLPROPERTIES (  
  'write.delete.mode' = 'merge-on-read',  
  'write.update.mode' = 'merge-on-read',  
  'write.merge.mode' = 'merge-on-read'  
)
```

- È possibile verificare le proprietà della tabella con il codice seguente:

```
DESCRIBE FORMATTED myns.orders_v3
```

- Rivedi la strategia di partizione. Un partizionamento eccessivo può portare a file di piccole dimensioni. Esegui la seguente query per ottenere la dimensione media dei file per la tua tabella:

```
SELECT avg(file_size_in_bytes) as avg_file_size_bytes
FROM myns.orders_v3.files
```

Incompatibilità con strumenti di terze parti

- Lo strumento di verifica supporta le specifiche V3
- Valuta la possibilità di mantenere le tabelle V2 per gli strumenti non supportati
- Contatta il fornitore degli strumenti per la tempistica del supporto V3

Utilizzo della Guida

- AWS Assistenza: contatta l'assistenza per problemi specifici relativi AWS al servizio
- Comunità Apache Iceberg: Iceberg Slack
- AWS Documentazione: Documentazione analitica AWS

Prezzi

- Amazon EMR: prezzi di [elaborazione e storage](#)
- [Prezzi Amazon SageMaker](#)
- AWS Glue: [Job run e prezzi del Data Catalog](#)
- Tabelle S3: prezzi per l'[archiviazione e le richieste](#)

Disponibilità

Il supporto di Apache Iceberg V3 per i vettori di cancellazione e la derivazione delle righe è disponibile in tutte le AWS regioni in cui operano Amazon EMR, Glue Data Catalog, AWS AWS Glue ETL e S3 Tables.

Il tipo di dati variante in S3 Tables è disponibile nelle seguenti AWS regioni: Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Asia Pacifico

(Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Tokyo), Canada (Centrale), Europa (Francoforte), Europa (Irlanda), Europa (Londra), Europa (Parigi), Europa (Parigi), Europa (Francoforte), Europa (Irlanda), Europa (Londra), Europa (Parigi), Europa (Stoccolma) e Sud America (San Paolo).

Risorse aggiuntive

- [Documentazione di Apache Iceberg V3](#)
- [Best practice per la migrazione](#)
- [Guida alle operazioni di base](#)

Replica delle tabelle S3

Le tabelle Amazon S3 supportano la replica automatica delle tabelle Apache Iceberg archiviate nei bucket di tabelle Amazon S3. Le destinazioni di replica possono trovarsi all'interno della stessa AWS regione, su più AWS regioni, sullo stesso account o su altri account. AWS Configurando la replica per le tabelle, è possibile mantenere repliche di sola lettura dei dati in più sedi. È possibile utilizzare le repliche per migliorare la disponibilità dei dati, soddisfare i requisiti di conformità e aumentare le prestazioni di accesso per le applicazioni distribuite.

La replica di S3 Tables mantiene la coerenza dei dati inviando tutti gli aggiornamenti delle tabelle, inclusi snapshot, metadati e file di dati, nella tabella di destinazione nello stesso ordine della tabella di origine.

Quando utilizzare la replica di S3 Tables

È possibile utilizzare la replica di S3 Tables per i seguenti scopi:

- **Riduci al minimo la latenza:** se i tuoi clienti si trovano in due aree geografiche, puoi ridurre al minimo la latenza durante l'accesso alle tabelle mantenendo le repliche di lettura nelle AWS regioni geograficamente più vicine agli utenti.
- **Conformità normativa:** puoi mantenere le repliche di lettura in aree geografiche o AWS account specifici, il che potrebbe aiutarti a soddisfare determinati requisiti normativi o di conformità. È possibile configurare il bucket della tabella di destinazione della replica per crittografare le tabelle con chiavi AWS KMS diverse da quelle di origine.
- **Analisi centralizzata:** se i dati sono distribuiti in più AWS regioni, è possibile replicare i Region-specific set di dati in una regione centralizzata per la creazione di report unificati, l'analisi

interregionale e l'addestramento dei modelli di machine learning. Ciò elimina la necessità di eseguire query su più regioni o creare pipeline di aggregazione dei dati personalizzate.

- Ambienti di test e sviluppo: puoi creare repliche di lettura delle tabelle di produzione in bucket separati Account AWS o di tabelle per fornire dati di test realistici per i team di sviluppo e controllo qualità. Ciò isola i carichi di lavoro di test dai sistemi di produzione, garantendo al contempo che gli ambienti di test dispongano di dati attuali e simili a quelli di produzione senza esportazioni manuali o processi di sincronizzazione dei dati.

Funzionalità

La replica di S3 Tables offre le seguenti funzionalità.

Read-only repliche per tabelle S3

La replica di S3 Tables crea repliche di sola lettura delle tabelle Apache Iceberg su bucket di tabelle. Puoi interrogare le repliche in modo indipendente utilizzando qualsiasi motore. Iceberg-compatible

Repliche gestite automaticamente

Il servizio di replica S3 Tables mantiene automaticamente le tabelle di replica. La replica in genere aggiorna le repliche entro pochi minuti dagli aggiornamenti all'origine. S3 Tables esegue il commit di tutti gli aggiornamenti nello stesso ordine della tabella di origine per mantenere la coerenza.

Replica su più destinazioni

È possibile replicare la stessa tabella su più bucket di tabelle di destinazione. Le destinazioni di replica possono trovarsi all'interno dello stesso Regione AWS, su più account Regioni AWS, nello stesso AWS account o in altri account. AWS

Conservazione indipendente delle istantanee

La scadenza delle istantanee per le tabelle di replica è indipendente dalla tabella di origine e consente di impostare periodi di conservazione diversi sulle tabelle di replica, se necessario. Ad esempio, è possibile configurare la tabella di origine per conservare le istantanee per 30 giorni impostando un periodo di conservazione di 90 giorni per le tabelle di replica. Se si configura un periodo di conservazione più lungo sulle repliche, le istantanee che scadono all'origine rimangono disponibili e interrogabili nelle repliche. Questa configurazione offre funzionalità estese di viaggio nel tempo per l'analisi storica.

Mantieni le tabelle di replica in livelli di storage a basso costo

È possibile configurare i bucket della tabella di destinazione per utilizzare la classe di Intelligent-Tiering storage S3, che ottimizza automaticamente i costi di storage in base ai modelli di accesso senza impatto sulle prestazioni o sovraccarico operativo. S3 Intelligent-Tiering è adatto per tabelle di replica a cui è possibile accedere meno frequentemente.

Per ulteriori informazioni sulla replica delle tabelle S3, consulta i seguenti argomenti.

Argomenti

- [Come funziona la replica di S3 Tables](#)
- [Configurazione della replica delle tabelle S3](#)
- [Gestione della replica delle tabelle S3](#)

Come funziona la replica di S3 Tables

La replica di S3 Tables crea repliche in sola lettura delle tabelle Apache Iceberg tra regioni e Account AWS. Le tabelle di replica vengono gestite automaticamente dal servizio S3 Tables e contengono i dati completi, i metadati e la cronologia delle istantanee della tabella di origine, rendendole interrogabili utilizzando qualsiasi motore per analisi e operazioni di viaggio nel tempo. Iceberg-compatible

Quando si configura la replica per una tabella, S3 Tables:

- Crea una tabella di replica di sola lettura in ogni bucket della tabella di destinazione con lo stesso nome e namespace della tabella di origine.
- Riempie la replica con lo stato più recente della tabella di origine
- Monitora la tabella di origine per verificare la presenza di nuovi aggiornamenti
- Effettua il commit di tutti gli aggiornamenti nelle repliche nello stesso ordine dell'origine per mantenere la coerenza

Per ulteriori informazioni, consultare le sezioni indicate di seguito.

Argomenti

- [Cosa viene replicato](#)
- [Come vengono replicati i dati](#)
- [Replica istantanea](#)

- [Considerazioni e limitazioni](#)

Cosa viene replicato

Vengono replicati i seguenti componenti della tabella:

- **Istantanee della tabella:** tutte le istantanee, incluse le istantanee compatte, vengono replicate in ordine cronologico, mantenendo le relazioni padre-figlio e i numeri di sequenza della tabella di origine. Ciò garantisce che le tabelle di replica offrano le stesse funzionalità di viaggio nel tempo delle tabelle di origine.
- **Dati della tabella:** tutti i file di dati a cui fanno riferimento le istantanee della tabella vengono replicati nella regione di destinazione. Questo include:
 - **File di metadati:** file metadata.json della tabella, manifesti, elenchi di manifesti, statistiche delle partizioni e statistiche delle tabelle.
 - **Elimina file:** tutti i file eliminati vengono replicati per mantenere la precisione dei dati nelle tabelle di replica.
 - **File di dati:** tutti i file di dati a cui fanno riferimento i manifesti vengono replicati.
- **Metadati della tabella:** replica completa dei metadati, incluse le informazioni sullo schema (attuali e cronologiche), le specifiche delle partizioni, i criteri di ordinamento e le proprietà delle tabelle.
 - **Informazioni sullo schema:** tutti gli schemi delle tabelle vengono replicati, inclusi lo schema corrente e le versioni storiche dello schema. Ciò garantisce che le query sulle tabelle di replica utilizzino le definizioni di colonna, i tipi di dati e le mappature dei campi corretti. Il processo di replica mantiene la cronologia dell'evoluzione dello schema, consentendo alle query relative ai viaggi nel tempo di funzionare correttamente sulle tabelle di replica.
 - **Specifiche di partizione:** le specifiche di partizione attuali e storiche vengono replicate, garantendo che le tabelle di replica mantengano la stessa strategia di partizionamento delle tabelle di origine.
 - **Ordini di ordinamento:** gli ordinamenti delle tabelle vengono replicati per mantenere le ottimizzazioni delle prestazioni delle query.

Come vengono replicati i dati

La replica determina uno stato valido per le tabelle di replica confrontando i metadati delle tabelle Apache Iceberg tra le tabelle di origine e di replica. La replica elabora i metadati in tre categorie per aggiornare la tabella di replica.

Per i metadati delle tabelle

Per i campi di metadati con versione, la replica unisce i valori della tabella di origine negli array della tabella di replica per i seguenti campi:

- `snapshots`— Unisce tutte le istantanee dalla tabella di origine all'array di istantanee della tabella di replica per `snapshot-id`.
- `snapshot-log`— Unisce i log delle istantanee dalla tabella di origine all'array `snapshot-log` della tabella di replica, ordinati per timestamp e `snapshot-id`.
- `sort-orders`— Unisce le definizioni degli ordinamenti dalla tabella di origine all'array di ordinamenti della tabella di replica per `order-id`.
- `partition-specs`— Unisce le specifiche di partizione dalla tabella di origine all'array delle specifiche delle partizioni della tabella di replica per `spec-id`.
- `schemas`— Unisce le definizioni dello schema dalla tabella di origine all'array degli schemi della tabella di replica per `schema-id`.

Per la configurazione della tabella

Per i campi che rappresentano la configurazione della tabella, la replica copia i valori direttamente dalla tabella di origine:

- `properties`
- `partition-statistics`
- `statistics`

Lo stato corrente della tabella viene trasferito anche dalla tabella di origine:

- `current-snapshot-id`
- `current-schema-id`
- `last-column-id`
- `last-partition-id`
- `last-sequence-number`
- `default-sort-order-id`
- `next-row-id`(Iceberg V3)
- `encryption-keys`(Iceberg V3)

Replica-specific stato

I seguenti campi vengono calcolati dai dati uniti e aggiornati per la tabella di replica:

- `location` viene aggiornato durante la replica in modo che punti alla posizione corretta del file nel bucket della tabella di replica, assicurando che tutti i riferimenti ai file siano validi nell'ambiente di destinazione.
- `metadata-log` contiene tutti i nomi di file di metadati di destinazione e viene aggiornato dopo ogni replica riuscita con il nome di file di metadati corrente.
- Tutti i percorsi dei file vengono modificati in modo da puntare alle posizioni della tabella di replica.

Replica istantanea

La replica di S3 Tables mantiene la cronologia completa delle istantanee tra le regioni replicando tutte le istantanee delle tabelle nello stesso ordine di commit della tabella di origine. Le relazioni padre-figlio della tabella di origine vengono mantenute nella tabella di replica.

Conservazione degli snapshot

È possibile configurare un periodo di conservazione delle istantanee personalizzato per le tabelle replicate diverso dal periodo di conservazione dell'origine. Ciò significa che anche se le istantanee sono scadute e non sono più disponibili nella tabella di origine, possono essere conservate nelle repliche.

Ad esempio, se la tabella di origine ha un periodo di conservazione delle istantanee di 30 giorni ma la tabella di replica è configurata con un periodo di conservazione di 90 giorni, la replica manterrà le istantanee dei due mesi precedenti che non sono più disponibili nella tabella di origine.

Le istantanee scadute manualmente nella tabella di origine vengono conservate anche nella tabella di replica. Ad esempio, se hai fatto scadere le istantanee nella tabella di origine a partire da febbraio utilizzando una procedura Spark, puoi comunque viaggiare nel tempo fino alle istantanee nella tabella di replica.

Considerazioni e limitazioni

Le seguenti considerazioni si applicano alle tabelle replicate:

- S3 Tables replica le tabelle Iceberg V2 e V3. Tuttavia, la replica delle tabelle aggiornate (V2 → V3) non è supportata.

- I file di metadati di dimensioni superiori a 500 MB non sono supportati.
- Sebbene gli aggiornamenti delle tabelle vengano in genere replicati in pochi minuti, la replica può richiedere più tempo a seconda delle dimensioni dell'aggiornamento della tabella da replicare, ad esempio, quando la replica inizia il backfill.
- Le tabelle con tag o rami non sono supportate.
- La replica non è supportata per le tabelle di metadati di Amazon S3 o altre AWS tabelle di sistema generate.
- Tutte le istantanee delle tabelle, incluse le istantanee compatte, vengono replicate dalla tabella di origine. Di conseguenza, la compattazione non è supportata nelle tabelle di replica.

Configurazione della replica delle tabelle S3

È possibile configurare la replica per creare automaticamente repliche di tabella da una tabella di origine a un massimo di cinque bucket di tabella di destinazione. La replica può essere configurata a livello di bucket (applicabile a tutte le tabelle del bucket) o a livello di tabella (per tabelle specifiche). Questo argomento spiega come configurare la replica utilizzando la console Amazon S3 o l'interfaccia a riga di AWS comando (AWS CLI).

Per ulteriori informazioni sulla configurazione della replica, consulta i seguenti argomenti.

Argomenti

- [Prerequisiti per l'impostazione della replica](#)
- [Comprensione delle configurazioni di replica](#)
- [Scelta tra replica a livello di bucket e a livello di tabella](#)
- [Configurazione della replica utilizzando la console Amazon S3](#)
- [Impostazione della replica utilizzando AWS CLI](#)

Prerequisiti per l'impostazione della replica

Prima di configurare la replica, assicurati di disporre di quanto segue:

Risorse obbligatorie

- Bucket della tabella di origine: il bucket della tabella contenente le tabelle che desideri replicare
- Bucket della tabella di destinazione: uno o più bucket di tabelle in cui si desidera replicare le tabelle (fino a 5 bucket di tabella di destinazione)

- **Tabelle di origine:** tabelle esistenti nel bucket della tabella di origine da replicare
- **Ruolo/i IAM:** ruolo IAM che concede ad Amazon S3 le autorizzazioni per replicare le tabelle per tuo conto

Autorizzazioni richieste

L'identità IAM utilizzata per configurare la replica deve avere le seguenti autorizzazioni:

Per la replica a livello di bucket:

- `s3tables:PutTableBucketReplication` nel bucket della tabella di origine
- `s3tables:GetTableBucketReplication` nel bucket della tabella sorgente
- `iam:PassRole` per il ruolo IAM di replica

Per la replica a livello di tabella:

- `s3tables:PutTableReplication` nella tabella di origine
- `s3tables:GetTableReplication` nella tabella dei sorgenti
- `iam:PassRole` per il ruolo IAM di replica

Per la replica su più account:

- Autorizzazioni previste dalla policy del bucket dell'account di destinazione

Requisiti aggiuntivi per la replica su più account

Se i bucket della tabella di origine e di destinazione si trovano in AWS account diversi, è necessario anche:

- Una policy del bucket sul bucket della tabella di destinazione che conceda all'account di origine le autorizzazioni per replicare le tabelle
- L'ID dell'account di destinazione e il bucket di tabella Amazon Resource Name (ARN)

Requisiti aggiuntivi per le tabelle crittografate

Se desideri crittografare le tabelle di replica con AWS KMS:

- Una chiave KMS nella regione di destinazione
- Autorizzazioni per utilizzare la chiave KMS nel tuo ruolo di replica IAM
- Una politica chiave KMS che consente al ruolo di replica di crittografare i dati

Comprensione delle configurazioni di replica

Una configurazione di replica definisce il modo in cui Amazon S3 replica le tabelle dal bucket di tabelle di origine. La replica può essere configurata a due livelli:

Bucket-level replica

Una configurazione di replica a livello di bucket si applica a tutte le tabelle nel bucket della tabella di origine. Quando configuri la replica a livello di bucket, Amazon S3 replica automaticamente tutte le tabelle esistenti e tutte le nuove tabelle create nel bucket.

Usa la replica a livello di bucket quando:

- Vuoi replicare tutte le tabelle in un bucket
- Desideri un comportamento di replica coerente su tutte le tabelle
- Desideri semplificare la gestione disponendo di un'unica configurazione

Table-level replica

Una configurazione di replica a livello di tabella si applica a una tabella specifica. Table-levelle configurazioni sostituiscono le configurazioni a livello di bucket per quella tabella specifica.

Utilizza la replica a livello di tabella quando:

- Vuoi replicare solo tabelle specifiche
- Sono necessarie destinazioni di replica diverse per tabelle diverse
- Vuoi sovrascrivere una configurazione a livello di bucket per determinate tabelle

Elementi di configurazione della replica

Ogni configurazione di replica contiene:

- Ruolo IAM: il ruolo che Amazon S3 assume per eseguire le operazioni di replica
- Regole: una o più regole di replica (limitate a 1 regola all'avvio). Ogni regola contiene:

- Destinazioni: elenco dei bucket ARN della tabella di destinazione (fino a 5 destinazioni)
- Stato: se la regola è abilitata o disattivata
- Token di versione: un token utilizzato per prevenire conflitti di scrittura durante l'aggiornamento delle configurazioni

Scelta tra replica a livello di bucket e a livello di tabella

Precedenza di configurazione

Quando esistono configurazioni a livello di bucket e a livello di tabella:

- Table-level la configurazione ha la precedenza per quella tabella specifica.
- Le altre tabelle seguono la configurazione a livello di bucket.

Configurazione della replica utilizzando la console Amazon S3

Questa procedura mostra come configurare la replica utilizzando la console Amazon S3.

Per configurare la replica a livello di bucket

Questa procedura mostra come creare una configurazione di replica con bucket di tabelle utilizzando la console Amazon S3. Una configurazione di replica con bucket di tabelle si applica a tutte le tabelle del bucket di tabella di origine.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione, scegli **Table buckets**.
3. Nell'elenco dei bucket di tabella, scegli il nome del bucket di tabella per il quale desideri configurare la replica.
4. Scegliere la scheda **Management (Gestione)**,
5. Nella sezione **Configurazione della replica del bucket della tabella**, scegli **Crea la configurazione della replica del bucket della tabella**.
6. Nella sezione **Destinazione**, configura le destinazioni di replica:
 - a. Nel campo **Table bucket ARN**, inserisci l'ARN del bucket della tabella di destinazione. Il formato è: `arn:aws:s3tables:region:account-id:bucket/table-bucket-name`.

In alternativa, scegli **Browse S3** per selezionare un table bucket dal tuo account.

- b. (Facoltativo) Per aggiungere altre destinazioni, scegli **Aggiungi destinazione**. Puoi aggiungere fino a 4 tabelle aggiuntive per un totale di 5 destinazioni.
7. Nella sezione del ruolo **IAM**, configura il ruolo di replica:
 - a. Per il metodo di selezione del ruolo **IAM**, scegli una delle seguenti opzioni:
 - Crea un nuovo ruolo IAM: Amazon S3 crea un nuovo ruolo con le autorizzazioni necessarie per la replica.
 - Scegli tra i ruoli IAM esistenti: seleziona un ruolo esistente con le autorizzazioni di replica richieste.
 - Inserisci l'ARN del ruolo IAM: inserisci manualmente l'ARN di un ruolo IAM esistente.
 - b. Se hai scelto **Scegli tra i ruoli IAM esistenti**, seleziona un ruolo dall'elenco a discesa dei ruoli **IAM**.
 - c. (Facoltativo) Scegli **Visualizza** per esaminare le autorizzazioni del ruolo selezionato nella console IAM.
8. Scegli **Crea configurazione di replica**.

Dopo aver creato la configurazione di replica, Amazon S3 avvia il processo di backfill iniziale. Puoi monitorare lo stato della replica nella sezione **Tabella dello stato della replica**, che mostra le informazioni su ciascuna destinazione, tra cui lo stato della replica, l'ARN della tabella di destinazione e gli ultimi metadati replicati.

Per configurare la replica a livello di tabella

Questa procedura mostra come creare una configurazione di replica a livello di tabella utilizzando la console Amazon S3. Una configurazione di replica di tabella si applica a una tabella specifica e sostituisce qualsiasi configurazione di replica a livello di bucket per quella tabella.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione, scegli **Table buckets**.
3. Nell'elenco dei bucket di tabella, scegli il nome del bucket di tabella che contiene la tabella che desideri replicare.
4. Scegliere la scheda **Tabelle**.

5. Nell'elenco **Tabelle**, scegli il nome della tabella che desideri replicare.
6. Scegliere la scheda **Management (Gestione)**,
7. Nella sezione **Configurazione della replica delle tabelle**, scegli **Crea configurazione di replica delle tabelle**.
8. Nella sezione **Destinazione**, configura le destinazioni di replica:
 - a. Nel campo **Table bucket ARN**, inserisci l'ARN del bucket della tabella di destinazione. Il formato è: `arn:aws:s3tables:region:account-id:bucket/table-bucket-name`.

In alternativa, scegli **Browse S3** per selezionare un table bucket dal tuo account.
 - b. (Facoltativo) Per aggiungere altre destinazioni, scegli **Aggiungi destinazione**. Puoi aggiungere fino a 4 tabelle aggiuntive per un totale di 5 destinazioni.
9. Nella sezione del ruolo **IAM**, configura il ruolo di replica:
 - a. Per il metodo di selezione del ruolo **IAM**, scegli una delle seguenti opzioni:
 - Crea un nuovo ruolo IAM: Amazon S3 crea un nuovo ruolo con le autorizzazioni necessarie per la replica.
 - Scegli tra i ruoli IAM esistenti: seleziona un ruolo esistente con le autorizzazioni di replica richieste.
 - Inserisci l'ARN del ruolo IAM: inserisci manualmente l'ARN di un ruolo IAM esistente.
 - b. Se hai scelto **Scegli tra i ruoli IAM esistenti**, seleziona un ruolo dall'elenco dei ruoli **IAM**.
 - c. (Facoltativo) Scegli **Visualizza** per esaminare le autorizzazioni del ruolo selezionato nella console IAM.
10. Scegli **Crea configurazione di replica**.

Cosa succede dopo?

Dopo aver creato la configurazione di replica:

- Amazon S3 avvia il processo di backfill iniziale, creando tabelle di replica in ogni bucket di destinazione
- Lo stato di replica cambia in **Replicating** una volta iniziato il backfill
- È possibile monitorare l'avanzamento della replica nella scheda **Gestione**
- Il tempo di replica iniziale dipende dalle dimensioni della tabella di origine

Impostazione della replica utilizzando AWS CLI

Questa procedura mostra come configurare la replica utilizzando AWS CLI. Sostituisci gli ID degli account, le aree e i nomi dei bucket con i tuoi valori effettivi. Aggiungi tutti i bucket di destinazione alle autorizzazioni.

Passaggio 1: creare un ruolo IAM per la replica

Innanzitutto, crea un ruolo IAM che Amazon S3 possa assumere per replicare le tue tabelle.

1. Crea un documento sulla politica di fiducia che consenta a S3 Tables di assumere il ruolo. Salvalo come: `trust-policy.json`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "replication.s3tables.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Crea il ruolo IAM:

```
aws iam create-role \
  --role-name S3TablesReplicationRole \
  --assume-role-policy-document file://trust-policy.json \
  --description "Role for S3 Tables replication"
```

3. Crea una policy di autorizzazione che conceda le autorizzazioni di replica. Salvalo con nome: `replication-permissions.json`

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3tables:GetTable",
      "s3tables:GetTableMetadataLocation",
      "s3tables:GetTableMaintenanceConfiguration",
      "s3tables:GetTableData"
    ],
    "Resource": "arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-  
demo-table-bucket-source/table/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3tables:ListTables"
    ],
    "Resource": "arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-  
demo-table-bucket-source"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3tables:CreateTable",
      "s3tables:CreateNamespace"
    ],
    "Resource": "arn:aws:s3tables:us-east-2:444455556666:bucket/amzn-s3-  
demo-table-bucket-destination"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3tables:PutTableData",
      "s3tables:GetTableData",
      "s3tables:UpdateTableMetadataLocation",
      "s3tables:PutTableMaintenanceConfiguration"
    ],
    "Resource": "arn:aws:s3tables:us-east-2:444455556666:bucket/amzn-s3-  
demo-table-bucket-destination/table/*"
  }
]
}

```

4. Allega la politica delle autorizzazioni al ruolo:

```
aws iam put-role-policy \  
  --role-name S3TablesReplicationRole \  
  --policy-name S3TablesReplicationPermissions \  
  --policy-document file://replication-permissions.json
```

Note

La politica delle autorizzazioni utilizza due ambiti di risorse perché le azioni operano a livelli diversi. CreateTable e CreateNamespace sono operazioni a livello di bucket che creano risorse nel bucket, quindi utilizzano il bucket ARN senza. `/table/*` PutTableData, GetTableDataUpdateTableMetadataLocation, e PutTableMaintenanceConfiguration operano su tabelle esistenti, quindi utilizzano il bucket ARN con. `/table/*`

5. (Facoltativo) Se utilizzi la crittografia KMS, aggiungi le autorizzazioni KMS alla tua policy:

```
{  
  "Effect": "Allow",  
  "Action": [  
    "kms:Decrypt",  
    "kms:GenerateDataKey",  
    "kms:Encrypt"  
  ],  
  "Resource": "arn:aws:kms:us-east-1:111122223333:key/SOURCE-KEY-ID"  
},  
{  
  "Effect": "Allow",  
  "Action": [  
    "kms:Decrypt",  
    "kms:GenerateDataKey"  
  ],  
  "Resource": [  
    "arn:aws:kms:us-west-2:444455556666:key/DESTINATION-KEY-ID-1"
```

```
]
}
```

(Cross-account solo) Fase 2: Configurazione della policy del bucket di destinazione

Se si esegue la replica su un AWS account diverso, l'account di destinazione deve concedere le autorizzazioni all'account di origine.

1. Nell'account di destinazione, crea una policy bucket per il bucket della tabella di destinazione. Salva questo come: `destination-bucket-policy.json`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/S3TablesReplicationRole"
      },
      "Action": [
        "s3tables:PutTableData",
        "s3tables:GetTableData",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:PutTableMaintenanceConfiguration"
      ],
      "Resource": "arn:aws:s3tables:us-east-2:444455556666:bucket/amzn-s3-demo-table-bucket-cross-account-destination/table/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/S3TablesReplicationRole"
      },
      "Action": [
        "s3tables:CreateTable",
        "s3tables:CreateNamespace"
      ],
      "Resource": "arn:aws:s3tables:us-east-2:444455556666:bucket/amzn-s3-demo-table-bucket-cross-account-destination"
    }
  ]
}
```

```
]
}
```

2. Applica la policy utilizzando l'API S3 Tables:

```
aws s3tables put-table-bucket-policy \
  --table-bucket-arn arn:aws:s3tables:us-west-2:444455556666:bucket/amzn-s3-demo-
  table-bucket-cross-account-destination \
  --resource-policy file://destination-bucket-policy.json \
  --profile destination-account
```

3. Modifica la chiave KMS di origine per consentire la replica e la manutenzione di S3 Tables:

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "allow replication to decrypt",
      "Effect": "Allow",
      "Principal": {
        "AWS": "replication_role_arn"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/SOURCE-KEY-ID"
    },
    {
      "Sid": "allow maintenance",
      "Effect": "Allow",
      "Principal": {
        "Service": "maintenance.s3tables.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/SOURCE-KEY-ID"
    }
  ]
}
```

```
    }
  ]
}
```

4. Allo stesso modo, aggiungi le autorizzazioni nella policy chiave del KMS di destinazione

```
{
  "Version": "2012-10-17",
  "Id": "key-policy-3",
  "Statement": [
    {
      "Sid": "allow maintenance",
      "Effect": "Allow",
      "Principal": {
        "Service": "maintenance.s3tables.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-west-2:444455556666:key/DESTINATION-KEY-
ID-1"
    },
    {
      "Sid": "allow replication to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "AWS": "replication_role_arn"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-west-2:444455556666:key/DESTINATION-KEY-
ID-1"
    }
  ]
}
```

Fase 3: Creare una configurazione di replica

È possibile utilizzare il AWS CLI per creare una configurazione di replica a livello di bucket o di tabella. Per ulteriori informazioni, consultare le procedure seguenti.

Crea una configurazione di replica a livello di bucket

Usa questo approccio per replicare tutte le tabelle in un bucket.

1. Crea un file di configurazione della replica. Salvalo con nome: `bucket-replication-config.json`

Example: Un'unica destinazione nello stesso account

```
{
  "role": "arn:aws:iam::111122223333:role/S3TablesReplicationRole",
  "rules": [
    {
      "destinations": [
        {
          "destinationTableBucketARN": "arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-bucket-dr"
        }
      ]
    }
  ]
}
```

Example: Diverse destinazioni in tutte le regioni

```
{
  "role": "arn:aws:iam::111122223333:role/S3TablesReplicationRole",
  "rules": [
    {
      "destinations": [
        {
          "destinationTableBucketARN": "arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-bucket-dr"
        },
        {

```



```

        "destinationTableBucketARN": "arn:aws:s3tables:eu-
west-1:111122223333:bucket/amzn-s3-demo-table-bucket-eu"
    },
    {
        "destinationTableBucketARN": "arn:aws:s3tables:ap-
south-1:111122223333:bucket/amzn-s3-demo-table-bucket-apac"
    }
]
}
]
}

```

Example: Cross-account replica

```

{
  "role": "arn:aws:iam::111122223333:role/S3TablesReplicationRole",
  "rules": [
    {
      "destinations": [
        {
          "destinationTableBucketARN": "arn:aws:s3tables:us-
east-1:444455556666:bucket/amzn-s3-demo-table-bucket-partner"
        }
      ]
    }
  ]
}

```

2. Applica la configurazione di replica a livello di bucket:

```

aws s3tables put-table-bucket-replication \
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
  --configuration file://bucket-replication-config.json

```

Output previsto:

```
{
  "versionToken": "3HL4kqtJl40Nr8X8gdRQBpUMLUo",
  "status": "Success"
}
```

Crea una configurazione di replica a livello di tabella

Utilizza questo approccio per replicare tabelle specifiche o per sovrascrivere la replica a livello di bucket.

1. Crea un file di configurazione della replica. Salvalo con nome: `table-replication-config.json`

Example: Replica su una singola tabella

```
{
  "role": "arn:aws:iam::<111122223333>:role/S3TablesReplicationRole",
  "rules": [
    {
      "destinations": [
        {
          "destinationTableBucketARN": "arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-table-bucket-analytics-bucket"
        }
      ]
    }
  ]
}
```

Example: Tabella con più destinazioni

```
{
  "role": "arn:aws:iam::<111122223333>:role/S3TablesReplicationRole",
  "rules": [
    {
```

```

    "destinations": [
      {
        "destinationTableBucketARN": "arn:aws:s3tables:us-
west-2:111122223333:bucket/amzn-s3-demo-table-bucket-dr"
      },
      {
        "destinationTableBucketARN": "arn:aws:s3tables:eu-
west-1:111122223333:bucket/amzn-s3-demo-table-bucket-eu"
      }
    ]
  }
]
}

```

2. Applica la configurazione di replica a livello di tabella:

```

aws s3tables put-table-replication \
  --table-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-
bucket/table/amzn-s3-demo-table-bucket-sales-data \
  --configuration file://table-replication-config.json

```

Output previsto:

```

{
  "versionToken": "xT2LZkFZ0UuTC2h8XqtGLx2Ak6M",
  "status": "Success"
}

```

Gestione della replica delle tabelle S3

Dopo aver configurato la replica di S3 Tables, puoi monitorare lo stato della replica per verificare cosa viene replicato. Puoi controllare lo stato della replica nella console Amazon S3 nella scheda Gestione della tabella di origine o utilizzando AWS CLI. Per ulteriori informazioni, consulta [Configurazione della replica delle tabelle S3](#). Questo argomento spiega come monitorare la replica e comprendere i diversi valori di stato che indicano se la replica è completata, in corso o non è riuscita.

Monitoraggio dello stato di replica

I processi di replica vengono eseguiti continuamente per le tabelle replicate. Puoi interrogare lo stato della replica con l' `GetTableReplicationStatus` API o visualizzarlo nella console Amazon S3.

Per ottenere lo stato della replica utilizzando AWS CLI

L'esempio seguente ottiene lo stato della replica utilizzando l' `GetTableReplicationStatusAPI`.

```
aws s3tables get-table-replication-status \  
  --table-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-  
bucket/table/sales-data
```

Output previsto:

```
{  
  "sourceTableARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-  
bucket/table/sales-data",  
  "destinations": [  
    {  
      "replicationStatus": "COMPLETED",  
      "destinationBucketARN": "arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-  
demo-table-bucket",  
      "destinationTableARN": "arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-  
demo-table-bucket/table/sales-data",  
      "lastSuccessfulReplicatedUpdate": {  
        "metadataLocation": "latest_table_metadata.json",  
        "timestamp": "2025-11-15T14:30:00Z"  
      }  
    },  
    {  
      "replicationStatus": "PENDING",  
      "destinationBucketARN": "arn:aws:s3tables:eu-west-1:111122223333:bucket/amzn-s3-  
demo-table-bucket-eu-bucket",  
      "destinationTableARN": "arn:aws:s3tables:eu-west-1:111122223333:bucket/amzn-s3-  
demo-table-bucket-eu-bucket/table/sales-data",  
      "lastSuccessfulReplicatedUpdate": {  
        "metadataLocation": "latest_table_metadata.json",  
        "timestamp": "2025-11-15T14:25:00Z"  
      }  
    }  
  ]  
}
```

```
    }  
  }  
]  
}
```

Per ulteriori informazioni, vedere [get-table-replication-status](#) nel Command Reference. AWS CLI

L'esempio seguente mostra una destinazione con lo stato FAILED, che include un campo: `failureMessage`

```
{  
  "replicationStatus": "FAILED",  
  "destinationBucketARN": "arn:aws:s3tables:eu-west-1:444455556666:bucket/amzn-s3-demo-table-bucket-partner",  
  "destinationTableARN": "arn:aws:s3tables:eu-west-1:444455556666:bucket/amzn-s3-demo-table-bucket-partner/table/sales-data",  
  "failureMessage": "Insufficient permissions given to successfully complete replication."  
}
```

Note

Il `get-table-replication` comando restituisce la configurazione della replica (ruolo, regole e destinazioni). Il `get-table-replication-status` comando restituisce lo stato della replica (COMPLETED, PENDING o FAILED), gli ultimi metadati replicati e i messaggi di errore.

Comprensione della risposta

La risposta contiene i seguenti elementi:

- `SourceTableARN`: l'ARN della tabella sorgente da replicare.
- `destinazioni`: una serie di oggetti di stato di destinazione, uno per ogni destinazione di replica configurata. Ogni oggetto di destinazione contiene:
 - `ReplicationStatus`: lo stato di replica corrente per questa destinazione (COMPLETATO, IN SOSPESO o FALLITO).

- `destinationBucketArn` — L'ARN del bucket della tabella di destinazione.
- `destinationTabLearn` — L'ARN della tabella di replica nel bucket di destinazione.
- `last SuccessfulReplicatedUpdate` — Informazioni sulla replica riuscita più recente:
 - `MetadataLocation`: il nome del file di metadati Iceberg che è stato replicato con successo l'ultima volta. Confrontalo con l'attuale posizione dei metadati della tabella di origine per determinare se la replica è aggiornata.
 - `timestamp`: l'ora in cui questo file di metadati è stato replicato nella destinazione.
- `failureMessage` (presente solo quando lo stato è FAILED): un messaggio di errore dettagliato che descrive il motivo per cui la replica non è riuscita.

Valori dello stato della replica

La replica può avere tre stati possibili per ciascuna destinazione:

- **COMPLETATO**: tutte le istantanee della tabella di origine sono state replicate correttamente nella destinazione. L'ultima posizione dei metadati della tabella di origine corrisponde all'ultima posizione dei metadati replicati.
- **IN SOSPESO**: la replica è in corso o nuovi commit sono in attesa di essere replicati. L'ultima posizione dei metadati della tabella di origine è diversa dall'ultima posizione dei metadati replicati.
- **FALLITO**: l'ultimo processo di replica per questa tabella non è riuscito. Nessun nuovo aggiornamento viene replicato.

Se una destinazione mostra lo stato NON RIUSCITO, controlla il `failureMessage` campo per i dettagli. Le cause più comuni includono autorizzazioni insufficienti, bucket di destinazione non trovato o problemi chiave del KMS. Dopo aver risolto la causa principale, il servizio riprova automaticamente la replica. È possibile monitorare il ripristino man mano che lo stato passa da FALLITO a IN SOSPESO a COMPLETATO.

Tabelle S3 Regioni AWS, endpoint e quote di servizio

Le seguenti sezioni includono le quote supportate Regioni AWS e di servizio per le tabelle S3.

Argomenti

- [Tabelle S3 Regioni AWS ed endpoint](#)
- [Quote di Tabelle S3](#)

Tabelle S3 Regioni AWS ed endpoint

Per un elenco delle Regioni in cui Tabelle S3 è attualmente disponibile, consulta [Endpoint di Amazon S3](#). Per connettersi a livello di codice a un AWS servizio, si utilizza un endpoint. Per ulteriori informazioni, consulta [Endpoint del servizio AWS](#).

S3 Tables supporta endpoint dual-stack per l'accesso pubblico e. AWS PrivateLink Dual-stack gli endpoint consentono di accedere ai bucket di tabelle S3 utilizzando il protocollo Internet versione 6 (IPv6), oltre al protocollo IPv4, a seconda di ciò che supporta la rete.

Gli endpoint dual-stack di Tabelle S3 utilizzano la seguente convenzione di denominazione:
`s3tables.aws-region.api.aws`

Per un elenco completo degli endpoint di Tabelle S3, consulta [Endpoint di Amazon S3](#).

Quote di Tabelle S3

Le quote, chiamate anche limiti, rappresentano il numero massimo di risorse o di operazioni di servizio consentite per il tuo Account AWS. Di seguito sono riportate le quote per le risorse di Tabelle S3. Per ulteriori informazioni sulle quote di Amazon S3, consulta [Quote di Amazon S3](#).

Nome	Predefinita	Adattabile	Description
Bucket di tabelle	10	Per richiedere un aumento delle quote, contattare Supporto .	Il numero di bucket di tabelle Amazon S3 che puoi creare in un account. Regione AWS
Spazi dei nomi	10.000	Per richiedere un aumento delle quote, contattare Supporto .	Il numero di spazi dei nomi delle tabelle Amazon S3 che è possibile creare per bucket di tabelle.
Tabelle	10.000	Per richiedere un aumento delle quote, contattare Supporto .	Il numero di tabelle Amazon S3 che è

Nome	Predefinita	Adattabile	Description
			possibile creare per bucket di tabelle.

Esecuzione di richieste a Tabelle S3 su IPv6

Amazon S3 supporta la possibilità di accedere ai bucket S3 utilizzando il protocollo Internet versione 6 (IPv6), oltre al protocollo IPv4, utilizzando endpoint dual-stack. Dual-stack gli endpoint si risolvono in un endpoint IPv6 o IPv4 a seconda di ciò che supporta la rete.

Di seguito sono riportati alcuni aspetti da prendere in considerazione prima di tentare di accedere a Tabelle S3 tramite protocollo IPv6:

- Il client e la rete che eseguono l'accesso al bucket di tabelle devono essere abilitati per l'uso del protocollo IPv6.
- Il client delle tabelle e il client S3 devono essere entrambi abilitati per il dual-stack.
- Se utilizzi policy IAM di filtraggio degli indirizzi IP, queste devono essere aggiornate per gestire gli indirizzi IPv6. Per ulteriori informazioni sulla gestione delle autorizzazioni di accesso con IAM, consulta [the section called "Identity and Access Management \(IAM\)"](#).
- Quando si utilizza IPv6, i file di log degli accessi al server generano indirizzi IP in un formato IPv6. È necessario aggiornare il software, gli script e gli strumenti esistenti utilizzati per analizzare i file di log di Amazon S3; affinché possano analizzare gli indirizzi Remote IP in formato IPv6. Per ulteriori informazioni, consulta [the section called "Registrazione dell'accesso al server"](#).

Nozioni di base sull'esecuzione di richieste di Tabelle S3 su IPv6

Quando effettui una richiesta a un endpoint dual-stack, l'URL del bucket di tabelle si risolve in un indirizzo IPv6 o IPv4, a seconda di ciò che supporta la rete. Se la rete preferisce il protocollo IPv4, le richieste utilizzeranno automaticamente l'IPv4. Se la rete preferisce il protocollo IPv6, le richieste utilizzeranno l'IPv6. Non è richiesta alcuna modifica alla configurazione oltre all'aggiornamento del client o dell'applicazione per abilitare l'endpoint dual-stack.

Quando si utilizza l'API REST, è possibile accedere direttamente a un endpoint Amazon S3 utilizzando il nome dell'endpoint (URI). Puoi accedere a Tabelle S3 e ai bucket di tabelle tramite un endpoint dual-stack utilizzando la seguente convenzione di denominazione:

s3tables.<region>.api.aws

Per un elenco completo degli endpoint per Tabelle S3, consulta [Endpoint e quote di Amazon Simple Storage Service](#).

Quando si utilizzano i client AWS CLI, AWS SDK e Iceberg, è possibile utilizzare un parametro o un flag per passare a un endpoint dual-stack. È inoltre possibile specificare l'endpoint dual-stack direttamente come sostituzione dell'endpoint Amazon S3 nel file di configurazione.

Puoi abilitare la risoluzione degli endpoint dual-stack nei kit SDK o nei client impostando il flag dual-stack tramite il seguente comando:

```
S3TablesClient client = S3TablesClient.builder()
    .region(Region.US_EAST_1)
    .dualstackEnabled(true)
    .build();
```

Per utilizzare l'endpoint dual-stack in, vedi Utilizzo degli endpoint dual-stack di AWS CLI. [AWS CLI](#)

Per informazioni sull'utilizzo degli endpoint dual-stack per, vedere,. AWS PrivateLink [Uso degli endpoint dual-stack per accedere a tabelle e bucket di tabelle](#)

Sicurezza per Tabelle S3

Amazon S3 offre una varietà di funzionalità e strumenti di sicurezza. Di seguito è riportato un elenco degli strumenti e delle funzionalità di sicurezza supportati dalle tabelle S3. Una corretta applicazione di questi strumenti può contribuire a garantire che le risorse siano protette e accessibili agli utenti interessati.

Identity-based politiche

[Identity-based policy](#) sono associate a un utente, gruppo o ruolo IAM. È possibile utilizzare le policy basate su identità per concedere a un'identità IAM l'accesso ai bucket di tabelle o alle tabelle. Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare e modificare tabelle e bucket di tabelle. Inoltre, non possono eseguire attività utilizzando la console S3 o le API AWS CLI REST di Amazon S3. È possibile creare utenti, gruppi e ruoli IAM nel proprio account e associare ad essi le policy di accesso. Quindi è possibile concedere o negare l'accesso alle risorse. Per creare e accedere a bucket e tabelle di tabelle, un amministratore

IAM deve concedere le autorizzazioni necessarie al ruolo o agli utenti AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta [Access management for S3 Tables](#).

Resource-based politiche

[Resource-based le politiche](#) sono collegate a una risorsa. È possibile creare policy basate su risorse per tabelle e bucket di tabelle. È possibile utilizzare una policy del bucket delle tabelle per controllare le autorizzazioni di accesso alle API a livello di bucket di tabelle e spazio dei nomi. Inoltre una policy del bucket di tabelle può essere utilizzata per controllare le autorizzazioni API a livello di tabella su più tabelle in un bucket. A seconda della definizione della policy, le autorizzazioni associate al bucket possono essere applicate a tutte le tabelle del bucket o solo ad alcune di esse. È anche possibile utilizzare una policy di tabella per concedere le autorizzazioni di accesso API a livello di tabella alle singole tabelle del bucket.

Quando riceve una richiesta per eseguire un'operazione su un bucket di tabelle o su una tabella, Tabelle S3 verifica innanzitutto che il richiedente disponga delle autorizzazioni necessarie. Valuta quindi tutte le policy di accesso, le policy utente e le policy basate sulle risorse pertinenti per decidere se autorizzare la richiesta (la policy dell'utente IAM, la policy del ruolo IAM, la policy del bucket di tabelle e la policy della tabella). Con le policy dei bucket e le policy delle tabelle, è possibile personalizzare l'accesso alle risorse per garantire che solo le identità approvate possano accedere alle risorse ed eseguire azioni su di esse. Per ulteriori informazioni, consulta [Access management for S3 Tables](#).

AWS Organizations politiche di controllo dei servizi (SCP) per le tabelle S3.

È possibile utilizzare Tabelle Amazon S3 nelle policy di controllo dei servizi per gestire le autorizzazioni per gli utenti dell'organizzazione. Analogamente alle policy IAM e alle policy relative alle risorse, nelle policy viene fatto riferimento a tutte le azioni a livello di tabella e di bucket come parte del namespace `s3tables`. Per ulteriori informazioni, consulta [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .

Argomenti

- [Protezione dei dati delle tabelle S3 con la crittografia](#)
- [Gestione degli accessi per Tabelle S3](#)
- [Connettività VPC per Tabelle S3](#)
- [Considerazioni e limitazioni sulla sicurezza per Tabelle S3](#)

Protezione dei dati delle tabelle S3 con la crittografia

Utilizzo della crittografia lato server con AWS KMS keys (SSE-KMS) nei bucket delle tabelle

Argomenti

- [Come SSE-KMS funziona per le tabelle e i bucket da tavolo](#)
- [Applicazione e definizione dell'ambito di SSE-KMS utilizzo per tabelle e bucket di tabelle](#)
- [Monitoraggio e controllo della SSE-KMS crittografia per tabelle e bucket di tabelle](#)
- [Requisiti di autorizzazione per la crittografia delle tabelle S3 SSE-KMS](#)
- [Specificare la crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket di tabelle](#)

I table bucket hanno una configurazione di crittografia predefinita che crittografa automaticamente le tabelle utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Questa crittografia si applica a tutte le tabelle nei bucket di tabelle S3 e non comporta costi aggiuntivi.

Se hai bisogno di un maggiore controllo sulle chiavi di crittografia, ad esempio gestendo la rotazione delle chiavi e la concessione delle policy di accesso, puoi configurare i bucket di tabelle in modo che utilizzino la crittografia lato server con () keys (). AWS Key Management Service AWS KMS SSE-KMS I controlli di sicurezza in dotazione AWS KMS possono aiutarti a soddisfare i requisiti di conformità relativi alla crittografia. Per ulteriori informazioni su SSE-KMS, vedere. [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#)

Come SSE-KMS funziona per le tabelle e i bucket da tavolo

SSE-KMS con secchi da tavolo si differenzia dai secchi per uso generico SSE-KMS nei seguenti modi:

- È possibile specificare le impostazioni di crittografia per i bucket di tabelle e le singole tabelle.
- È possibile utilizzare le chiavi gestite dal cliente solo con. SSE-KMS AWS le chiavi gestite non sono supportate.
- È necessario concedere le autorizzazioni per determinati ruoli e responsabili AWS del servizio per accedere AWS KMS alla chiave. Per ulteriori informazioni, consulta [Requisiti di autorizzazione per la crittografia delle tabelle S3 SSE-KMS](#). Sono incluse le concessione di accesso a:
 - Il principale di manutenzione S3: per eseguire la manutenzione delle tabelle crittografate

- Il tuo ruolo di integrazione con S3 Tables: per lavorare con tabelle crittografate nei servizi di analisi AWS
- Il ruolo di accesso client: per l'accesso diretto alle tabelle crittografate dai client Apache Iceberg
- Il principale di S3 Metadata: per l'aggiornamento delle tabelle di metadati S3 crittografate
- Le tabelle crittografate utilizzano chiavi a livello di tabella che riducono al minimo il numero di richieste effettuate per AWS KMS rendere più conveniente l'utilizzo delle tabelle SSE-KMS crittografate.

SSE-KMS crittografia per i bucket di tabelle

Quando crei un bucket di tabelle, puoi scegliere SSE-KMS come tipo di crittografia predefinito e selezionare una chiave KMS specifica che verrà utilizzata per la crittografia. Tutte le tabelle create all'interno di quel bucket erediteranno automaticamente queste impostazioni di crittografia dal relativo bucket di tabelle. Puoi utilizzare l' AWS CLI API S3 o gli AWS SDK per modificare o rimuovere le impostazioni di crittografia predefinite su un bucket di tabelle in qualsiasi momento. Quando si modificano le impostazioni di crittografia su un bucket di tabelle, tali impostazioni si applicano solo alle nuove tabelle create nel bucket. Le impostazioni di crittografia delle tabelle preesistenti non vengono modificate. Per ulteriori informazioni, consulta [Specifica della crittografia per bucket di tabelle](#).

SSE-KMS crittografia per le tabelle

È anche possibile crittografare una singola tabella con una chiave KMS diversa, indipendentemente dalla configurazione di crittografia predefinita del bucket. Per impostare la crittografia per una singola tabella, è necessario specificare la chiave di crittografia desiderata al momento della creazione della tabella. Per modificare la crittografia di una tabella esistente, è necessario creare una tabella con la chiave desiderata e copiare i dati dalla vecchia tabella a quella nuova. Per ulteriori informazioni, consulta [Specifica della crittografia per tabelle](#).

Quando si utilizza AWS KMS la crittografia, S3 Tables crea automaticamente chiavi di dati univoche a livello di tabella che crittografano i nuovi oggetti associati a ciascuna tabella. Queste chiavi vengono utilizzate per un periodo di tempo limitato, riducendo al minimo la necessità di AWS KMS richieste aggiuntive durante le operazioni di crittografia e riducendo il costo della crittografia. analogamente a [Chiavi S3 Bucket per SSE-KMS](#).

Applicazione e definizione dell'ambito di SSE-KMS utilizzo per tabelle e bucket di tabelle

È possibile utilizzare le politiche basate sulle risorse di S3 Tables, le politiche chiave KMS, le politiche basate sull'identità IAM o qualsiasi combinazione di queste, per imporre l'uso di per le tabelle e i bucket di tabelle S3. SSE-KMS Per ulteriori informazioni sulle policy di identità e risorse per le tabelle, consulta [Gestione degli accessi per Tabelle S3](#). Per ulteriori informazioni sulle policy della chiave, consulta [Policy della chiave](#) nella Guida per gli sviluppatori di AWS Key Management Service . Gli esempi seguenti mostrano come è possibile utilizzare le politiche per applicarle. SSE-KMS

Imporre l'uso di SSE-KMS per tutte le tabelle con una policy table bucket

Questo è un esempio di policy di bucket di tabelle che impedisce agli utenti di creare tabelle in uno specifico bucket di tabelle a meno che non crittografino le tabelle con una chiave AWS KMS specifica. Per utilizzare questa politica, sostituiscila *user input placeholders* con le tue informazioni:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceKMSEncryptionAlgorithm",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3tables:CreateTable"
      ],
      "Resource": [
        "arn:aws:s3tables:us-west-2:111122223333:bucket/example-table-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "s3tables:sseAlgorithm": "aws:kms"
        }
      }
    },
    {
      "Sid": "EnforceKMSEncryptionKey",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
```

```

    "s3tables:CreateTable"
  ],
  "Resource": [
    "arn:aws:s3tables:us-west-2:111122223333:bucket/example-table-bucket/*"
  ],
  "Condition": {
    "StringNotEquals": {
      "s3tables:kmsKeyArn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  }
}
]
}

```

Richiedere agli utenti di utilizzare SSE-KMS la crittografia con una policy IAM

Questa policy di identità IAM richiede agli utenti di utilizzare una AWS KMS chiave specifica per la crittografia durante la creazione o la configurazione delle risorse di S3 Tables. Per utilizzare questa policy, sostituiscila *user input placeholders* con le tue informazioni:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireSSEKMSOnTables",
      "Action": [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption",
        "s3tables:CreateTable"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3tables:sseAlgorithm": "aws:kms"
        }
      }
    },
    {
      "Sid": "RequireKMSKeyOnTables",
      "Action": [

```

```

        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption",
        "s3tables:CreateTable"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
        "StringNotEquals": {
            "s3tables:kmsKeyArn": "<key_arn>"
        }
    }
}
]
}

```

Limitazione dell'uso di una chiave a un bucket di tabelle specifico con una policy della chiave KMS

Questo esempio di policy della chiave KMS consente l'utilizzo della chiave solo da parte di un utente specifico per operazioni di crittografia in un bucket di tabella specifico. Questo tipo di policy è utile per limitare l'accesso a una chiave in scenari multi-account. Per utilizzare questa politica, sostituiscila *user input placeholders* con le tue informazioni:

JSON

```

{
  "Version": "2012-10-17",
  "Id": "Id",
  "Statement": [
    {
      "Sid": "AllowPermissionsToKMS",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "<table-bucket-arn>/*"
        }
      }
    }
  ]
}

```

```
}  
  }  
    }  
      ]  
    }  
  }
```

Monitoraggio e controllo della SSE-KMS crittografia per tabelle e bucket di tabelle

Per verificare l'utilizzo delle AWS KMS chiavi per i dati SSE-KMS crittografati, puoi utilizzare AWS CloudTrail i log. Puoi ottenere informazioni dettagliate sulle tue operazioni [crittografiche](#), ad esempio `GenerateDataKey` e `Decrypt`. CloudTrail supporta numerosi valori di [attributo](#) per filtrare la ricerca, tra cui nome dell'evento, nome utente e origine dell'evento.

Puoi tenere traccia delle richieste di configurazione della crittografia per le tabelle e i bucket di tabelle Amazon S3 utilizzando gli eventi. CloudTrail I seguenti nomi di eventi API vengono utilizzati nei CloudTrail log:

- `s3tables:PutTableBucketEncryption`
- `s3tables:GetTableBucketEncryption`
- `s3tables>DeleteTableBucketEncryption`
- `s3tables:GetTableEncryption`
- `s3tables:CreateTable`
- `s3tables:CreateTableBucket`

Note

EventBridge non è supportato per i bucket di tabelle.

Requisiti di autorizzazione per la crittografia delle tabelle S3 SSE-KMS

Quando utilizzi la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS) per le tabelle nei bucket di tabelle S3, devi concedere autorizzazioni per diverse identità nel tuo account. Come minimo, l'identità di accesso e il principale della manutenzione di Tabelle S3 devono avere accesso alla chiave, le altre autorizzazioni richieste dipendono dal caso d'uso.

Autorizzazioni richieste

Per accedere a una tabella crittografata con una chiave KMS, sono necessarie le seguenti autorizzazioni per la chiave:

- `kms:GenerateDataKey`
- `kms:Decrypt`

Important

Per utilizzare SSE-KMS sulle tabelle le esigenze del responsabile del servizio di manutenzione di Amazon S3 Tables (maintenance.s3tables.amazonaws.com) e le autorizzazioni sulla chiave. `kms:GenerateDataKey` `kms:Decrypt`

Autorizzazioni aggiuntive

Queste autorizzazioni aggiuntive sono necessarie a seconda del caso d'uso:

- Autorizzazioni per i servizi di AWS analisi e accesso diretto: se lavori con tabelle SSE-KMS crittografate tramite servizi di AWS analisi o motori di terze parti che accedono direttamente alle tabelle S3, il ruolo IAM che utilizzi richiede l'autorizzazione per utilizzare la tua chiave KMS.
- Autorizzazioni con Lake Formation abilitato: se hai optato AWS Lake Formation per il controllo degli accessi, il ruolo del servizio Lake Formation necessita dell'autorizzazione per utilizzare la tua chiave KMS.
- Autorizzazioni per le tabelle di metadati S3: se utilizzi la SSE-KMS crittografia per le tabelle di metadati S3, devi fornire al servizio S3 Metadata service principal () l'accesso alla tua chiave KMS. `metadata.s3.amazonaws.com` Ciò consente a S3 Metadata di aggiornare le tabelle crittografate in modo che riflettano le ultime modifiche apportate ai dati.

Note

Per le chiavi KMS multi-account, il ruolo IAM richiede sia l'autorizzazione di accesso alla chiave sia l'autorizzazione esplicita nella policy della chiave. Per ulteriori informazioni sulle autorizzazioni tra account per le chiavi KMS, [consulta Consentire agli account esterni di utilizzare una chiave KMS nella Service Developer Guide. AWS](#) AWS Key Management Service

Argomenti

- [Concessione delle autorizzazioni per la chiave KMS al principale del servizio di manutenzione di Tabelle S3](#)
- [Concessione ai principali IAM delle autorizzazioni per lavorare con tabelle crittografate in modalità integrata AWS servizi di analisi](#)
- [Concessione ai principali IAM delle autorizzazioni per lavorare con tabelle crittografate quando Lake Formation è abilitato](#)
- [Concessione delle autorizzazioni per l'utilizzo della chiave KMS al principale del servizio S3 Metadata](#)

Concessione delle autorizzazioni per la chiave KMS al principale del servizio di manutenzione di Tabelle S3

Questa autorizzazione è necessaria per creare tabelle SSE-KMS crittografate e per consentire la manutenzione automatica delle tabelle, ad esempio la compattazione, la gestione delle istantanee e la rimozione di file senza riferimenti sulle tabelle crittografate.

Note

Ogni volta che richiedi la creazione di una tabella SSE-KMS crittografata, S3 Tables verifica che il `maintenance.s3tables.amazonaws.com` principale abbia accesso alla tua chiave KMS. Per eseguire questo controllo, viene creato temporaneamente un oggetto a zero byte nel bucket di tabelle, che verrà rimosso automaticamente dalle operazioni di manutenzione con la [rimozione dei file senza riferimenti](#). Se la chiave KMS specificata per la crittografia non dispone dell'accesso di manutenzione, l'operazione `createTable` avrà esito negativo.

Per concedere l'accesso di manutenzione alle tabelle SSE-KMS crittografate, puoi utilizzare la seguente politica chiave di esempio. In questa policy, al principale del servizio `maintenance.s3tables.amazonaws.com` viene fornita l'autorizzazione a utilizzare una chiave KMS specifica per crittografare e decrittografare le tabelle in un bucket di tabelle specifico. Per utilizzare la policy, sostituiscila *user input placeholders* con le tue informazioni:

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "EnableKeyUsage",
    "Effect": "Allow",
    "Principal": {
      "Service": "maintenance.s3tables.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "<table-or-table-bucket-
arn>/*"
      }
    }
  }
]
}

```

Concessione ai principali IAM delle autorizzazioni per lavorare con tabelle crittografate in modalità integrata AWS servizi di analisi

Per lavorare con le tabelle S3 nei servizi di AWS analisi, integri i tuoi bucket di tabelle con. AWS Glue Data Catalog Questa integrazione consente ai servizi di AWS analisi di scoprire e accedere automaticamente ai dati delle tabelle. Per ulteriori informazioni sull'integrazione, consulta [Integrazione di Amazon S3 Tables con AWS servizi di analisi](#).

Quando lavori con tabelle SSE-KMS crittografate tramite servizi di AWS analisi o motori di terze parti e open source che accedono direttamente alle tabelle S3, il ruolo IAM che utilizzi richiede l'autorizzazione per utilizzare la tua AWS KMS chiave per le operazioni di crittografia.

Puoi concedere l'accesso con chiave KMS tramite una policy IAM associata al tuo ruolo o tramite una policy chiave KMS.

IAM policy

Allega questa policy in linea al ruolo IAM che usi per eseguire le query per consentire l'accesso con chiave KMS. Sostituisci la chiave KMS ARN con la tua.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKMSKeyUsage",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

KMS key policy

In alternativa, allega questa dichiarazione alla tua policy chiave KMS per consentire al ruolo IAM specificato di utilizzare la chiave. Sostituisci il ruolo ARN con il ruolo IAM che usi per le interrogazioni.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::<catalog-account-id>:role/<role-name>"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey",
  ],
  "Resource": "*"
}
```

Concessione ai principali IAM delle autorizzazioni per lavorare con tabelle crittografate quando Lake Formation è abilitato

Se hai optato AWS Lake Formation per il controllo degli accessi sull'integrazione con S3 Tables, il ruolo del servizio Lake Formation necessita dell'autorizzazione per utilizzare la tua AWS KMS chiave per le operazioni di crittografia. Lake Formation utilizza questo ruolo per fornire le credenziali per conto dei principali che accedono alle tue tabelle.

Il seguente esempio di politica chiave KMS concede al ruolo del servizio Lake Formation l'autorizzazione a utilizzare una chiave KMS specifica nell'account per le operazioni di crittografia. Sostituisci i valori segnaposto con i tuoi.

```
{
  "Sid": "AllowTableRoleAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/service-role/S3TablesRoleForLakeFormation"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "<kms-key-arn>"
}
```

Concessione delle autorizzazioni per l'utilizzo della chiave KMS al principale del servizio S3 Metadata

Per consentire ad Amazon S3 di aggiornare le tabelle di SSE-KMS metadati crittografate ed eseguire la manutenzione su tali tabelle di metadati, puoi utilizzare il seguente esempio di policy chiave. In questa policy, si consente ai principali del servizio metadata.s3.amazonaws.com e maintenance.s3tables.amazonaws.com di crittografare e decrittografare le tabelle in un bucket di tabelle specifico utilizzando una chiave specifica. Per utilizzare la policy, sostituiscila con le *user input placeholders* tue informazioni:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "EnableKeyUsage",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "maintenance.s3tables.amazonaws.com",
            "metadata.s3.amazonaws.com"
        ]
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "<table-or-table-bucket-
arn>/*"
        }
    }
}

```

Specificare la crittografia lato server con AWS KMS keys (SSE-KMS) nei bucket di tabelle

Tutti i bucket di tabelle Amazon S3 hanno la crittografia configurata per impostazione predefinita e tutte le nuove tabelle create in un bucket di tabelle vengono crittografate automaticamente quando sono inattive. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket di tabelle. Se desideri specificare un tipo di crittografia diverso, puoi utilizzare la crittografia lato server con AWS Key Management Service (AWS KMS) keys (). SSE-KMS

Puoi specificare SSE-KMS la crittografia nelle tue CreateTable richieste CreateTableBucket or oppure puoi impostare la configurazione di crittografia predefinita nel bucket di tabella di una richiesta. PutTableBucketEncryption

Important

Per consentire la manutenzione automatica su tabelle e bucket di tabelle SSE-KMS crittografati, devi concedere al principale del servizio maintenance.s3tables.amazonaws.com

l'autorizzazione all'uso della tua chiave KMS. Per ulteriori informazioni, consulta [Requisiti di autorizzazione per la crittografia delle tabelle S3 SSE-KMS](#).

Specifica della crittografia per bucket di tabelle

Puoi specificare SSE-KMS come tipo di crittografia predefinito quando crei un nuovo bucket di tabelle, ad esempio, vedi. [Creazione di un bucket di tabelle](#) Dopo aver creato un bucket di tabella, puoi specificare l'uso di SSE-KMS come impostazione di crittografia predefinita utilizzando le operazioni dell'API REST, AWS gli SDK e (). AWS Command Line Interface AWS CLI

Note

Quando si specifica SSE-KMS come tipo di crittografia predefinito, la chiave utilizzata per la crittografia deve consentire l'accesso all'entità del servizio di manutenzione di S3 Tables. Se il principale del servizio di manutenzione non dispone dell'accesso, non sarà possibile creare tabelle in quel bucket di tabelle. Per ulteriori informazioni, consulta [Concessione delle autorizzazioni per la chiave KMS al principale del servizio di manutenzione di Tabelle S3](#).

Utilizzo di AWS CLI

Per utilizzare il seguente AWS CLI comando di esempio, sostituiscilo *user input placeholders* con le tue informazioni.

```
aws s3tables put-table-bucket-encryption \
  --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
  table-bucket; \
  --encryption-configuration '{
    "sseAlgorithm": "aws:kms",
    "kmsKeyArn": "arn:aws:kms:us-
  east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }' \
  --region us-east-1
```

È possibile rimuovere l'impostazione di crittografia predefinita per un bucket di tabelle utilizzando l'operazione [DeleteTableBucketEncryption](#) API. Quando rimuovi le impostazioni di crittografia, le nuove tabelle create nel bucket di tabelle utilizzeranno la crittografia predefinita SSE-S3.

Specifica della crittografia per tabelle

È possibile applicare SSE-KMS la crittografia a una nuova tabella quando la si crea utilizzando motori di query, operazioni API REST, AWS SDK e AWS Command Line Interface (AWS CLI). Le impostazioni di crittografia specificate durante la creazione di una tabella hanno la precedenza sull'impostazione di crittografia predefinita del bucket di tabelle.

Note

Quando si utilizza SSE-KMS la crittografia per una tabella, la chiave utilizzata per la crittografia deve consentire al responsabile del servizio di manutenzione di S3 Tables di accedervi. Se il principale del servizio di manutenzione non dispone dell'accesso, non sarà possibile creare la tabella. Per ulteriori informazioni, consulta [Concessione delle autorizzazioni per la chiave KMS al principale del servizio di manutenzione di Tabelle S3](#).

Autorizzazioni richieste

Per creare tabelle crittografate sono necessarie le seguenti autorizzazioni:

- `s3tables:CreateTable`
- `s3tables:PutTableEncryption`

Utilizzo di AWS CLI

L' AWS CLI esempio seguente crea una nuova tabella con uno schema di base e la crittografa con una chiave gestita AWS KMS dal cliente. Per utilizzare il comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3tables create-table \  
  --table-bucket-arn "arn:aws:s3tables:Region:ownerAccountId:bucket/amzn-s3-demo-table-  
bucket" \  
  --namespace "mydataset" \  
  --name "orders" \  
  --format "ICEBERG" \  
  --encryption-configuration '{  
    "sseAlgorithm": "aws:kms",  
    "kmsKeyArn":  
    "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
```



```

}' \
--metadata '{
  "iceberg": {
    "schema": {
      "fields": [
        {
          "name": "order_id",
          "type": "string",
          "required": true
        },
        {
          "name": "order_date",
          "type": "timestamp",
          "required": true
        },
        {
          "name": "total_amount",
          "type": "decimal(10,2)",
          "required": true
        }
      ]
    }
  }
}'

```

La protezione dei dati ha lo scopo di proteggere i dati sia in transito (durante la trasmissione verso e da Amazon S3), sia quando sono a riposo (ovvero quando sono archiviati su disco nei data center Amazon S3). Tabelle S3 protegge sempre i dati in transito utilizzando Transport Layer Security (1.2 e versioni successive) tramite HTTPS. Per la protezione dei dati a riposo nei bucket di tabelle S3 sono disponibili le opzioni seguenti:

Server-side crittografia con chiavi gestite da Amazon S3 () SSE-S3

Tutti i bucket di tabelle Amazon S3 hanno la crittografia configurata per impostazione predefinita. L'opzione predefinita per la crittografia lato server è con le chiavi gestite di Amazon S3 (). SSE-S3 Questa crittografia non comporta costi aggiuntivi e si applica a tutte le tabelle nei bucket di tabelle S3, a meno che si specifichi un'altra forma di crittografia. Ogni oggetto è crittografato con una chiave univoca. Come protezione aggiuntiva, SSE-S3 crittografa la chiave stessa con una chiave root che ruota regolarmente. SSE-S3 utilizza uno dei più potenti cifrari a blocchi disponibili, Advanced Encryption Standard () a 256 bit, per crittografare i dati. AES-256

Server-side crittografia con chiavi () AWS KMS SSE-KMS

Puoi scegliere di configurare bucket o tabelle per utilizzare la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (). SSE-KMS I controlli di sicurezza in dotazione AWS KMS possono aiutarti a soddisfare i requisiti di conformità relativi alla crittografia. SSE-KMS ti offre un maggiore controllo sulle tue chiavi di crittografia consentendoti di effettuare le seguenti operazioni:

- Creare, visualizzare, modificare, monitorare, abilitare o disabilitare, ruotare e pianificare l'eliminazione delle chiavi KMS.
- Definire le policy che controllano come e da chi possono essere utilizzate le chiavi KMS.
- Tieni traccia dell'utilizzo delle chiavi AWS CloudTrail per verificare che le tue chiavi KMS vengano utilizzate correttamente.

S3 Tables supporta l'utilizzo di chiavi gestite dal cliente SSE-KMS per crittografare le tabelle. AWS le chiavi gestite non sono supportate. Per ulteriori informazioni sull'utilizzo SSE-KMS delle tabelle e dei bucket di tabelle S3, vedere. [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket delle tabelle](#)

Gestione degli accessi per Tabelle S3

In Tabelle S3 le risorse includono i bucket di tabelle e le tabelle in essi contenute. L'utente root di chi ha creato la Account AWS risorsa (il proprietario della risorsa) e gli utenti AWS Identity and Access Management (IAM) all'interno di quell'account che dispongono delle autorizzazioni necessarie possono accedere a una risorsa che hanno creato. Il proprietario della risorsa specifica gli utenti che possono accedere alla risorsa e le azioni che sono autorizzati a eseguire su di essa. Amazon S3 dispone di diversi strumenti di gestione degli accessi che è possibile utilizzare per concedere ad altri l'accesso alle risorse S3. Se hai integrato le tue tabelle con AWS Lake Formation, puoi anche gestire l'accesso granulare alle tabelle e ai namespace. I seguenti argomenti forniscono una panoramica delle risorse, delle azioni IAM e delle chiavi di condizione per Tabelle S3. Forniscono inoltre esempi di policy basate su risorse e identità per Tabelle S3.

Argomenti

- [Resources](#)
- [Azioni per Tabelle S3](#)
- [Chiavi di condizione per Tabelle S3](#)
- [Policy IAM basate su identità per Tabelle S3](#)

- [Resource-based politiche per S3 Tables](#)
- [AWS politiche gestite per le tabelle S3](#)
- [Concessione dell'accesso con la semantica SQL](#)
- [Gestione dell'accesso a una tabella o a un database con Lake Formation](#)

Resources

Le risorse di Tabelle S3 includono i bucket di tabelle e le tabelle in essi contenute.

- Bucket di tabelle: i bucket di tabelle sono progettati specificamente per le tabelle e offrono transazioni al secondo (TPS) più elevate e un throughput di query migliore rispetto alle tabelle autogestite nei bucket S3 per uso generico. I bucket di tabelle offrono le stesse caratteristiche di durabilità, disponibilità, scalabilità e prestazioni dei bucket generici di Amazon S3.
- Tabelle: le tabelle nei bucket di tabelle vengono archiviate in formato Apache Iceberg. È possibile eseguire query su queste tabelle utilizzando SQL standard nei motori di query che supportano Iceberg.

Gli Amazon Resource Names (ARN) per tabelle e bucket di tabelle contengono lo spazio dei `s3tables` nomi, l'ID e il nome del bucket. Regione AWS Account AWS Per accedere ed eseguire azioni sulle tabelle e sui bucket di tabelle, è necessario utilizzare i seguenti formati ARN:

- Formato ARN di tabella:

```
arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-bucket/table/demo-tableID
```

Azioni per Tabelle S3

In una policy basata su identità o una policy basata su risorse, vengono definite le azioni di Tabelle S3 consentite e negate per principali IAM specifici. Le azioni delle tabelle corrispondono alle operazioni API a livello di bucket e tabella. Tutte le azioni fanno parte di uno spazio dei nomi IAM univoco: `s3tables`.

Quando si utilizza un'azione in una policy, in genere si consente o si nega l'accesso all'operazione API con lo stesso nome. Tuttavia, in alcuni casi, una singola azione controlla l'accesso a più operazioni API. Ad esempio, le azioni `s3tables:GetTableData` includono le autorizzazioni per le operazioni API `GetObject`, `ListParts` e `ListMultiparts`.

Di seguito sono riportate le azioni supportate per i bucket di tabelle. Le seguenti azioni possono essere specificate nell'elemento `Action` di una policy delle risorse o una policy IAM.

Azione	Description	Livello di accesso	Cross-account accesso
<code>s3tables:CreateTableBucket</code>	Concede le autorizzazioni per creare un bucket di tabelle	Write	No
<code>s3tables:GetTableBucket</code>	Concede l'autorizzazione per recuperare e l'ARN di un bucket di tabelle, il nome del bucket di tabelle e la data di creazione.	Write	Sì
<code>s3tables:ListTableBuckets</code>	Concede l'autorizzazione per elencare tutti i bucket di tabelle in questo account.	Read	No
<code>s3tables:CreateNamespace</code>	Concede l'autorizzazione per creare uno	Write	Sì

Azione	Description	Livello di accesso	Cross-account accesso
	spazio dei nomi in un bucket di tabelle		
s3tables: GetNamespace	Concede l'autorizzazione per recuperare i dettagli dello spazio dei nomi	Read	Sì
s3tables: ListNamespaces	Concede l'autorizzazione per elencare tutti gli spazi dei nomi nel bucket di tabelle.	Read	Sì
s3tables: DeleteNamespace	Concede l'autorizzazione per eliminare uno spazio dei nomi in un bucket di tabelle	Write	Sì

Azione	Description	Livello di accesso	Cross-account accesso
s3tables:DeleteTableBucket	Concede l'autorizzazione per eliminare il bucket	Write	Sì
s3tables:PutTableBucketPolicy	Concede l'autorizzazione per aggiungere o sostituire una policy di bucket	Permissions Management	No
s3tables:GetTableBucketPolicy	Concede l'autorizzazione per recuperare la policy di bucket	Read	No
s3tables:DeleteTableBucketPolicy	Concede l'autorizzazione per eliminare la policy del bucket	Permissions Management	No

Azione	Description	Livello di accesso	Cross-account accesso
s3tables: GetTableBucketMaintenanceConfiguration	Concede l'autorizzazione per recuperare la configurazione di manutenzione per un bucket di tabelle	Read	Sì
s3tables: PutTableBucketMaintenanceConfiguration	Concede l'autorizzazione per aggiungere o sostituire la configurazione di manutenzione per un bucket di tabelle	Write	Sì
s3tables: PutTableBucketEncryption	Concede l'autorizzazione per aggiungere o sostituire la configurazione di crittografia per un bucket di tabelle	Write	No

Azione	Description	Livello di accesso	Cross-account accesso
s3tables: GetTableBucketEncryption	Concede l'autorizzazione per recuperare la configurazione di crittografia per un bucket di tabelle	Read	No
s3tables: DeleteTableBucketEncryption	Concede l'autorizzazione per eliminare la configurazione di crittografia per un bucket di tabelle	Write	No

Le seguenti azioni sono supportate per le tabelle:

Azione	Description	Livello di accesso	Cross-account accesso
s3tables: GetTableMaintenanceConfiguration	Concede l'autorizzazione per recuperare la configurazione di manutenzi	Read	Sì

Azione	Description	Livello di accesso	Cross-account accesso
	one per una tabella		
s3tables:PutTableMaintenanceConfiguration	Concede l'autorizzazione per aggiungere o sostituire la configurazione di manutenzione per una tabella	Write	Sì
s3tables:PutTablePolicy	Concede l'autorizzazione per aggiungere o sostituire una policy di tabella	Permissions Management	No
s3tables:GetTablePolicy	Concede l'autorizzazione per recuperare la policy della tabella	Read	No
s3tables:DeleteTablePolicy	Concede l'autorizzazione per eliminare la policy della tabella	Permissions management	No

Azione	Description	Livello di accesso	Cross-account accesso
s3tables: CreateTable	Concede l'autorizzazione per creare una tabella in un bucket di tabelle	Write	Sì
s3tables: GetTable	Concede l'autorizzazione per recuperare le informazioni di una tabella	Read	Sì
s3tables: GetTableMetadataLocation	Concede l'autorizzazione per recuperare il puntatore della tabella root (file di metadati)	Read	Sì
s3tables: ListTables	Concede l'autorizzazione per elencare tutte le tabelle in un bucket di tabelle	Read	Sì

Azione	Description	Livello di accesso	Cross-account accesso
s3tables: RenameTable	Concedere l'autorizzazione per modificare il nome di una tabella.	Write	Sì
s3tables: UpdateTableMetadataLocation	Concede l'autorizzazione per aggiornare il puntatore della tabella root (file di metadati)	Write	Sì
s3tables: GetTableData	Concede l'autorizzazione per leggere i metadati della tabella e gli oggetti dati memorizzati nel bucket di tabelle	Read	Sì

Azione	Description	Livello di accesso	Cross-account accesso
s3tables: PutTableData	Concede l'autorizzazione per scrivere i metadati della tabella e gli oggetti dati memorizzati nel bucket di tabelle	Write	Sì
s3tables: GetTableEncryption	Concede l'autorizzazione per recuperare le impostazioni di crittografia per una tabella	Write	No
s3tables: PutTableEncryption	Concede l'autorizzazione per aggiungere la crittografia a una tabella	Write	No
s3tables: DeleteTable	Concede l'autorizzazione per eliminare una tabella da un bucket di tabelle	Write	Sì

Per eseguire azioni di lettura e scrittura a livello di tabella, Tabelle S3 supporta operazioni API Amazon S3 come `GetObject` e `PutObject`. La seguente tabella fornisce un elenco di operazioni a livello di oggetto. Quando si concedono autorizzazioni di lettura e scrittura alle tabelle, si utilizzano le azioni seguenti.

Azione	API oggetto di S3		
s3tables: GetTableData	GetObject , ListParts , HeadObject		
s3tables: PutTableData	PutObject , CreateMultipartUpload , CompleteMultipartUpload , UploadPart , AbortMultipartUpload		

Ad esempio, se un utente dispone di autorizzazioni `GetTableData`, può leggere tutti i file associati alla tabella, come il file di metadati, il manifesto, i file di elenco manifesto e i file di dati Parquet.

Chiavi di condizione per Tabelle S3

Tabelle S3 supporta le [chiavi di contesto delle condizioni globali di AWS](#).

Inoltre, Tabelle S3 definisce le seguenti chiavi di condizione che è possibile utilizzare in una policy di accesso.

Chiave di condizione	Description	Tipo	
s3tables:tableName	<p>Filtra l'accesso in base al nome delle tabelle nel bucket di tabelle.</p> <p>È possibile utilizzare la chiave di condizione s3tables:tableName per scrivere policy IAM o di bucket di tabelle che limitano l'accesso degli utenti o delle applicazioni solo alle tabelle che soddisfano la condizione del nome.</p> <p>È important e notare che se si utilizza</p>	String	

Chiave di condizione	Description	Tipo	
	la chiave di condizione <code>s3tables:tableName</code> per controllare l'accesso, le modifiche al nome delle tabelle potrebbero influire su queste policy. Valore di esempio: <code>"s3tables:tableName":"department"</code>		

Chiave di condizione	Description	Tipo	
s3tables:namespace	<p>Filtra l'accesso in base agli spazi dei nomi creati nel bucket di tabelle.</p> <p>È possibile utilizzare la chiave di condizione s3tables:namespace per scrivere policy di IAM, di tabella o di bucket di tabelle che limitano l'accesso di utenti o applicazioni alle tabelle che fanno parte di uno specifico spazio dei nomi. Valore di esempio: "s3tables:namespace":"hr"</p>	String	

Chiave di condizione	Description	Tipo	
	È important e notare che se si utilizza la chiave di condizione <code>s3tables: namespace</code> per controllare l'accesso, le modifiche agli spazi dei nomi potrebbero influire su queste policy.		

Chiave di condizione	Description	Tipo	
s3tables:SSEAlgorithm	<p>Filtra l'accesso tramite l'algoritmo di crittografia lato server utilizzato per crittografare una tabella.</p> <p>È possibile utilizzare la chiave di condizione s3tables:SSEAlgorithm per scrivere policy di IAM, di tabella o di bucket di tabelle che limitano l'accesso degli utenti o delle applicazioni alle tabelle crittografate con un determinato tipo di crittografia. Valore di</p>	String	

Chiave di condizione	Description	Tipo	
	<div><div>esempio: "s3tables :SSEAlgor ithm":"aw s:kms"</div><div>È important e notare che se si utilizza la chiave di condizione s3tables: SSEAlgori thm per controllare l'accesso, le modifiche alla crittogra fia potrebber o influire su queste policy.</div></div>		

Chiave di condizione	Description	Tipo	
s3tables:KMSKeyArn	<p>Filtra l'accesso in base alla AWS KMS chiave ARN per la chiave utilizzata per crittografare una tabella</p> <p>È possibile utilizzare la chiave di condizione s3tables:KMSKeyArn per scrivere policy di IAM, di tabella o di bucket di tabelle che limitano l'accesso degli utenti o delle applicazioni alle tabelle crittografate con una chiave KMS specifica.</p> <p>È important e notare che</p>	ARN	

Chiave di condizione	Description	Tipo	
	se si utilizza la chiave di condizione <code>s3tables:KMSKeyArn</code> per controllare l'accesso, le modifiche alla chiave KMS potrebbero influire su queste policy.		

Policy IAM basate su identità per Tabelle S3

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare tabelle e bucket di tabelle. Inoltre, non sono in grado di eseguire attività utilizzando la console S3, l' AWS Command Line Interface (AWS CLI) o le REST API di Amazon S3. Per creare bucket e tabelle di tabelle e accedervi, un amministratore AWS Identity and Access Management (IAM) deve concedere le autorizzazioni necessarie al ruolo o agli utenti IAM. Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Nel seguente argomento sono forniti esempi di policy IAM basate su identità. Per utilizzare le seguenti politiche di esempio, sostituiscile *user input placeholders* con le tue informazioni.

Argomenti

- [Esempio 1: Consentire l'accesso per creare e utilizzare bucket di tabelle](#)
- [Esempio 2: Consentire l'accesso per creare e utilizzare tabelle in un bucket di tabelle](#)

Esempio 1: Consentire l'accesso per creare e utilizzare bucket di tabelle

.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBucketActions",
      "Effect": "Allow",
      "Action": [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketPolicy",
        "s3tables:GetTableBucketPolicy",
        "s3tables:ListTableBuckets",
        "s3tables:GetTableBucket"
      ],
      "Resource": "arn:aws:s3tables:us-east-1:111122223333:bucket/*"
    }
  ]
}
```

Esempio 2: Consentire l'accesso per creare e utilizzare tabelle in un bucket di tabelle

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBucketActions",
      "Effect": "Allow",
      "Action": [
        "s3tables:GetTableBucket",
        "s3tables:ListTables",
        "s3tables:CreateTable",
        "s3tables:PutTableData",
        "s3tables:GetTableData",
        "s3tables:GetTable",
        "s3tables:GetTableMetadataLocation",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:GetNamespace",
        "s3tables:CreateNamespace",

```

```

        "s3tables:ListNamespaces"
    ],
    "Resource": [
        "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  

bucket",
        "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  

bucket/table/*"
    ]
}
]
}

```

Resource-based politiche per S3 Tables

Tabelle S3 fornisce policy basate sulle risorse per la gestione dell'accesso ai bucket delle tabelle e alle tabelle: policy dei bucket delle tabelle e policy delle tabelle. Puoi utilizzare una policy dei bucket delle tabelle per concedere le autorizzazioni di accesso all'API a livello di bucket delle tabelle, spazio dei nomi o tabella. Le autorizzazioni associate al bucket delle tabelle possono essere applicate a tutte le tabelle del bucket o solo a parte di esse, a seconda della definizione della policy. È possibile utilizzare una policy della tabella per concedere autorizzazioni a livello di tabella.

Quando riceve una richiesta, Tabelle S3 verifica innanzitutto che il richiedente disponga delle autorizzazioni necessarie. Valuta quindi tutte le policy di accesso, le policy utente e le policy basate sulle risorse pertinenti per decidere se autorizzare la richiesta (la policy dell'utente IAM, la policy del ruolo IAM, la policy del bucket di tabelle e la policy della tabella). Ad esempio, se una policy del bucket delle tabelle concede a un utente le autorizzazioni per eseguire tutte le azioni sulle tabelle nel bucket (inclusa `DeleteTable`), ma una singola tabella include una policy di tabella che nega l'azione `DeleteTable` a tutti gli utenti, l'utente non può eliminare la tabella.

Il seguente argomento include esempi di policy relative alle tabelle e ai bucket delle tabelle. Per usare queste policy, sostituisci *user input placeholders* con le tue informazioni.

Note

- Ogni policy che concede autorizzazioni per modificare le tabelle deve includere autorizzazioni per consentire a `GetTableMetadataLocation` di accedere al file radice della tabella. Per ulteriori informazioni, consulta [GetTableMetadataLocation](#).
- Ogni volta che si esegue un'attività di scrittura o eliminazione sulla tabella, includere le autorizzazioni per `UpdateTableMetadataLocation` nella tua policy di accesso.

- È consigliabile utilizzare una policy del bucket delle tabelle per regolare l'accesso alle azioni a livello di bucket e una policy della tabella per regolare l'accesso alle azioni a livello di tabella. Nei casi in cui si desidera definire lo stesso set di autorizzazioni su più tabelle, è consigliabile utilizzare una policy del bucket delle tabelle.

Argomenti

- [Esempio 1: la policy del bucket delle tabelle consente l'accesso a PutBucketMaintenanceConfiguration per i bucket in un account](#)
- [Esempio 2: policy Table bucket per consentire l'accesso in lettura \(SELECT\) alle tabelle archiviate nel namespace hr](#)
- [Esempio 3: policy della tabella per consentire all'utente di eliminare una tabella](#)

Esempio 1: la policy del bucket delle tabelle consente l'accesso a **PutBucketMaintenanceConfiguration** per i bucket in un account

La seguente policy esemplificativa del bucket delle tabelle consente all'`data steward` di IAM di eliminare gli oggetti senza riferimento per tutti i bucket di un account consentendo l'accesso a `PutBucketMaintenanceConfiguration`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/datasteward"
      },
      "Action": [
        "s3tables:PutTableBucketMaintenanceConfiguration"
      ],
      "Resource": "arn:aws:s3tables:us-east-1:111122223333:bucket/*"
    }
  ]
}
```


Esempio 2: policy Table bucket per consentire l'accesso in lettura (SELECT) alle tabelle archiviate nel namespace **hr**

Di seguito è riportata una policy di bucket di tabelle di esempio che consente a Jane, un utente con ID Account AWS 123456789012 di accedere alle tabelle archiviate nel namespace **hr** in un bucket di tabelle.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Jane"
      },
      "Action": [
        "s3tables:GetTableData",
        "s3tables:GetTableMetadataLocation"
      ],
      "Resource": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket/table/*",
      "Condition": {
        "StringLike": {
          "s3tables:namespace": "hr"
        }
      }
    }
  ]
}
```

Esempio 3: policy della tabella per consentire all'utente di eliminare una tabella

Il seguente esempio di policy di tabella consente al ruolo IAM di `data_steward` di eliminare una tabella.

JSON

```
{
```

```
"Version": "2012-10-17",
"Id": "DeleteTable",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/datasteward"
    },
    "Action": [
      "s3tables:DeleteTable",
      "s3tables:UpdateTableMetadataLocation",
      "s3tables:PutTableData",
      "s3tables:GetTableMetadataLocation"
    ],
    "Resource": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-
demo-bucket/table/tableUUID"
  }
]
```

AWS politiche gestite per le tabelle S3

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. Le policy gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché sono disponibili per tutti i clienti. AWS si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. Se AWS aggiorna le autorizzazioni definite in una policy AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui la policy è associata. AWS è più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AmazonS3TablesFullAccess

È possibile allegare la policy AmazonS3TablesFullAccess alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso completo a Tabelle Amazon S3. Per ulteriori informazioni su questa policy, consulta [AmazonS3TablesFullAccess](#).

AWS politica gestita: AmazonS3TablesReadOnlyAccess

È possibile allegare la policy AmazonS3TablesReadOnlyAccess alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso in sola lettura a Tabelle Amazon S3. Per ulteriori informazioni su questa policy, consulta [AmazonS3TablesReadOnlyAccess](#).

AWS politica gestita: AmazonS3TablesLakeFormationServiceRole

È possibile allegare la policy AmazonS3TablesLakeFormationServiceRole alle identità IAM. Questa politica concede autorizzazioni che consentono al ruolo di AWS Lake Formation servizio di accedere alle tabelle S3. AWS KMS le autorizzazioni vengono utilizzate per consentire a Lake Formation di accedere alle tabelle crittografate. Per ulteriori informazioni su questa policy, consulta [AmazonS3TablesLakeFormationServiceRole](#).

Amazon S3 Tables si aggiorna a AWS policy gestite

Visualizza i dettagli sugli aggiornamenti delle policy AWS gestite per Amazon S3 Tables da quando S3 Tables ha iniziato a tracciare queste modifiche.

Modifica	Descrizione	Data
Tabelle Amazon S3 aggiornate. AmazonS3TablesFullAccess	S3 Tables ha aggiornato la policy AWS gestita denominata AmazonS3TablesFullAccess. Questo aggiornamento concede l'autorizzazione a passare un ruolo al servizio S3 Tables Replication.	2 dicembre 2025
Tabelle Amazon S3 ha aggiunto AmazonS3TablesLakeFormationServiceRole.	S3 Tables ha aggiunto una nuova politica AWS gestita denominata AmazonS3TablesLakeFormationServiceRole. Questa	19 maggio 2025

Modifica	Descrizione	Data
	policy fornisce le autorizzazioni che consentono al ruolo di servizio Lake Formation l'accesso a Tabelle S3.	
Tabelle Amazon S3 ha aggiunto AmazonS3TablesFullAccess .	S3 Tables ha aggiunto una nuova politica gestita AWS denominata. AmazonS3TablesFullAccess Questa policy concede le autorizzazioni che consentono o l'accesso completo a Tabelle Amazon S3.	3 dicembre 2024
Tabelle Amazon S3 ha aggiunto AmazonS3TablesReadOnlyAccess .	S3 Tables ha aggiunto una nuova politica gestita AWS denominata. AmazonS3TablesReadOnlyAccess Questa policy concede le autorizzazioni che consentono o l'accesso in sola lettura a Tabelle Amazon S3.	3 dicembre 2024
Tabelle Amazon S3 ha iniziato a monitorare le modifiche.	Amazon S3 Tables ha iniziato a tracciare le modifiche per le sue AWS policy gestite.	3 dicembre 2024

Concessione dell'accesso con la semantica SQL

È possibile fornire autorizzazioni alle tabelle utilizzando la semantica SQL nelle policy di tabelle e di bucket di tabelle. Esempi di semantica SQL che è possibile utilizzare sono CREATE, INSERT, DELETE, UPDATE e ALTER. La tabella seguente fornisce un elenco di azioni API associate alla semantica SQL che è possibile utilizzare per fornire autorizzazioni agli utenti.

Tabelle S3 supporta parzialmente le autorizzazioni con la semantica SQL. Ad esempio, l'API CreateTable crea solo una tabella vuota nel bucket di tabelle. Sono necessarie autorizzazioni

aggiuntive come `UpdateTableMetadata`, `PutTableData` e `GetTableMetadataLocation` per poter impostare lo schema della tabella. Queste autorizzazioni aggiuntive significano anche che si sta concedendo all'utente l'autorizzazione per inserire righe nella tabella. Se si desidera regolare l'accesso esclusivamente sulla base della semantica SQL, è consigliabile utilizzare [AWS Lake Formation](#) o una qualsiasi soluzione di terze parti integrata con Tabelle S3.

Table-level attività	Azioni di IAM		
SELECT	s3tables: GetTableData , s3tables: GetTableMetadataLocation		
CREATE	s3tables: CreateTable , s3tables: UpdateTableMetadataLocation , s3tables: PutTableData , s3tables: GetTableMetadataLocation ,		
INSERT	s3tables: UpdateTableMetadataLocation ,		

Table-level attività	Azioni di IAM		
	s3tables: PutTableData , s3tables: GetTableMetadataLocation		
UPDATE	s3tables: UpdateTableMetadataLocation , s3tables: PutTableData , s3tables: GetTableMetadataLocation		

Table-level attività	Azioni di IAM		
ALTER,RENAME	s3tables: UpdateTab leMetadat aLocation , s3tables: PutTableD ata , s3tables: GetTableM etadataLo cation , s3tables: RenameTab le		
DELETE,DROP	s3tables: DeleteTab le , s3tables: UpdateTab leMetadat aLocation , s3tables: PutTableD ata , s3tables: GetTableM etadataLo cation		

 Note

L'autorizzazione `s3tables:DeleteTable` è necessaria per eliminare una tabella da un bucket di tabelle. Questa autorizzazione consente di rimuovere definitivamente una tabella e tutti i dati e i metadati associati. Utilizza questa autorizzazione con attenzione perché l'operazione di eliminazione non può essere annullata.

Gestione dell'accesso a una tabella o a un database con Lake Formation

Se i bucket di tabelle sono integrati con il servizio di AWS analisi tramite Lake Formation, Lake Formation gestisce l'accesso alle tabelle e richiede che ogni principale IAM (utente o ruolo) sia autorizzato a eseguire le relative azioni. Lake Formation utilizza il proprio modello di autorizzazioni Lake Formation che consente un controllo granulare degli accessi per le risorse del Catalogo dati.

Per ulteriori informazioni, consulta la pagina relativa alla [panoramica delle autorizzazioni di Lake Formation](#) nella Guida per gli sviluppatori di AWS Lake Formation .

Esistono due tipi principali di autorizzazioni in AWS Lake Formation:

1. Le autorizzazioni di accesso ai metadati controllano la possibilità di creare, leggere, aggiornare ed eliminare database e tabelle di metadati nel Catalogo dati.
2. Le autorizzazioni di accesso ai dati sottostanti controllano la capacità di leggere e scrivere dati nelle posizioni Amazon S3 sottostanti a cui fanno riferimento le risorse del Catalogo dati.

Lake Formation utilizza una combinazione del proprio modello di autorizzazioni e del modello di autorizzazioni IAM per controllare l'accesso alle risorse del Catalogo dati e ai dati sottostanti:

- Affinché una richiesta di accesso alle risorse del Catalogo dati o ai dati sottostanti abbia esito positivo, la richiesta deve superare i controlli di autorizzazione sia di IAM sia di Lake Formation.
- Le autorizzazioni IAM controllano l'accesso a Lake Formation, alle AWS Glue API e alle risorse, mentre le autorizzazioni Lake Formation controllano l'accesso alle risorse del Data Catalog, alle posizioni Amazon S3 e ai dati sottostanti.

Le autorizzazioni Lake Formation si applicano solo nella Regione in cui sono state concesse e un principale deve essere autorizzato da un amministratore del data lake o da un altro principale con le autorizzazioni necessarie al fine di ottenere le autorizzazioni Lake Formation.

 Note

L'utente che ha eseguito l'integrazione del bucket di tabelle dispone già delle autorizzazioni Lake Formation per le tabelle. Se sei l'unico principale che accede alle tabelle, questa fase può essere ignorata. È sufficiente fornire le autorizzazioni Lake Formation sulle tabelle ad altri principali IAM. Ciò consente ad altri principali di accedere alla tabella durante l'esecuzione di query. Per ulteriori informazioni, consulta [Concessione dell'autorizzazione Lake Formation per una tabella o un database](#).

Concessione dell'autorizzazione Lake Formation per una tabella o un database

È possibile fornire un'autorizzazione Lake Formation al principale per una tabella o un database di un bucket di tabelle tramite la console Lake Formation o la AWS CLI.

 Note

Quando concedi le autorizzazioni di Lake Formation su una risorsa Data Catalog a un account esterno o direttamente a un responsabile IAM in un altro account, Lake Formation utilizza il servizio AWS Resource Access Manager (AWS RAM) per condividere la risorsa. Se l'account assegnatario appartiene alla stessa organizzazione dell'account concedente, la risorsa condivisa è immediatamente disponibile per l'assegnatario. Se l'account assegnatario non appartiene alla stessa organizzazione, AWS RAM invia un invito all'account assegnatario per accettare o rifiutare la concessione della risorsa. Quindi, per rendere disponibile la risorsa condivisa, l'amministratore del data lake nell'account del beneficiario deve utilizzare la AWS RAM console o AWS CLI accettare l'invito. Per ulteriori informazioni sulla condivisione dei dati tra account, consulta la condivisione [Cross-account dei dati in Lake Formation](#) nella Developer Guide. AWS Lake Formation

Console

1. Apri la AWS Lake Formation console all'indirizzo <https://console.aws.amazon.com/lakeformation/> e accedi come amministratore del data lake. Per ulteriori informazioni su come creare un amministratore del data lake, consulta [Creare un amministratore di data lake](#) nella Guida per gli sviluppatori di AWS Lake Formation .
2. Nel riquadro di navigazione scegli Autorizzazioni dati, quindi seleziona Concedi.
3. Nella pagina Concedi le autorizzazioni, in Principali, esegui una delle seguenti operazioni:

- Per Amazon Athena o Amazon Redshift, scegli Utenti e ruoli IAM e seleziona il principale IAM che usi per le query.
 - Per Amazon Data Firehose, scegli Utenti e ruoli IAM e seleziona il ruolo di servizio creato per lo streaming alle tabelle.
 - Per Quick, scegli utenti e gruppi SAML e inserisci l'Amazon Resource Name (ARN) del tuo utente amministratore di Quick.
 - Per l'accesso agli AWS Glue REST endpoint, scegli utenti e ruoli IAM, quindi seleziona il ruolo IAM che hai creato per il tuo cliente. Per ulteriori informazioni, consulta [Creazione di un ruolo IAM per il client](#)
4. Nella sezione LF-Tags Risorse del catalogo, scegli Risorse Named Data Catalog.
 5. Per Cataloghi, scegli il catalogo secondario creato al momento dell'integrazione del bucket di tabelle, ad esempio *account-id:s3tablescatalog/amzn-s3-demo-bucket*.
 6. Per Database, scegli lo spazio dei nomi del bucket di tabelle S3 che è stato creato.
 7. (Facoltativo) Per Tabelle, scegli la tabella S3 creata nel bucket di tabelle.

 Note

Per creare una nuova tabella nell'editor di query Athena, non occorre selezionare una tabella.

8. Esegui una delle seguenti operazioni:
 - Se hai specificato una tabella nel passaggio precedente, per Autorizzazioni per le tabelle scegli Super.
 - Se non hai specificato una tabella nel passaggio precedente, vai a Autorizzazioni del database. Per la condivisione dei dati multi-account, non è possibile scegliere Super per fornire all'altro principale tutte le autorizzazioni sul database. Scegli invece autorizzazioni più dettagliate, come Descrivi.
9. Scegliere Concedi.

CLI

1. Assicurati di eseguire i seguenti AWS CLI comandi come amministratore del data lake. Per ulteriori informazioni, consulta [Creare un amministratore di data lake](#) nella Guida per gli sviluppatori di AWS Lake Formation .

2. Esegui il seguente comando per concedere le autorizzazioni di Lake Formation sulla tabella nel bucket di tabelle S3 a un principale IAM per accedere alla tabella. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws lakeformation grant-permissions \  
--region us-east-1 \  
--cli-input-json \  
'{  
  "Principal": {  
    "DataLakePrincipalIdentifier": "user or role ARN, for example,  
arn:aws:iam::account-id:role/example-role"  
  },  
  "Resource": {  
    "Table": {  
      "CatalogId": "account-id:s3tablescatalog/amzn-s3-demo-bucket",  
      "DatabaseName": "S3 table bucket namespace, for example,  
test_namespace",  
      "Name": "S3 table bucket table name, for example test_table"  
    }  
  },  
  "Permissions": [  
    "ALL"  
  ]  
}'
```

Connettività VPC per Tabelle S3

Tutte le tabelle in Tabelle S3 sono nel formato Apache Iceberg e sono costituite da due tipi di oggetti S3. Questi due tipi di oggetti sono file di dati in cui sono archiviati dati e file di metadati che tengono traccia delle informazioni sui file di dati in momenti diversi. Tutte le operazioni relative ai bucket di tabelle, agli spazi dei nomi e alle tabelle (ad esempio CreateNamespace, CreateTable e così via) vengono instradate tramite un endpoint Tabelle S3 (`s3tables.region.amazonaws.com`) e tutte le operazioni a livello di oggetto che leggono o scrivono i file di dati e metadati continuano a essere instradate attraverso un endpoint del servizio S3 (`s3.region.amazonaws.com`).

Per accedere a S3 Tables, Amazon S3 supporta due tipi di endpoint VPC utilizzando AWS PrivateLink: endpoint gateway ed endpoint di interfaccia. Un endpoint gateway è un gateway specificato nella tabella di routing per accedere a S3 dal tuo VPC tramite la rete. AWS Gli endpoint di interfaccia estendono le funzionalità degli endpoint gateway utilizzando indirizzi IP privati per

instradare le richieste verso Amazon S3 dal VPC, on-premises o da un VPC in un'altra Regione AWS tramite peering VPC o AWS Transit Gateway.

Per accedere a Tabelle S3 da un VPC, è consigliabile creare due endpoint VPC (uno per S3 e l'altro per Tabelle S3). È possibile creare un gateway o un endpoint di interfaccia per indirizzare le operazioni a livello di file (oggetto) verso S3 e un endpoint di interfaccia per indirizzare le operazioni a livello di bucket e tabella verso Tabelle S3. Gli endpoint VPC possono essere creati e utilizzati per richieste a livello di file utilizzando S3. Per ulteriori informazioni, consulta [Gateway endpoint](#) nella Guida per l'utente. AWS PrivateLink

Per ulteriori informazioni sull'utilizzo AWS PrivateLink per creare e utilizzare endpoint per tabelle S3, consulta i seguenti argomenti. Per creare un endpoint di interfaccia VPC, consulta [Creazione di un endpoint VPC](#) nella Guida AWS PrivateLink .

Argomenti

- [Creazione di endpoint VPC per Tabelle S3](#)
- [Accesso ai bucket e alle tabelle di tabelle tramite gli endpoint utilizzando AWS CLI](#)
- [Configurazione di una rete VPC quando si utilizzano motori di query](#)
- [Uso degli endpoint dual-stack per accedere a tabelle e bucket di tabelle](#)
- [Utilizzo delle condizioni delle policy degli endpoint VPC con le policy dei bucket table](#)
- [Limitazione dell'accesso a Tabelle S3 all'interno della rete VPC](#)

Creazione di endpoint VPC per Tabelle S3

Quando si crea un endpoint VPC, Tabelle S3 genera due tipi di nomi DNS specifici degli endpoint: regionale e zonale.

- Il formato di un nome DNS regionale è il seguente:
`VPCendpointID.s3tables.AWSregion.vpce.amazonaws.com`. Ad esempio, per l'ID endpoint VPC `vpce-1a2b3c4d`, il nome DNS generato sarà simile a `vpce-1a2b3c4d-5e6f.s3tables.us-east-1.vpce.amazonaws.com`.
- Il formato di un nome DNS zonale è il seguente: `VPCendpointID-AvailabilityZone.s3tables.AWSregion.vpce.amazonaws.com`. Ad esempio, per l'ID endpoint VPC `vpce-1a2b3c4d-5e6f.`, il nome DNS generato potrebbe essere simile a `vpce-1a2b3c4d-5e6f-us-east-1a.s3tables.us-east-1.vpce.amazonaws.com`.

Un nome DNS zonale include la zona di disponibilità dell'utente. È possibile utilizzare i nomi DNS zonali se l'architettura isola le zone di disponibilità. I nomi DNS S3 specifici degli endpoint possono essere risolti dal dominio DNS pubblico S3.

Le opzioni DNS private consentono anche di semplificare l'instradamento del traffico S3 sugli endpoint VPC e di sfruttare il percorso di rete più economico disponibile per l'applicazione. Il DNS privato mappa l'endpoint pubblico di Tabelle S3, ad esempio `s3tables.region.amazonaws.com`, su un IP privato nel VPC dell'utente. È possibile utilizzare le opzioni DNS private per indirizzare il traffico S3 regionale senza aggiornare i client S3 per usare i nomi DNS specifici degli endpoint di interfaccia.

Accesso ai bucket e alle tabelle di tabelle tramite gli endpoint utilizzando AWS CLI

È possibile utilizzare AWS Command Line Interface (AWS CLI) per accedere ai bucket e alle tabelle delle tabelle tramite gli endpoint dell'interfaccia. Con il AWS CLI, `aws s3` i comandi indirizzano il traffico attraverso l'endpoint Amazon S3. I `aws s3tables` AWS CLI comandi utilizzano l'endpoint Amazon S3 Tables.

Un esempio di endpoint VPC `s3tables` è `vpce-0123456afghjipljw-nmopsqea.s3tables.region.vpce.amazonaws.com`

Un endpoint VPC `s3tables` non include un nome di bucket. Puoi accedere all'endpoint `s3tables` VPC utilizzando i comandi `aws s3tables` AWS CLI

Un esempio di endpoint VPC `s3` è `amzn-s3-demo-bucket.vpce-0123456afghjipljw-nmopsqea.s3.region.vpce.amazonaws.com`

È possibile accedere all'endpoint `s3` VPC utilizzando i comandi `aws s3` AWS CLI

Utilizzo di AWS CLI

Per accedere ai bucket e alle tabelle di tabelle tramite gli endpoint dell'interfaccia utilizzando AWS CLI i parametri `-region` e `-endpoint-url`. Per eseguire azioni a livello di tabelle e bucket di tabelle, utilizzare l'URL dell'endpoint Tabelle S3. Per eseguire azioni a livello di oggetto, utilizzare l'URL dell'endpoint Amazon S3.

Negli esempi seguenti, sostituiscili *user input placeholders* con le tue informazioni.

Esempio 1: Utilizzo dell'URL dell'endpoint per elencare i bucket di tabelle nel proprio account

```
aws s3tables list-table-buckets --endpoint https://vpce-0123456afghjpljb-aac.s3tables.us-east-1.vpce.amazonaws.com --region us-east-1
```

Esempio 2: Utilizzo di un URL dell'endpoint per elencare le tabelle nel proprio bucket

```
aws s3tables list-tables --table-bucket-arn arn:aws:s3tables:us-east-1:123456789301:bucket/amzn-s3-demo-bucket --endpoint https://vpce-0123456afghjpljb-aac.s3tables.us-east-1.vpce.amazonaws.com --region us-east-1
```

Configurazione di una rete VPC quando si utilizzano motori di query

Completare la procedura seguente per configurare una rete VPC quando si utilizzano motori di query.

1. Per iniziare, è possibile creare o aggiornare un VPC. Per ulteriori informazioni, consulta la sezione [Creazione di un VPC](#).
2. Per le operazioni a livello di bucket di tabelle e di tabelle che instradano a Tabelle S3, creare un nuovo endpoint di interfaccia. Per ulteriori informazioni, consulta [Accedere a un AWS servizio utilizzando un endpoint](#) VPC di interfaccia.
3. Per tutte le operazioni a livello di oggetto che instradano ad Amazon S3, creare un endpoint gateway o un endpoint di interfaccia. Per ulteriori informazioni sugli endpoint gateway, consulta [Creare un endpoint del gateway](#).
4. Successivamente, configurare le risorse di dati e avviare un cluster Amazon EMR. Per ulteriori informazioni, consulta [Nozioni di base su Amazon EMR](#).
5. Pertanto è possibile inviare un'applicazione Spark con una configurazione aggiuntiva selezionando i nomi DNS dall'endpoint VPC. Ad esempio, `spark.sql.catalog.ice_catalog.s3tables.endpoint` e `https://interface-endpoint.s3tables.us-east-1.vpce.amazonaws.com` Per ulteriori informazioni, consulta [Inviare il lavoro al cluster Amazon EMR](#).

Uso degli endpoint dual-stack per accedere a tabelle e bucket di tabelle

S3 Tables supporta la connettività dual-stack per. AWS PrivateLink Dual-stack gli endpoint consentono di accedere ai bucket di tabelle S3 utilizzando il protocollo Internet versione 6 (IPv6), oltre al protocollo IPv4, a seconda di ciò che supporta la rete. Puoi accedere a un bucket S3 tramite un endpoint dual-stack utilizzando la seguente convenzione di denominazione:

```
s3tables.<region>.api.aws
```

Di seguito sono riportati alcuni aspetti da prendere in considerazione prima di tentare di accedere a Tabelle S3 e ai bucket di tabelle tramite protocollo IPv6 su VPC:

- Il client utilizzato per accedere alle tabelle e il client S3 devono essere entrambi abilitati per il dual-stack.
- L'ingresso IPv6 non è abilitato per impostazione predefinita per i gruppi di sicurezza VPC. Per consentire l'accesso IPv6, è necessario aggiungere una nuova regola che permetta il traffico HTTPS (porta TCP 443) al gruppo di sicurezza. Per ulteriori informazioni, consulta [Configurazione di regole del gruppo di sicurezza](#) nella Guida per l'utente di Amazon EC2.
- Se al VPC non sono assegnati CIDR IPv6, sarà necessario aggiungere manualmente un intervallo CIDR IPv6 al VPC. Per ulteriori informazioni, consulta [Aggiunta del supporto IPv6 per il VPC](#) nella Guida per l'utente di AWS PrivateLink .
- Se utilizzi policy IAM di filtraggio degli indirizzi IP, queste devono essere aggiornate per gestire gli indirizzi IPv6. Per ulteriori informazioni sulla gestione delle autorizzazioni di accesso con IAM, consulta [Gestione delle identità e degli accessi per Amazon S3](#).

Per creare un nuovo endpoint VPC che utilizzi l'endpoint dual-stack per Tabelle S3, utilizza il comando della CLI di esempio:

```
aws ec2 create-vpc-endpoint \  
  --vpc-id vpc-id \  
  --service-name com.amazonaws.aws-region.s3tables \  
  --subnet-ids subnet-1 subnet-2 \  
  --vpc-endpoint-type Interface \  
  --ip-address-type dualstack \  
  --dns-options "DnsRecordIpType=dualstack" \  
  --security-group-ids sg-id \  
  --region aws-region
```

Per ulteriori informazioni sulla creazione di endpoint VPC, consulta [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di VPC.

Se la tua rete supporta il protocollo IPv6 e desideri aggiornare il VPC per abilitarlo, puoi utilizzare il seguente comando della CLI:

```
aws ec2 modify-vpc-endpoint \  

```

```
--vpc-endpoint-id vpce-id \  
--ip-address-type dualstack \  
--dns-options "DnsRecordIpType=dualstack" \  
--region aws-region
```

Utilizzo delle condizioni delle policy degli endpoint VPC con le policy dei bucket table

È possibile utilizzare le chiavi di `aws:VpcSourceIp` condizione

`aws:SourceVpceaws:SourceVpc`, e in una policy del bucket della tabella per limitare l'accesso alle risorse del bucket della tabella da uno specifico endpoint VPC o VPC. Per ulteriori informazioni su queste chiavi di condizione, consulta le chiavi di contesto delle condizioni [AWS globali](#) nella IAM User Guide.

Quando utilizzi le [Iceberg REST API](#), S3 Tables invia richieste ad Amazon S3 per tuo conto per leggere e scrivere i metadati delle tabelle. Quando una richiesta Iceberg REST API viene effettuata tramite un endpoint VPC, il VPC di origine della richiesta iniziale non viene conservato nella tabella delle richieste di metadati ad Amazon S3. Se la tua policy table bucket limita l'accesso utilizzando queste chiavi di condizione, devi aggiungere anche una condizione per consentire queste richieste di metadati di tabella `aws:CalledVia` da parte di S3 Tables.

Il seguente esempio di policy bucket per tabelle nega tutte le azioni di S3 Tables a meno che la richiesta non provenga dall'endpoint VPC specificato o sia una richiesta effettuata dall'endpoint Amazon S3 Tables per tuo conto. Iceberg REST

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "RestrictToVPCe",  
      "Effect": "Deny",  
      "Principal": "*",  
      "Action": "s3tables:*",  
      "Resource": [  
        "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket",  
        "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket/*"  
      ],  
    },  
  ],  
}
```



```

        "Condition": {
            "StringNotEqualsIfExists": {
                "aws:SourceVpce": "vpce-1a2b3c4d",
                "aws:CalledViaLast": "s3tables.amazonaws.com"
            }
        }
    ]
}

```

Limitazione dell'accesso a Tabelle S3 all'interno della rete VPC

Analogamente alle policy basate sulle risorse, è possibile associare una policy degli endpoint all'endpoint VPC che controlla l'accesso a tabelle e bucket di tabelle. Nell'esempio seguente, la policy degli endpoint di interfaccia limita l'accesso solo a specifici bucket di tabelle.

JSON

```

{
    "Version": "2012-10-17",
    "Id": "Policy141511512309",
    "Statement": [
        {
            "Sid": "Access-to-specific-bucket-only",
            "Principal": "*",
            "Action": "s3tables:*",
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket",
                "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket/*"
            ]
        }
    ]
}

```

Considerazioni e limitazioni sulla sicurezza per Tabelle S3

Il seguente elenco descrive le funzioni e funzionalità di sicurezza e controllo degli accessi non supportate o limitate per Tabelle S3.

- Le policy di accesso pubblico non sono supportate. Gli utenti non possono modificare le policy di bucket o di tabella per consentire l'accesso pubblico.
- Gli URL prefirmati per l'accesso agli oggetti associati a una tabella non sono supportati.
- Le richieste effettuate tramite HTTP non sono supportate. Amazon S3 risponde automaticamente con un reindirizzamento HTTP per qualsiasi richiesta effettuata tramite HTTP per aggiornare le richieste a HTTPS.
- È necessario utilizzare AWS la versione 4 di Signature quando si effettuano richieste a un punto di accesso utilizzando le API REST.
- Le richieste effettuate tramite l'Internet Protocol versione 6 (IPv6) sono supportate solo per le azioni a livello di oggetto sugli endpoint di archiviazione delle tabelle e non per le azioni a livello di tabella e di bucket.
- Le policy di accesso dei bucket di tabelle e delle tabelle sono limitate a una dimensione di 20 KB.

Registrazione di log e monitoraggio per Tabelle S3

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di Tabelle Amazon S3. È consigliabile raccogliere i dati di monitoraggio da tutte le tabelle presenti nei bucket, così da facilitare il debug di eventuali guasti su più punti.

AWS fornisce diversi strumenti per monitorare le risorse di S3 Tables e rispondere a potenziali incidenti.

Amazon Alarms CloudWatch

Utilizzando gli CloudWatch allarmi Amazon, osservi una singola metrica in un periodo di tempo specificato. Se la metrica supera una determinata soglia, viene inviata una notifica a un argomento o a una policy di Amazon SNS. AWS Auto Scaling CloudWatch gli allarmi non richiamano azioni perché si trovano in uno stato particolare. È necessario invece cambiare lo stato e mantenerlo per un numero di periodi specificato. Per ulteriori informazioni, consulta [Metriche di monitoraggio con Amazon CloudWatch](#).

AWS CloudTrail Registri

CloudTrail fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon S3. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon S3, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#).

Argomenti

- [Registrazione con AWS CloudTrail per tabelle S3](#)
- [Metriche di monitoraggio con Amazon CloudWatch](#)

Registrazione con AWS CloudTrail per tabelle S3

Amazon S3 è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o servizio. AWS CloudTrail acquisisce tutte le chiamate API per Amazon S3 come eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon S3, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e dettagli aggiuntivi. Quando si verifica un'attività di evento supportata in Amazon S3, tale attività viene registrata in un CloudTrail evento. Puoi utilizzare AWS CloudTrail trail per registrare eventi di gestione ed eventi di dati per S3 Tables. Per ulteriori informazioni, consulta [Amazon S3 CloudTrail events](#) e [What is? AWS CloudTrail](#) nella Guida per l'AWS CloudTrail utente.

CloudTrail eventi di gestione per S3 Tables

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse dell'AWS account.

Per impostazione predefinita, CloudTrail registra gli eventi di gestione per le tabelle S3. Gli eventi eventsource di CloudTrail gestione per S3 Tables sono. `s3tables.amazonaws.com` Quando configuri il tuo AWS account, gli eventi di CloudTrail gestione sono abilitati per impostazione predefinita. Le seguenti azioni API vengono tracciate CloudTrail e registrate come eventi di gestione.

- [CreateNamespace](#)
- [CreateTable](#)
- [CreateTableBucket](#)
- [DeleteNamespace](#)

- [DeleteTable](#)
- [DeleteTableBucket](#)
- [DeleteTableBucketPolicy](#)
- [DeleteTablePolicy](#)
- [GetNamespace](#)
- [GetTable](#)
- [GetTableBucket](#)
- [GetTableBucketMaintenanceConfiguration](#)
- [GetTableBucketPolicy](#)
- [GetTableMaintenanceConfiguration](#)
- [GetTableMaintenanceJobStatus](#)
- [GetTableMetadataLocation](#)
- [GetTablePolicy](#)
- [ListNamespaces](#)
- [ListTableBuckets](#)
- [ListTables](#)
- [PutTableBucketMaintenanceConfiguration](#)
- [PutTableMaintenanceConfiguration](#)
- [PutBucketPolicy](#)
- [PutTablePolicy](#)
- [RenameTable](#)
- [UpdateTableMetadataLocation](#)

Per ulteriori informazioni sugli eventi di CloudTrail gestione, consulta [Registrazione degli eventi di gestione](#) nella Guida per l'AWS CloudTrail utente.

CloudTrail eventi di gestione per la manutenzione di S3 Tables

S3 registra le operazioni di manutenzione automatica come eventi di `TablesMaintenanceEvent` gestione in. CloudTrail Questi eventi si verificano durante operazioni come la compattazione e la scadenza delle snapshot. Per ulteriori informazioni sulla manutenzione delle tabelle S3, consulta [Manutenzione delle tabelle](#).

Come identificare gli eventi di manutenzione

È possibile identificare gli eventi di manutenzione di S3 Tables nei CloudTrail log in base ai seguenti valori di attributo:

- `eventSource: s3tables.amazonaws.com`
- `eventType: AwsServiceEvent`
- `eventName: TablesMaintenanceEvent`
- `userAgent: maintenance.s3tables.amazonaws.com`
- `activityType:`
 - `IcebergCompaction` (per la compattazione)
 - `IcebergSnapshotManagement` (per la scadenza delle snapshot)

Per un esempio di evento di manutenzione della compattazione, consulta [Esempio: file di CloudTrail registro per un evento di gestione della manutenzione della tabella](#).

CloudTrail eventi di dati per S3 Tables

Gli eventi sui dati forniscono informazioni sulle operazioni sulle risorse eseguite su o in una risorsa. Per impostazione predefinita, i CloudTrail percorsi non registrano gli eventi relativi ai dati, ma è possibile configurare i percorsi per registrare gli eventi relativi ai dati.

Quando registri gli eventi di dati per un trail in CloudTrail, scegli o specifichi il tipo di risorsa. Tabelle S3 ha due tipi di risorse: `AWS::S3Tables::Table` e `AWS::S3Tables::TableBucket`.

Vengono registrati i seguenti eventi relativi ai CloudTrail dati.

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CreateMultipartUpload](#)
- [GetObject](#)
- [HeadObject](#)
- [ListParts](#)
- [PutObject](#)
- [UploadPart](#)

Per ulteriori informazioni sugli eventi CloudTrail relativi ai dati, vedere [Registrazione degli eventi relativi ai dati](#) nella Guida per l'AWS CloudTrail utente.

Per ulteriori informazioni sugli CloudTrail eventi per S3 Tables, consulta i seguenti argomenti:

Argomenti

- [AWS CloudTrail esempi di file di registro degli eventi di dati per le tabelle S3](#)

AWS CloudTrail esempi di file di registro degli eventi di dati per le tabelle S3

Un file di AWS CloudTrail registro include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. Questo argomento fornisce file di registro di esempio per gli eventi di CloudTrail dati per le tabelle S3.

Argomenti

- [Esempio: file di CloudTrail registro per l'evento di GetObject dati](#)
- [Esempio: file di CloudTrail registro per un evento di gestione della manutenzione della tabella](#)
- [Esempio: file di CloudTrail registro per l'evento di dati PutObject](#)

Esempio: file di CloudTrail registro per l'evento di **GetObject** dati

L'esempio seguente mostra un esempio di file di CloudTrail registro che dimostra il funzionamento dell'[GetObjectAPI](#).

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::111122223333:user/myUserName",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "myUserName"
  },
  "eventTime": "2024-11-22T17:12:25Z",
  "eventSource": "s3tables.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "[aws-cli/2.18.5]",
```

```

    "requestParameters": {
      "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
      "key": "product-info.json"
    },
    "responseElements": null,
    "additionalEventData": {
      "SignatureVersion": "SigV4",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "bytesTransferredIn": 0,
      "AuthenticationMethod": "AuthHeader",
      "xAmzId2": "q6xhNJYmhg",
      "bytesTransferredOut": 28441
    },
    "requestID": "07D681123BD12AED",
    "eventID": "f2b287f3-0df1-1234-a2f4-c4bdfed47657",
    "readOnly": true,
    "resources": [{
      "accountId": "111122223333",
      "type": "AWS::S3Tables::TableBucket",
      "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket1"
    }, {
      "accountId": "111122223333",
      "type": "AWS::S3Tables::Table",
      "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-  
bucket/table/111aa1111-22bb-33cc-44dd-5555eee66ffff"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "444455556666",
    "eventCategory": "Data",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-  
east-1.amazonaws.com"
    }
  }
}

```

Esempio: file di CloudTrail registro per un evento di gestione della manutenzione della tabella

Di seguito è riportato un esempio di file di CloudTrail registro che dimostra un evento di manutenzione per la compattazione della tabella eseguito da S3 come parte della manutenzione automatica della tabella. Per ulteriori informazioni sugli eventi per la manutenzione delle tabelle, consulta [CloudTrail eventi di gestione per la manutenzione di S3 Tables](#)

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "maintenance.s3tables.amazonaws.com"
  },
  "eventTime": "2025-09-18T20:13:14Z",
  "eventSource": "s3tables.amazonaws.com",
  "eventName": "TablesMaintenanceEvent",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "maintenance.s3tables.amazonaws.com",
  "userAgent": "maintenance.s3tables.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "b8f96329-ef5c-32b5-94f6-eeed9061ea32",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::S3Tables::TableBucket",
      "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket"
    },
    {
      "accountId": "111122223333",
      "type": "AWS::S3Tables::Table",
      "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket/table/7ff7750e-23b3-481e-a90a-7d87d423d336"
    }
  ],
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "sharedEventID": "62a57826-a66e-479b-befa-0e65663ee9e8",
  "serviceEventDetails": {
    "activityType": "icebergCompaction"
  },
}
```



```
"eventCategory": "Management"
}
```

Esempio: file di CloudTrail registro per l'evento di dati **PutObject**

L'esempio seguente mostra un esempio di file di CloudTrail registro che dimostra il funzionamento dell'[PutObjectAPI](#).

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::444455556666:user/"myUserName",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "myUserName"
  },
  "eventTime": "2024-11-22T17:12:25Z",
  "eventSource": "s3tables.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "[aws-cli/2.18.5]",
  "requestParameters": {
    "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
    "key": "product-info.json"
  },
  "responseElements": {
    "x-amz-server-side-encryption": "AES256",
    "x-amz-version-id": "13zAFMdccAjt3MWd6ehxgCCCDRdkAKDw"
  },
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "bytesTransferredIn": 28441,
    "AuthenticationMethod": "AuthHeader",
    "xAmzId2": "q6xhCJYmhg",
    "bytesTransferredOut": 0
  },
  "requestID": "28d2faaf-1234-4649-997d-EXAMPLE72818",
```

```

    "eventID": "694d604a-d190-1234-0dd1-EXAMPLEe20c1",
    "readOnly": false,
    "resources": [{
      "accountId": "444455556666",
      "type": "AWS::S3Tables::TableBucket",
      "ARN": "arn:aws:s3tables:us-east-1:444455556666:bucket/amzn-s3-demo-
bucket1"
    }, {
      "accountId": "444455556666",
      "type": "AWS::S3Tables::Table",
      "ARN": "arn:aws:s3tables:us-east-1:444455556666:bucket/amzn-s3-demo-
bucket1/table/b89ec883-b1d9-4b37-9cd7-b86f590123f4"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
    }
  }
}

```

Metriche di monitoraggio con Amazon CloudWatch

Puoi utilizzare le CloudWatch metriche di Amazon per tracciare le prestazioni, rilevare anomalie e monitorare lo stato operativo delle tabelle. Esistono diversi set di CloudWatch metriche che puoi utilizzare con S3 Tables.

Metriche di archiviazione giornaliere per tabelle e bucket di tabelle

Monitora la quantità di dati archiviati nelle tabelle e nei bucket di tabelle, inclusi la dimensione totale in byte e il numero di file. Queste metriche tengono traccia dei byte di archiviazione totali per livello di accesso e del numero di file a livello di tabella, bucket della tabella e namespace. Le metriche di archiviazione per Tabelle S3 vengono riportate una volta al giorno e sono disponibili per tutti i clienti senza costi aggiuntivi.

Metriche di manutenzione delle tabelle

Monitora le operazioni di manutenzione automatizzate eseguite da Amazon S3 sulle tue tabelle, come la compattazione. Queste metriche tengono traccia del numero di byte e file elaborati

durante le attività di manutenzione. Queste metriche di manutenzione per Tabelle S3 vengono riportate una volta al giorno e sono disponibili per tutti i clienti senza costi aggiuntivi.

Metriche di richiesta

Puoi monitorare le richieste di Tabelle S3 per identificare rapidamente i problemi operativi e intraprendere le operazioni appropriate. Queste CloudWatch metriche possono essere abilitate opzionalmente per singoli bucket di tabelle. Le metriche delle richieste per le tabelle S3 vengono segnalate una volta al minuto e vengono fatturate alla stessa tariffa delle metriche personalizzate. CloudWatch Le metriche di richiesta includono:

- numero delle operazioni del piano dati (GET, PUT, HEAD, POST)
- byte trasferiti
- misurazioni della latenza
- percentuali di errore

Note

Best-effort CloudWatch consegna delle metriche

CloudWatch le metriche vengono fornite con il massimo impegno possibile. La maggior parte delle richieste per un oggetto Amazon S3 con metriche di richiesta comportano l'invio di un punto dati a CloudWatch

La completezza e la tempestività dei parametri non è garantita. È possibile che il data point per una richiesta specifica venga restituito con un timestamp successivo a quello del momento effettivo di elaborazione della richiesta. Il data point potrebbe subire un ritardo di un minuto prima di essere disponibile oppure potrebbe non essere consegnato affatto. CloudWatch le metriche relative alle richieste ti danno un'idea della natura del traffico diretto verso il tuo bucket in tempo quasi reale, ma non intendono essere un resoconto completo di tutte le richieste. Dalla natura best-effort di questa funzione deriva che i report disponibili nella dashboard di gestione dei costi e della fatturazione potrebbero includere una o più richieste di accesso che non compaiono nelle metriche del bucket.

Metriche e dimensioni

Le metriche e le dimensioni di storage che S3 Tables invia ad Amazon CloudWatch sono elencate nelle tabelle seguenti.

 Note**Best-effort CloudWatch consegna delle metriche**

CloudWatch le metriche vengono fornite con il massimo impegno possibile. La maggior parte delle richieste per un oggetto Amazon S3 con metriche di richiesta comportano l'invio di un punto dati a CloudWatch.

La completezza e la tempestività dei parametri non è garantita. È possibile che il data point per una richiesta specifica venga restituito con un timestamp successivo a quello del momento effettivo di elaborazione della richiesta. Il data point potrebbe subire un ritardo di un minuto prima di essere disponibile oppure potrebbe non essere consegnato affatto. CloudWatch le metriche relative alle richieste ti danno un'idea della natura del traffico diretto verso il tuo bucket in tempo quasi reale, ma non intendono essere un resoconto completo di tutte le richieste. Dalla natura best-effort di questa funzione deriva che i report disponibili nella dashboard di gestione dei costi e della fatturazione potrebbero includere una o più richieste di accesso che non compaiono nelle metriche del bucket.

Metriche di archiviazione giornaliere per i bucket da tavolo in CloudWatch

Il AWS/S3/Tables namespace include le seguenti metriche di archiviazione giornaliere, disponibili senza costi aggiuntivi. È possibile filtrare queste metriche per nome del bucket di tabelle, della tabella o del namespace.

Metriche di archiviazione giornaliere

Nome parametro	Description	unità	Statistiche	Granularity (Granularità)
Archiviazione dei bucket totale	La quantità di archiviazione in byte utilizzata da tutte le tabelle in un bucket di tabelle	Byte	Somma	Giornaliero
Numero di file totale	Il numero totale di tutti i file archiviati in un bucket di tabelle	Conteggio	Somma	Giornaliero

Metriche di manutenzione delle tabelle

Il `AWS/S3/Tables` namespace include le seguenti metriche di manutenzione della tabella, disponibili senza costi aggiuntivi. È possibile filtrare queste metriche per nome del bucket di tabelle, della tabella o del namespace.

Metriche di manutenzione delle tabelle

Nome parametro	Description	unità	Statistiche	Granularity (Granularità)
CompactionBytesProcessed	Il numero di byte elaborati durante le operazioni di compattazione delle tabelle	Byte	Somma	Giornaliero
CompactionObjectsCount	Il numero di oggetti elaborati durante le operazioni di compattazione delle tabelle	Conteggio	Somma	Giornaliero

Richiedi le metriche per tabelle e bucket di tabelle in CloudWatch

Il `AWS/S3/Tables` namespace include le seguenti metriche di richiesta, fatturate alla stessa tariffa delle metriche personalizzate. CloudWatch È possibile filtrare queste metriche per nome del bucket di tabelle, della tabella o del namespace.

Note

Le metriche delle richieste vengono pubblicate solo quando tutte e tre le dimensioni (`TableBucketName`, `Namespace`) possono essere risolte. `TableName` Le richieste destinate a una tabella o a un namespace che non esiste non vengono visualizzate nelle CloudWatch metriche delle richieste. Per monitorare queste richieste, usa `AWS CloudTrail`

Metriche di richiesta

Nome parametro	Description	unità	Statistiche	Granularity (Granularità)
Numero delle richieste totali	Il numero totale di richieste HTTP effettuate a un bucket di tabella, indipendentemente dal tipo. Questa metrica non include <code>GetTableMetadataLocation</code> né <code>UpdateTableMetadataLocation</code> richieste.	Conteggio	Somma	1 minuto
Numero delle richieste GET	Il numero di richieste HTTP GET effettuate per recuperare e oggetti dalle tabelle. Questa metrica non include <code>GetTableMetadataLocation</code> le richieste.	Conteggio	Somma	1 minuto
Numero delle richieste PUT	Il numero di richieste HTTP PUT effettuate per aggiungere oggetti alle tabelle. Questa metrica non include <code>UpdateTableMetadataLocation</code> le richieste.	Conteggio	Somma	1 minuto
Numero delle richieste HEAD	Il numero di richieste HTTP HEAD effettuate per recuperare e i metadati dalle tabelle.	Conteggio	Somma	1 minuto
Le richieste di post contano	Il numero di richieste HTTP POST effettuate alle tabelle.	Conteggio	Somma	1 minuto
<code>UpdateTableMetadataLocation</code>	Il numero di <code>UpdateTableMetadataLocation</code> richieste fatte a un bucket da tavolo. Questa metrica non	Conteggio	Somma	1 minuto

Nome parametro	Description	unità	Statistiche	Granularity (Granularità)
conteggio delle richieste	è inclusa in Put requests count o. All requests count			
GetTableMetadataLocation le richieste contano	Il numero di GetTableMetadataLocation richieste fatte a un bucket da tavolo. Questa metrica non è inclusa in Get requests count o. All requests count	Conteggio	Somma	1 minuto
BytesDownloaded	Il numero di byte scaricati per le richieste di tabella.	Byte	Somma	1 minuto
BytesUploaded	Il numero di byte caricati per le richieste di tabella.	Byte	Somma	1 minuto
4xxErrors	Il numero di codici di stato di errore del client HTTP 4xx restituiti.	Conteggio	Somma	1 minuto
5xxErrors	Il numero di codici di stato di errore del server HTTP 5xx restituiti.	Conteggio	Somma	1 minuto
FirstByte Latency	Il tempo per richiesta che intercorre tra la ricezione della richiesta completa e il momento in cui la risposta inizia a essere restituita.	Millisecondi	Somma	1 minuto
TotalRequestLatency	Il tempo trascorso per richiesta dal primo byte ricevuto all'ultimo byte inviato.	Millisecondi	Somma	1 minuto

Dimensioni delle tabelle S3 in CloudWatch

Le dimensioni elencate di seguito vengono utilizzate per filtrare le metriche di Tabelle S3.

Dimensioni di Tabelle S3

Nome della dimensione	Description	Valore di esempio
TableBucketName	Il nome del bucket di tabelle Amazon S3	my-table-bucket
Namespace	Il namespace all'interno del bucket di tabelle contenente una o più tabelle	my-department
TableName	Il nome di una tabella specifica all'interno di un namespace	transactions

Accesso alle metriche CloudWatch

Puoi monitorare le metriche di S3 Tables utilizzando la CloudWatch console, l'API o l'API AWS CLI. CloudWatch Questa sezione spiega come accedere alle metriche utilizzando i vari metodi previsti.

Utilizzo della console S3

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nell'elenco di bucket, seleziona il nome del bucket contenente le tabelle di cui desideri visualizzare le metriche.
4. Seleziona la scheda Parametri.
5. Scegli il riquadro Visualizza CloudWatch in qualsiasi metrica per accedere alla CloudWatch console e visualizzare le metriche disponibili nel namespace. AWS/S3/Tables

Utilizzo di AWS CLI

Per elencare le metriche per le tabelle S3 utilizzando il AWS CLI, usa il `list-metrics` comando con il parametro impostato su: `--namespace AWS/S3/Tables`


```
aws cloudwatch list-metrics --namespace AWS/S3/Tables
```

Per ottenere statistiche per una metrica specifica di Tabelle S3, utilizza il comando `get-metric-statistics`. Ad esempio:

```
aws cloudwatch get-metric-statistics \  
--namespace AWS/S3/Tables \  
--metric-name TotalBucketStorage \  
--dimensions Name=TableBucketName,Value=MyTableBucket \  
--start-time 2025-03-01T00:00:00 \  
--end-time 2025-03-02T00:00:00 \  
--period 86400 \  
--statistics Average
```

Best practice

- Quando recuperi le metriche, imposta il valore del periodo in base alla granularità della metrica. Per le metriche giornaliere (come le metriche di archiviazione), utilizza 86.400 secondi (24 ore). Per le metriche a livello di minuto (come le metriche di richiesta), utilizza 60 secondi.
- Utilizza le dimensioni in modo appropriato per filtrare le metriche in base all'ambito desiderato (bucket di tabelle, namespace o livello di tabella individuale).
- Prendi in considerazione la possibilità di utilizzare la matematica metrica per creare metriche derivate che rispondano meglio alle tue esigenze di monitoraggio.

Risorse correlate

- [Amazon Concepts CloudWatch](#)
- [Utilizzo di Amazon CloudWatch Dashboards](#)

Gestione delle metriche CloudWatch

Per impostazione predefinita, le metriche di archiviazione sono abilitate per tutte le tabelle e i bucket di Tabelle Amazon S3. Puoi abilitare o disabilitare le metriche di richiesta aggiuntive tramite la console, AWS Command Line Interface (AWS CLI) o AWS gli SDK.

Prerequisiti

- Richiede l'autorizzazione IAM `s3table:PutTableBucketMetricsConfiguration`

 Note

Le metriche di richiesta di S3 Tables vengono fatturate alla stessa tariffa delle metriche personalizzate. CloudWatch

Utilizzo di AWS Console di gestione

Per abilitare o disabilitare metriche aggiuntive

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Bucket di tabelle.
3. Nell'elenco di bucket, seleziona il nome del bucket di tabelle che contiene le tabelle di cui si desidera richiedere le metriche.
4. Seleziona la scheda Parametri.
5. Dal pannello delle metriche di richiesta, seleziona Modifica.
6. Seleziona Abilitato o Disabilitato, quindi seleziona Salva modifiche.

Utilizzo di AWS CLI

Questi esempi mostrano come abilitare o disabilitare le metriche delle richieste per i bucket di tabelle utilizzando AWS CLI. Per utilizzare questi comandi, sostituire *user input placeholders* con le proprie informazioni.

Example: Per abilitare le metriche di richiesta per un bucket di tabelle:

```
aws s3tables put-table-bucket-metrics-configuration \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-
bucket
```

Example: Per disabilitare le metriche di richiesta per un bucket di tabelle:

```
aws s3tables delete-table-bucket-metrics-configuration \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-
bucket
```

Utilizzo di S3 Vectors e bucket vettoriali

Che cos'è Amazon S3 Vectors?

Amazon S3 Vectors offre storage vettoriale personalizzato e ottimizzato in termini di costi per agenti AI, inferenza, RAG e ricerca semantica. S3 Vectors è progettato per fornire la stessa elasticità, durata e disponibilità di Amazon S3 e offre una latenza inferiore al secondo per le query poco frequenti e fino a 100 millisecondi per le query più frequenti. Avrai a disposizione un set dedicato di operazioni API per archiviare, accedere e interrogare dati vettoriali senza dover fornire alcuna infrastruttura. S3 Vectors è composto da diversi componenti chiave che funzionano insieme:

- **Bucket di vettori:** un nuovo tipo di bucket creato appositamente per archiviare e sottoporre a query i vettori.
- **Indici vettoriali:** in un bucket vettoriale, puoi organizzare i dati vettoriali all'interno di indici vettoriali. Esegui query di somiglianza sui dati vettoriali all'interno di indici vettoriali.
- **Vettori:** archivi i vettori nell'indice vettoriale. Per le applicazioni di ricerca per similarità e di intelligenza artificiale, i vettori vengono creati come embedding vettoriali, ossia rappresentazioni numeriche che preservano le relazioni semantiche tra i contenuti (come testo, immagini o audio) in modo che elementi simili siano posizionati vicini tra loro. S3 Vectors può eseguire ricerche per similarità basate sul significato semantico anziché sulla corrispondenza esatta confrontando matematicamente quanto i vettori sono vicini tra loro. Quando si aggiungono dati vettoriali a un indice vettoriale, è anche possibile collegare i metadati per future query di filtro basate su una serie di condizioni (ad esempio timestamp, categorie e preferenze dell'utente).

Le scritture su S3 Vectors sono fortemente coerenti, il che significa che è possibile immediatamente accedere ai dati aggiunti più di recente. Man mano che si scrivono, aggiornano ed eliminano i vettori nel tempo, S3 Vectors ottimizza automaticamente i dati vettoriali per ottenere il miglior rapporto prezzo/prestazioni possibile per l'archiviazione vettoriale, anche se i set di dati scalano e si evolvono. È possibile controllare l'accesso ai dati vettoriali con i meccanismi di controllo degli accessi esistenti di Amazon S3, incluse le policy di bucket e IAM. Per ulteriori informazioni sui limiti degli indici vettoriali per bucket e sui limiti degli indici vettoriali per indice, consulta [Limitazioni e restrizioni](#).

Casi d'uso: ricerche per similarità su set di dati di grandi dimensioni

Le ricerche per similarità consentono di trovare elementi concettualmente correlati tra loro in base alle rispettive rappresentazioni vettoriali, anziché alla corrispondenza esatta delle parole chiave. Queste ricerche individuano contenuti con significati o caratteristiche simili, anche quando le parole o gli elementi visivi esatti sono diversi.

I casi d'uso più comuni della ricerca per similarità con S3 Vectors sono:

- Diagnostica per immagini: individua similarità tra milioni di immagini mediche per facilitare la diagnosi e la scelta del trattamento
- Violazione del copyright: individua contenuti potenzialmente derivati in grandi librerie multimediali
- Deduplicazione delle immagini: rileva e rimuovi immagini duplicate o pressoché duplicate da raccolte di immagini di grandi dimensioni
- Comprensione dei video: cerca scene o contenuti specifici all'interno di risorse video
- Ricerca di documenti aziendali: abilita la ricerca semantica dei documenti aziendali per trovare informazioni pertinenti in base al significato
- Personalizzazione: fornisci consigli personalizzati individuando articoli simili

È consigliabile utilizzare S3 Vectors per creare applicazioni di ricerca vettoriale e di IA agentica convenienti con tempi di ricerca inferiori al secondo. Con i bucket vettoriali, paghi solo per ciò che usi e puoi risparmiare sui costi di caricamento, archiviazione e query degli embedding vettoriali. Per ulteriori informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Funzionalità di S3 Vectors

Archiviazione appositamente progettata per vettori

S3 Vectors è la prima archiviazione di oggetti creata appositamente nel cloud per archiviare e sottoporre a query i vettori. I bucket vettoriali sono progettati per fornire un'archiviazione conveniente, elastica e durevole per i dati vettoriali.

Gli embedding vettoriali trasformano il modo in cui i clienti utilizzano e recuperano i dati non strutturati, rilevando similarità tra immagini mediche, individuando anomalie in migliaia di ore di riprese video, navigando attraverso ampie codebase e identificando la giurisprudenza più rilevante per una determinata questione legale. Queste applicazioni emergenti si combinano con modelli di

embedding per codificare il significato semantico dei dati (ad esempio testo, immagini, video, codice) come embedding vettoriali numerici.

In un bucket vettoriale, è possibile organizzare i dati vettoriali all'interno di indici vettoriali, senza dover predisporre l'infrastruttura. Man mano che si scrivono, aggiornano ed eliminano i vettori nel tempo, S3 Vectors ottimizza automaticamente i dati vettoriali per ottenere il miglior rapporto prezzo/prestazioni possibile per l'archiviazione vettoriale, anche se i set di dati scalano e si evolvono. Per ulteriori informazioni sui limiti degli indici vettoriali per bucket e sui limiti degli indici vettoriali per indice, consulta [Limitazioni e restrizioni](#).

Esecuzione di query di somiglianza

Con S3 Vectors, puoi eseguire query per trovare i vettori più simili a un vettore di query, con tempi di risposta inferiori al secondo per le query poco frequenti e fino a 100 millisecondi per le query più frequenti. S3 Vectors è ideale per carichi di lavoro in cui le query sono meno frequenti.

Filtro dei metadati

È possibile collegare i metadati (ad esempio anno, autore, genere e posizione) come coppie chiave-valore ai vettori. Per impostazione predefinita, tutti i metadati sono filtrabili a meno che non vengano esplicitamente specificati come non filtrabili. È possibile utilizzare metadati filtrabili per filtrare i risultati delle query in base a attributi specifici, migliorando la pertinenza delle query. Gli indici vettoriali supportano i metadati di tipo stringa, numerico, booleano ed elenco. Per ulteriori informazioni sui limiti di dimensione dei metadati per vettore e sui limiti di dimensione dei metadati filtrabili per vettore, consulta [Limitazioni e restrizioni](#).

Gestione degli accessi e sicurezza

Puoi gestire l'accesso alle risorse in bucket vettoriali con IAM e [Service Control Policies](#) in Organizations AWS. S3 Vectors utilizza un namespace di servizio diverso dal namespace `s3vectors` di Amazon S3. Pertanto, è possibile progettare policy appositamente per il servizio S3 Vectors e le relative risorse. È possibile progettare policy per fornire l'accesso a singoli indici vettoriali, a tutti gli indici vettoriali all'interno di un bucket vettoriale o a tutti i bucket vettoriali in un account. Tutte le impostazioni di Blocco dell'accesso pubblico Amazon S3 sono sempre abilitate per i bucket vettoriali e non possono essere disabilitate.

Integrazione con i servizi AWS

S3 Vectors si integra con altri AWS servizi per migliorare le capacità di elaborazione vettoriale:

- [Amazon OpenSearch Service](#): ottimizza i costi di storage vettoriale continuando a utilizzare le operazioni OpenSearch API. È ideale per carichi di lavoro che richiedono funzionalità di ricerca avanzata come ricerca ibrida, aggregazioni, filtri avanzati e ricerca con facet. Puoi anche esportare uno snapshot di un indice vettoriale S3 in Amazon OpenSearch Serverless per una ricerca vettoriale con QPS elevato e bassa latenza.
- [Knowledge Base per Amazon Bedrock](#): seleziona un indice vettoriale in S3 Vectors come archivio vettoriale per risparmiare sui costi di archiviazione per le applicazioni di generazione potenziata da recupero dati (RAG).
- [Amazon Bedrock in SageMaker Unified Studio](#): sviluppa e testa basi di conoscenza utilizzando S3 Vectors come archivio vettoriale.

Tutorial: Nozioni di base su S3 Vectors

In questo tutorial, crei un bucket vettoriale S3 e un indice vettoriale in una console Regione AWS Amazon S3. Successivamente, utilizzi un modello di embedding Amazon Bedrock per generare embedding vettoriali dei dati e archivarli nell'indice vettoriale per eseguire ricerche semantiche.

Per iniziare, crea un AWS account se non ne hai già uno. Per ulteriori informazioni sull'impostazione con un account, consulta [Nozioni di base su Amazon S3](#).

Argomenti

- [Fase 1. Creazione di un bucket vettoriale con la console](#)
- [Fase 2. Creazione di un indice vettoriale in un bucket vettoriale con la console](#)
- [Fase 3. Inserimento di vettori in un indice vettoriale con SDK per Python \(Boto3\)](#)
- [Passaggio 4. Query sui vettori in un indice vettoriale con SDK per Python \(Boto3\)](#)
- [\(Facoltativo\) Automazione della creazione di embedding vettoriali con S3 Vectors Embed CLI](#)
- [\(Facoltativo\) Integrazione di S3 Vectors con Knowledge Base per Amazon Bedrock](#)
- [\(Facoltativo\) Integra i vettori S3 con Amazon OpenSearch](#)

Fase 1. Creazione di un bucket vettoriale con la console

I bucket vettoriali S3 sono un tipo di bucket Amazon S3 progettato appositamente per poter archiviare e sottoporre a query i vettori. Per scrivere e sottoporre a query i dati vettoriali si utilizzano operazioni API dedicate. È possibile controllare l'accesso ai dati vettoriali con meccanismi di controllo degli accessi come le policy basate su identità IAM e le policy basate su risorse.

In questa fase utilizzi la console Amazon S3 per creare il tuo primo bucket vettoriale. Per altri metodi per creare un bucket vettoriale, consulta [Creazione di un bucket vettoriale](#).

Come creare un bucket vettoriale

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di vettori.
3. Nella pagina Bucket di vettori scegli Crea bucket di vettore.
4. Nella pagina Crea bucket di vettore inserisci un nome nel campo Nome del bucket di vettore. In questo tutorial, lo usiamo *media-embeddings* come nome vettoriale del bucket. I nomi dei bucket vettoriali devono essere composti da un numero di caratteri compreso tra 3 e 63 ed essere univoci all'interno di una Regione AWS. I caratteri validi sono lettere minuscole (a-z), numeri (0-9) e trattini (-).

Note

Il nome del bucket vettoriale non può essere cambiato dopo la creazione del bucket.

5. In Crittografia scegli Specifica il tipo di crittografia. Hai la possibilità di specificare il tipo di crittografia come crittografia lato server con AWS Key Management Service chiavi (SSE-KMS) o la crittografia lato server predefinita con chiavi gestite Amazon S3 (SSE-S3). In questo tutorial scegli Crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3). Per ulteriori informazioni sull'impostazione della configurazione della crittografia per i bucket vettoriali, consulta [Protezione e crittografia dei dati in S3 Vectors](#).

Note

Il tipo di crittografia non può essere cambiato dopo la creazione del bucket vettoriale.

6. In Tag (facoltativo), puoi aggiungere tag come coppie chiave-valore per organizzare e specificare le autorizzazioni per i tuoi bucket vettoriali. Immettere una chiave e un valore. Per aggiungere un altro tag, scegliere Add Tag (Aggiungi tag). Puoi inserire fino a 50 tag per un bucket vettoriale. Per ulteriori informazioni, consulta [Utilizzo di tag con bucket vettoriali S3](#).
7. Scegli Crea bucket di vettore.

Fase 2. Creazione di un indice vettoriale in un bucket vettoriale con la console

Note

Scegli con attenzione i parametri di configurazione dell'indice vettoriale. Dopo aver creato un indice vettoriale, non è possibile aggiornare il nome dell'indice vettoriale, la dimensione, la metrica della distanza o le chiavi di metadati non filtrabili. Per modificare uno di questi valori, occorre creare un nuovo indice vettoriale.

In questa fase crei un indice vettoriale nel bucket vettoriale. L'indice vettoriale viene utilizzato per archiviare e sottoporre a query gli embedding vettoriali. Per ulteriori informazioni sugli indici vettoriali, consulta [Indici vettoriali](#).

Come creare un indice vettoriale

1. Vai al bucket vettoriale appena creato nell'elenco Bucket di vettori sulla console Amazon S3.
2. Scegli Crea indice di vettore.
3. Nella pagina Crea indice di vettore, inserisci un nome nel campo Nome dell'indice di vettore. In questo tutorial, usiamo *movies* come nome dell'indice vettoriale.

I nomi degli indici vettoriale devono essere composti da un numero di caratteri compreso tra 3 e 63 ed essere univoci all'interno del bucket vettoriale. I caratteri validi sono lettere minuscole (a-z), numeri (0-9), trattini (-) e punti (.).

Il nome dell'indice vettoriale non può essere cambiato dopo la creazione dell'indice.

4. In Dimensione, specifica un valore numerico compreso tra 1 e 4.096 che determini quanti numeri saranno presenti in ogni vettore generato dal modello di embedding vettoriale. I modelli di embedding sono specifici modelli di machine learning (ML) che convertono i dati (ad esempio testo o immagini) in vettori numerici. I modelli di embedding in genere producono output di dimensioni comprese tra 500 e 2000, con ogni dimensione rappresentata da un numero in virgola mobile. In questo tutorial utilizzi il modello di embedding Titan Text v2 di Amazon Bedrock. Questo modello di embedding utilizza vettori a 1024 dimensioni per impostazione predefinita, quindi imposti la dimensione per l'indice vettoriale su 1024.

Il valore della dimensione non può essere cambiato dopo la creazione dell'indice. Specifica con attenzione il valore della dimensione in base alle raccomandazioni del modello di embedding.

5. In Metrica della distanza, scegli Coseno (che misura la somiglianza angolare) o Euclideo (che misura la distanza in linea retta) come metrica della distanza per definire in che modo viene calcolata la somiglianza tra i vettori durante le query. In questo tutorial scegli Coseno.

La metrica della distanza non può essere cambiata dopo la creazione dell'indice. Scegli con attenzione la metrica della distanza in base alle raccomandazioni del modello di embedding.

6. In Impostazioni aggiuntive (facoltativo), è possibile specificare le chiavi di metadati non filtrabili per archiviare informazioni supplementari insieme agli embedding vettoriali.

Note

Puoi collegare a ciascun vettore i metadati filtrabili come coppie chiave-valore quando inserisci i dati vettoriali dopo aver creato l'indice. Per impostazione predefinita, tutte le chiavi di metadati collegate ai vettori sono filtrabili e possono essere utilizzate come filtri in una query di somiglianza. Solo le chiavi di metadati specificate come non filtrabili durante la creazione dell'indice vettoriale non possono essere utilizzate come filtro.

Ogni chiave di metadati non filtrabili deve essere composta da un numero di caratteri compreso tra 1 e 63 ed essere univoca all'interno dell'indice vettoriale. Queste chiavi sono utili per archiviare informazioni di riferimento che non è necessario filtrare durante le query di somiglianza. Ad esempio, quando utilizzi gli embedding di testo, potresti voler conservare blocchi di testo originali a scopo di riferimento. In questo tutorial aggiungi una chiave di metadati non filtrabili denominata `source_text` per archiviare i dati di testo per cui desideri creare embedding vettoriali.

Non è possibile aggiornare le chiavi di metadati non filtrabili dopo la creazione dell'indice. Pianifica con attenzione la struttura dei metadati.

7. In Crittografia scegli Specifica il tipo di crittografia. Hai la possibilità di utilizzare le impostazioni di crittografia a livello di bucket o sovrascrivere le impostazioni di crittografia per l'indice vettoriale. Se sovrascrivi le impostazioni a livello di bucket, hai la possibilità di specificare il tipo di crittografia per l'indice vettoriale come crittografia lato server con chiavi del servizio di gestione delle AWS chiavi (SSE-KMS) o crittografia lato server con chiavi gestite Amazon S3 (SSE-S3). In questo tutorial, scegliamo di utilizzare le impostazioni del bucket per la crittografia. Per ulteriori

informazioni sull'impostazione della configurazione di crittografia per bucket e indici vettoriali, consulta [Protezione e crittografia dei dati in S3 Vectors](#)

8. In Tag (facoltativo), puoi aggiungere tag come coppie chiave-valore per monitorare e organizzare i costi degli indici vettoriali utilizzando AWS Billing and Cost Management. Immettere una chiave e un valore. Per aggiungere un altro tag, scegliere Add Tag (Aggiungi tag). Puoi inserire fino a 50 tag per un indice vettoriale. Per ulteriori informazioni, consulta [Utilizzo di tag con bucket vettoriali S3](#).
9. Scegli Crea indice di vettore.

Verifica che il nuovo indice vettoriale sia presente nel bucket.

Fase 3. Inserimento di vettori in un indice vettoriale con SDK per Python (Boto3)

Per inserire, elencare e interrogare i vettori, usa o l' AWS SDKsAPI AWS CLI REST di Amazon S3.

Questo passaggio consiste nell'inserire incorporamenti vettoriali nell'indice vettoriale con l'operazione API. [PutVectors](#)

Dovrai innanzitutto generare embedding vettoriali utilizzando il modello di embedding desiderato. Se utilizzi Amazon Bedrock, genera incorporamenti utilizzando l'operazione [InvokeModelAPI](#) per specificare il tuo modello di incorporamento preferito. In alternativa, per generare e inserire embedding vettoriali con un singolo comando, consulta [\(Facoltativo\) Automazione della creazione di embedding vettoriali con S3 Vectors Embed CLI](#).

Il codice di esempio seguente genera incorporamenti vettoriali a 1024 dimensioni con il modello Titan Text Embeddings V2 di Amazon Bedrock utilizzando e li memorizza nel tuo indice vettoriale utilizzando AWS SDK per Python (Boto3) l'API. PutVectors Insieme a ciascun vettore, colleghi coppie chiave-valore come metadati filtrabili. Inoltre, utilizziamo una chiave di metadati non filtrabile `source_text` denominata per preservare il testo originale da cui deriva ogni vettore. Per massimizzare il throughput delle richieste e ottimizzarne la velocità e l'efficienza, è consigliabile inserire ed eliminare i vettori in batch. Per ulteriori informazioni, consulta [Best practice per S3 Vectors](#).

```
# Populate a vector index with embeddings from Amazon Titan Text Embeddings V2.
import boto3
import json
```

```
# Create Bedrock Runtime and S3 Vectors clients in the AWS Region of your choice.
bedrock = boto3.client("bedrock-runtime", region_name="us-west-2")
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

# Texts to convert to embeddings.
texts = [
    "Star Wars: A farm boy joins rebels to fight an evil empire in space",
    "Jurassic Park: Scientists create dinosaurs in a theme park that goes wrong",
    "Finding Nemo: A father fish searches the ocean to find his lost son"
]

# Generate vector embeddings.
embeddings = []
for text in texts:
    response = bedrock.invoke_model(
        modelId="amazon.titan-embed-text-v2:0",
        body=json.dumps({"inputText": text})
    )

    # Extract embedding from response.
    response_body = json.loads(response["body"].read())
    embeddings.append(response_body["embedding"])

# Write embeddings into vector index with metadata.
s3vectors.put_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    vectors=[
        {
            "key": "Star Wars",
            "data": {"float32": embeddings[0]},
            "metadata": {"source_text": texts[0], "genre": "scifi"}
        },
        {
            "key": "Jurassic Park",
            "data": {"float32": embeddings[1]},
            "metadata": {"source_text": texts[1], "genre": "scifi"}
        },
        {
            "key": "Finding Nemo",
            "data": {"float32": embeddings[2]},
            "metadata": {"source_text": texts[2], "genre": "family"}
        }
    ]
]
```

>

Passaggio 4. Query sui vettori in un indice vettoriale con SDK per Python (Boto3)

Dopo aver archiviato gli incorporamenti dei vettori nell'indice vettoriale, puoi eseguire una ricerca di similarità utilizzando l'operazione API. [QueryVectors](#)

Dovrai innanzitutto generare gli embedding vettoriali delle query utilizzando lo stesso modello di embedding utilizzato durante l'inserimento in [Fase 3. Inserimento di vettori in un indice vettoriale con SDK per Python \(Boto3\)](#). In questo tutorial utilizzi il modello Embedding di testo Amazon V2 di Amazon Bedrock tramite SDK per Python (Boto3).

Puoi eseguire una ricerca per similarità per ottenere i vettori corrispondenti più simili. In una ricerca per similarità, è possibile facoltativamente filtrare utilizzando chiavi di metadati per limitare i risultati in base a criteri specifici pur mantenendo la pertinenza semantica.

```
# Query a vector index with an embedding from Amazon Titan Text Embeddings V2.
import boto3
import json

# Create Bedrock Runtime and S3 Vectors clients in the AWS Region of your choice.
bedrock = boto3.client("bedrock-runtime", region_name="us-west-2")
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

# Query text to convert to an embedding.
input_text = "adventures in space"

# Generate the vector embedding.
response = bedrock.invoke_model(
    modelId="amazon.titan-embed-text-v2:0",
    body=json.dumps({"inputText": input_text})
)

# Extract embedding from response.
model_response = json.loads(response["body"].read())
embedding = model_response["embedding"]

# Query vector index.
response = s3vectors.query_vectors(
    vectorBucketName="media-embeddings",
```

```
    indexName="movies",
    queryVector={"float32": embedding},
    topK=3,
    returnDistance=True,
    returnMetadata=True
)
print(json.dumps(response["vectors"], indent=2))

# Query vector index with a metadata filter.
response = s3vectors.query_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=3,
    filter={"genre": "scifi"},
    returnDistance=True,
    returnMetadata=True
)
print(json.dumps(response["vectors"], indent=2))
```

(Facoltativo) Automazione della creazione di embedding vettoriali con S3 Vectors Embed CLI

La CLI di Amazon S3 Vectors Embed è uno strumento a riga di comando standalone che semplifica il processo di utilizzo degli embedding vettoriali in S3 Vectors. Con singoli comandi, puoi creare embedding vettoriali per i dati utilizzando Amazon Bedrock e quindi archivarli e sottoporli a query nell'indice vettoriale S3. Lo strumento supporta i seguenti comandi:

- `s3vectors-embed put`: genera embedding vettoriali di testo, contenuto di file o oggetti S3 e li archivia come vettori in un indice vettoriale S3.
- `s3vectors-embed query`: esegue l'embedding dell'input di una query e cerca vettori simili in un indice vettoriale S3.

Per ulteriori informazioni sui comandi e sull'utilizzo, consulta il repository CLI di [Amazon S3 Vectors Embed](#). GitHub

(Facoltativo) Integrazione di S3 Vectors con Knowledge Base per Amazon Bedrock

Knowledge Base per Amazon Bedrock si integra con S3 Vectors per l'archiviazione conveniente e a lungo termine di set di dati vettoriali.

Prerequisiti

Esamina i [prerequisiti](#) per assicurarti di disporre delle autorizzazioni necessarie per creare una knowledge base per Amazon Bedrock.

- Autorizzazioni IAM appropriate per entrambi i servizi S3 Vectors e Amazon Bedrock. Per ulteriori informazioni sulle autorizzazioni IAM per S3 Vectors, consulta [Identity and Access Management in S3 Vectors](#).
- Documenti di origine pronti per essere importati nella knowledge base.
- Conoscenza dei requisiti del modello di embedding.

Creazione di una knowledge base per Amazon Bedrock con S3 Vectors nella console

Amazon Bedrock Knowledge Bases fornisce un flusso di lavoro end-to-end RAG completamente gestito. Quando crei una knowledge base con S3 Vectors, Amazon Bedrock recupera automaticamente i dati dall'origine dati S3, converte i contenuti in blocchi di testo, genera gli embedding e li archivia nell'indice vettoriale. È quindi possibile eseguire query sulla knowledge base e ottenere risposte basate sui blocchi recuperati dai dati di origine.

Come creare una knowledge base per Amazon Bedrock con S3 Vectors nella console

1. Accedi all' Console di gestione AWS utilizzo di un [ruolo IAM con autorizzazioni Amazon Bedrock](#) e apri la console Amazon Bedrock all'indirizzo. <https://console.aws.amazon.com/bedrock/>
2. Nel riquadro di navigazione a sinistra, scegli Knowledge base.
3. Nella sezione Knowledge base, scegli Crea. Nell'elenco a discesa, scegli Knowledge base con archivio vettoriale.
4. In questo tutorial mantieni i valori predefiniti per Nome della knowledge base, Descrizione della knowledge base e Autorizzazioni IAM.
5. Per Scegli un tipo di origine dati, scegli l'origine dati a cui collegare la knowledge base. In questo tutorial scegli Amazon S3.

6. (Facoltativo) Fornisci eventuali Tag o Log delle applicazioni.
7. Scegli Next (Successivo).
8. In questo tutorial mantieni le impostazioni predefinite per Nome dell'origine dati, Ubicazione dell'origine dati, Strategia di analisi e Strategia di chunking nella pagina Configura l'origine dati.
9. Per URI S3, inserisci il bucket per uso generico S3 contenente i file di origine oppure scegli Sfoglia S3 e scegli il bucket per uso generico S3.
10. Per i dati S3 crittografati, seleziona Aggiungi chiave KMS gestita dal cliente per i dati S3 e specifica la chiave KMS gestita dal cliente.
11. Scegli Successivo per procedere alla fase successiva e specifica le opzioni Modello di embedding e Archivio vettoriale.
12. Nella sezione Modello di embedding, scegli Seleziona modello e scegli un modello di embedding compatibile per l'uso con S3 Vectors. È necessario utilizzare embedding in virgola mobile. Il tipo binario non è supportato.
13. (Facoltativo) Espandi la sezione Configurazioni aggiuntive per visualizzare le seguenti opzioni di configurazione (non tutti i modelli supportano tutte le configurazioni):
 - Tipo di embedding: scegli se convertire i dati in embedding vettoriali in virgola mobile (float32) (più precisi ma più costosi) o embedding vettoriali binari (meno precisi, ma meno costosi). Per l'integrazione con S3 Vectors, è necessario scegliere Embedding vettoriali in virgola mobile.
 - Dimensioni vettoriali: scegli la dimensione raccomandata per i modelli di embedding.
14. Nella sezione Archivio vettoriale, scegli il metodo raccomandato Crea rapidamente un nuovo archivio vettoriale per la configurazione automatica di un nuovo bucket vettoriale oppure scegli Usa un archivio vettoriale esistente per utilizzare un bucket vettoriale esistente, se disponibile. Per informazioni sull'utilizzo di un flusso di archivio vettoriale esistente, consulta [Prerequisiti per l'utilizzo di un archivio vettoriale creato per una knowledge base](#) nella Guida per l'utente di Amazon Bedrock.
15. Per Configurazioni aggiuntive, il bucket vettoriale utilizza per impostazione predefinita la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3). Puoi scegliere di utilizzare la tua chiave KMS per la crittografia lato server con le chiavi del servizio di gestione delle AWS chiavi (SSE-KMS) per un maggiore controllo sulle impostazioni di crittografia.
16. Scegli Successivo per esaminare i dettagli della knowledge base, quindi scegli Crea una knowledge base.

 Note

Il tempo richiesto per creare una knowledge base dipende dalle specifiche configurazioni. Una volta completata la creazione di una knowledge base, lo stato della knowledge base cambia per indicare che è pronta o disponibile. Una volta che la knowledge base è pronta e disponibile, sincronizza l'origine dati per la prima volta oppure ogni volta che desideri aggiornare i contenuti. Per sincronizzare l'origine dati, scegli la knowledge base nella console e scegli Sincronizza nella sezione Panoramica dell'origine dati.

(Facoltativo) Integra i vettori S3 con Amazon OpenSearch

[Amazon OpenSearch Service](#) è un servizio completamente gestito che semplifica l'implementazione, la scalabilità e il AWS funzionamento OpenSearch nel cloud. Esistono due integrazioni tra S3 Vectors e OpenSearch. Una consiste nell'esportare i dati vettoriali da S3 Vectors a Serverless per funzionalità di ricerca ad OpenSearch alte prestazioni. L'altro utilizza S3 Vectors come motore di archiviazione economico, pur mantenendo l'accesso alle funzionalità OpenSearch.

Per ulteriori informazioni, consulta [Utilizzo di vettori S3 con servizio OpenSearch](#).

Bucket vettoriali

I bucket vettoriali sono un tipo di bucket Amazon S3 progettato specificamente per l'archiviazione e l'interrogazione di dati vettoriali. I bucket vettoriali utilizzano API dedicate per gestire i dati vettoriali in modo efficiente e ridurre i costi di caricamento, archiviazione e interrogazione degli embedding vettoriali. I bucket vettoriali forniscono la base per organizzare i dati vettoriali in indici, consentendoti di eseguire ricerche di somiglianza su set di dati di grandi dimensioni e di beneficiare al contempo della disponibilità, della durabilità, della scalabilità e dell'economicità di Amazon S3.

I bucket vettoriali sono ottimizzati per l'archiviazione a lungo termine dei vettori, con tempi di ricerca inferiori al secondo. Puoi eseguire query di somiglianza sui dati vettoriali e, facoltativamente, allegare metadati per filtrare le query in base a condizioni specifiche come date, categorie o preferenze dell'utente.

Ogni bucket vettoriale dispone di un nome della risorsa Amazon (ARN) univoco ed è associato a una policy di risorsa. Gli ARN dei bucket vettoriali seguono il seguente formato:

```
arn:aws:s3vectors:Region:OwnerAccountID:bucket/bucket-name
```


All'interno di un bucket vettoriale, puoi creare indici vettoriali per archiviare e interrogare i dati. Ogni bucket vettoriale esiste all'interno di una AWS regione specifica ed è possibile creare più indici vettoriali all'interno di un bucket vettoriale. I bucket vettoriali supportano meccanismi di sicurezza e controllo degli accessi, tra cui policy IAM basate sull'identità e policy di bucket. Puoi utilizzare le policy di bucket per concedere o limitare l'accesso a indici specifici all'interno del bucket vettoriale.

Caratteristiche principali dei bucket vettoriali:

- Purpose-built per l'archiviazione vettoriale e le operazioni di ricerca di similarità.
- Le scritture altamente coerenti assicurano che i dati vettoriali siano immediatamente accessibili.
- Ottimizzazione automatica dei dati vettoriali per garantire il miglior rapporto prezzo-prestazioni man mano che i set di dati vengono scalati.

Per ulteriori informazioni sui limiti degli indici vettoriali per bucket e altre limitazioni, consulta [Limitazioni e restrizioni](#).

Argomenti

- [Regole di denominazione dei bucket vettoriali](#)
- [Creazione di un bucket vettoriale](#)
- [Elenco di bucket vettoriali](#)
- [Visualizzazione degli attributi del bucket vettoriale](#)
- [Eliminazione di un bucket vettoriale vuoto](#)
- [Gestione delle policy di bucket vettoriali](#)
- [Utilizzo di tag con bucket vettoriali S3](#)

Regole di denominazione dei bucket vettoriali

I nomi dei bucket vettoriali devono seguire convenzioni di denominazione specifiche per garantire l'unicità all'interno di una regione. AWS Amazon S3 applica i seguenti requisiti di denominazione dei bucket e non è possibile creare un bucket vettoriale se queste regole non vengono rispettate. Inoltre, esistono best practice che, sebbene non applicate, aiutano a prevenire i conflitti quando si lavora con i bucket vettoriali a livello di codice o tramite la console.

Requisiti di denominazione dei bucket vettoriali

Quando si creano bucket vettoriali, è necessario attenersi ai seguenti requisiti:

- I nomi dei bucket vettoriali devono essere univoci nello stesso account per ogni regione. AWS AWS
- I nomi dei bucket vettoriali devono avere una lunghezza compresa tra 3 e 63 caratteri.
- I nomi dei bucket vettoriali possono essere costituiti solo da lettere minuscole (a-z), numeri (0-9) e trattini (-).
- I nomi dei bucket vettoriali devono iniziare e terminare con una lettera o un numero.

Best practice per la denominazione

Ti consigliamo di seguire queste best practice per assegnare un nome ai bucket vettoriali:

- Utilizza nomi descrittivi che riflettano lo scopo dei dati vettoriali (ad es. consigli sui prodotti ed embedding di documenti).
- Evita di utilizzare informazioni riservate nei nomi dei bucket poiché potrebbero apparire nei log e. URLs
- Mantieni i nomi concisi ma significativi per una gestione e un'identificazione più semplici.

Queste convenzioni di denominazione garantiscono l'accesso affidabile ai bucket vettoriali tramite la console di gestione AWS , l'API REST di Amazon S3, la CLI e. AWS AWS SDKs

Creazione di un bucket vettoriale

Puoi creare un bucket vettoriale utilizzando la console S3 o la CLI. AWS Tutti i dati archiviati nei bucket vettoriali sono sempre crittografati a riposo. Per impostazione predefinita, i bucket vettoriali utilizzano SSE-S3 per crittografare i dati vettoriali. Puoi scegliere di configurare i bucket per utilizzare invece la crittografia lato server con le chiavi del AWS Key Management Service () (AWS KMS SSE-KMS). Le impostazioni di crittografia dei bucket non possono essere modificate dopo la creazione di un bucket vettoriale, quindi è importante scegliere il metodo di crittografia appropriato in base ai requisiti di sicurezza e alle esigenze di conformità. Per ulteriori informazioni sulla sicurezza nei bucket vettoriali, consulta [Protezione e crittografia dei dati in S3 Vectors](#).

Utilizzo della console S3

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket di vettori.
3. Scegli Crea bucket di vettore.

4. In Nome del bucket di vettore inserisci il nome del bucket.

Il nome del bucket deve rispettare le seguenti regole di denominazione:

- Il nome del bucket essere composto da un numero di caratteri compreso tra 3 e 63.
- Il nome del bucket può contenere solo lettere minuscole, numeri e trattini.
- Il nome del bucket deve essere univoco all'interno del tuo AWS account per una AWS regione.

Per ulteriori informazioni sulle regole di denominazione dei bucket vettoriali, consulta [Regole di denominazione dei bucket vettoriali](#).

 Important

Non è possibile modificare il nome del bucket vettoriale dopo averlo creato.

5. Per Crittografia, scegli una delle seguenti opzioni:

- Non specificare il tipo di crittografia: Amazon S3 applica automaticamente la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) come livello base di crittografia per i nuovi vettori. Questa opzione rappresenta la configurazione più semplice, che non richiede ulteriori impostazioni.
- Specifica il tipo di crittografia: scegli un metodo di crittografia specifico:
 - Crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3): scegli esplicitamente di utilizzare SSE-S3. Amazon S3 crittografa i dati vettoriali mentre li scrivono sullo storage e li decrittografa quando vi accedi. AWS gestisce automaticamente tutte le chiavi di crittografia.
 - Crittografia lato server con AWS chiavi del servizio di gestione delle chiavi (SSE-KMS): utilizza chiavi gestite dal cliente (CMKs) AWS KMS, offrendo un maggiore controllo sulle chiavi di crittografia, sulla rotazione delle chiavi e sulle politiche di accesso.

Se si seleziona SSE-KMS, sono disponibili ulteriori opzioni:

- Scegli tra AWS KMS le tue chiavi: seleziona una chiave gestita dal cliente esistente dal tuo account.
- Inserisci l'ARN della AWS KMS chiave: specifica l'ARN completo di una chiave KMS (formato richiesto).
- Crea una chiave KMS: apre la console AWS KMS per creare una nuova chiave gestita dal cliente.

Requisiti della chiave KMS:

- La chiave KMS deve trovarsi nella stessa Regione del bucket vettoriale.
- È necessario specificare l'ARN completo della chiave KMS (la IDs chiave e gli alias non sono supportati).
- È necessario fornire al principale del servizio S3 Vectors (`indexing.s3vectors.amazonaws.com`) l'autorizzazione `kms:Decrypt` per utilizzare la chiave. Per ulteriori informazioni su un esempio di policy AWS KMS chiave, consulta [Protezione e crittografia dei dati in S3 Vectors](#)

Per informazioni dettagliate sulle opzioni di crittografia e sulla configurazione delle chiavi KMS, consulta [Utilizzo della crittografia SSE-KMS](#).

Important

Le impostazioni di crittografia non possono essere modificate dopo la creazione del bucket vettoriale. Scegline con attenzione in base ai requisiti di sicurezza e conformità a lungo termine.

6. In Tag (facoltativo), puoi aggiungere tag come coppie chiave-valore per monitorare e organizzare i costi degli indici vettoriali utilizzando AWS Billing and Cost Management. Immettere una chiave e un valore. Per aggiungere un altro tag, scegliere Add Tag (Aggiungi tag). Puoi inserire fino a 50 tag per un indice vettoriale. Per ulteriori informazioni, consulta [Utilizzo di tag con bucket vettoriali S3](#).
7. Scegli Crea bucket di vettore.

Dopo la creazione viene visualizzato un messaggio di conferma. Il nuovo bucket vettoriale è presente nell'elenco dei bucket vettoriali ed è pronto per la creazione di indici vettoriali al suo interno.

Usando il AWS CLI

È possibile creare un bucket vettoriale con crittografia SSE-S3 utilizzando il comando riportato di seguito. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors create-vector-bucket \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket"
```

Per creare un bucket vettoriale con crittografia SSE-KMS utilizzando una chiave KMS gestita dal cliente:

```
aws s3vectors create-vector-bucket \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --encryption-configuration '{"sseType": "aws:kms", "kmsKeyArn": "arn:aws:kms:us-  
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"}'
```

Usando il AWS SDKs

SDK for Python

```
import boto3  
  
# Create a S3 Vectors client in the AWS Region of your choice.  
s3vectors = boto3.client("s3vectors", region_name="us-west-2")  
  
#Create a vector bucket  
s3vectors.create_vector_bucket(vectorBucketName="media-embeddings")
```

Elenco di bucket vettoriali

Puoi visualizzare tutti i tuoi bucket vettoriali utilizzando la console Amazon S3 o AWS gli AWS CLI SDK. Le operazioni di elenco supportano il filtraggio basato sul prefisso per aiutarti a trovare bucket specifici quando nel tuo account sono presenti molti bucket vettoriali. Per ulteriori informazioni sui `ListVectorBuckets` limiti dei prefissi e sui limiti di risposta, consulta [ListVectorBuckets](#) Amazon S3 API Reference.

Funzionalità di ricerca dei prefissi

La ricerca dei prefissi consente di elencare i bucket che iniziano con un prefisso specifico, semplificando l'organizzazione e la ricerca dei bucket vettoriali correlati. Questa funzione è particolarmente utile quando utilizzi convenzioni di denominazione che raggruppano bucket correlati:

- Environment-based: `production-vectors-`, `staging-vectors-`, `dev-vectors-`
- In base al caso d'uso: `ml-model-vectors-`, `document-search-`, `image-similarity-`
- Team-based: `data-science-vectors-`, `ml-platform-vectors-`

Utilizzo della console S3

Per elencare i bucket vettoriali

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket di vettori.

La console mostra un elenco di tutti i bucket vettoriali con le seguenti informazioni:

- Nome: nome univoco del bucket vettoriale
- Data di creazione: quando è stato creato il bucket
- Nome della risorsa Amazon (ARN): nome ARN completo per l'accesso programmatico

Per filtrare l'elenco:

- Per trovare un bucket in base all'inizio del suo nome, inserisci un nome o un prefisso vettoriale nella casella di ricerca sopra l'elenco dei bucket.
- Utilizza i prefissi per trovare gruppi di bucket correlati (ad esempio, digita "prod-" per trovare tutti i bucket di produzione)

L'elenco si aggiorna in tempo reale durante la digitazione

Utilizzo di AWS CLI

```
aws s3vectors list-vector-buckets
```

Utilizzo di AWS SDK

SDK for Python

```
import boto3

# Create a S3 Vectors client in the AWS Region of your choice.
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

#List vector buckets
response = s3vectors.list_vector_buckets()
buckets = response["vectorBuckets"]
```

```
print(buckets)
```

Visualizzazione degli attributi del bucket vettoriale

Puoi visualizzare informazioni dettagliate su un bucket vettoriale, incluse le sue proprietà, le impostazioni di crittografia e i dettagli di creazione utilizzando l'API REST di Amazon S3, AWS gli SDK, la console S3 o l'interfaccia a riga di AWS comando (CLI). AWS Per ulteriori informazioni `GetVectorBucket`, consulta Amazon S3 API [GetVectorBucket](#) Reference.

Utilizzo della console S3

1. Accedi alla console e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket di vettori.
3. La console mostra un elenco di tutti i tuoi bucket vettoriali. Trova un bucket in base all'inizio del nome del bucket, inserisci il nome o il prefisso di un bucket vettoriale nella casella di ricerca sopra l'elenco dei bucket. Una volta individuato il bucket vettoriale, puoi visualizzare informazioni dettagliate su di esso, incluse le impostazioni di crittografia, i tag e i dettagli di creazione nella scheda Proprietà.

Utilizzo di AWS CLI

```
aws s3vectors get-vector-bucket --vector-bucket-name "amzn-s3-demo-vector-bucket"
```

Eliminazione di un bucket vettoriale vuoto

Puoi eliminare un bucket vettoriale quando non è più necessario. Per eliminare un bucket vettoriale, devi prima eliminare tutti gli indici vettoriali al suo interno. Eliminando un indice vettoriale, vengono eliminati anche tutti i dati vettoriali al suo interno. Usa l'API REST di Amazon S3, AWS gli SDK, la console S3 o l'interfaccia a riga di AWS comando (AWS CLI) per eliminare un bucket vettoriale.

Prima di eliminare un bucket vettoriale, devi:

- Eliminare tutti gli indici vettoriali nel bucket.
- Assicurarti che non siano in corso operazioni sul bucket o sui relativi indici.

⚠ Important

- L'eliminazione del bucket è permanente e non può essere annullata.
- Tutti i dati e le configurazioni associati al bucket vengono definitivamente persi.
- Dopo l'eliminazione del bucket, il relativo nome può essere riutilizzato.
- Qualsiasi applicazione o script che fa riferimento al bucket restituirà errori dopo l'eliminazione.

Utilizzo della console S3

1. Accedi alla console e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket di vettori.
3. La console mostra un elenco di tutti i tuoi bucket vettoriali. Trova un bucket in base all'inizio del nome del bucket, inserisci il nome o il prefisso di un bucket vettoriale nella casella di ricerca sopra l'elenco dei bucket. Una volta individuato e scelto il bucket vettoriale, seleziona l'opzione Elimina.
4. Per confermare l'eliminazione, digita **delete** e seleziona Elimina bucket vettoriale.

Utilizzo di AWS CLI

Verifica innanzitutto che non siano presenti indici vettoriali nel bucket. Per ulteriori informazioni su come verificare che il bucket sia vuoto, consulta [Elenco degli indici vettoriali](#).

Se sono presenti indici, è necessario eliminare tutti i vettori da ciascun indice e successivamente eliminare gli indici. Per ulteriori informazioni su come verificare che il bucket sia vuoto, consulta [Elenco dei vettori](#), [Eliminazione dei vettori da un indice vettoriale](#) e [Eliminazione di un indice vettoriale](#).

Per eliminare il bucket vettoriale vuoto, usa il seguente comando di esempio e sostituiscilo *user input placeholders* con le tue informazioni.

```
aws s3vectors delete-vector-bucket \  
--vector-bucket-name "amzn-s3-demo-vector-bucket"
```


Utilizzo di AWS SDK

SDK for Python

```
import boto3

# Create a S3 Vectors client in the AWS Region of your choice.
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

#Delete a vector bucket
response = s3vectors.delete_vector_bucket(vectorBucketName="media-embeddings")
```

Gestione delle policy di bucket vettoriali

Le policy di bucket vettoriali sono policy basate sulle risorse che puoi collegare direttamente ai bucket vettoriali per controllare l'accesso al bucket e al suo contenuto. Puoi aggiungere, visualizzare, modificare ed eliminare le policy dei bucket vettoriali utilizzando l'API REST di Amazon S3 AWS SDKs, la console S3 o AWS l'interfaccia a riga di comando (CLI).AWS Le policy bucket per i bucket vettoriali possono concedere autorizzazioni ai principali di altri AWS account, rendendole utili per scenari di accesso tra account.

Operazioni di gestione delle policy

- [PutVectorBucketPolicy](#)— Aggiungi o aggiorna una policy sui bucket.
- [GetVectorBucketPolicy](#)— Recupera la policy attuale del bucket.
- [DeleteVectorBucketPolicy](#)— Rimuovi la bucket policy.

Aggiunta di una policy di bucket vettoriale

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Scegli Vector bucket e seleziona il nome del bucket vettoriale a cui desideri aggiungere una policy.
4. Scegli la scheda Autorizzazioni.
5. In Vector bucket policy, scegli Modifica.

6. Nell'editor della policy, inserisci il file JSON della policy stessa.
7. (Facoltativo) Seleziona Esempi di policy per visualizzare esempi di policy da adattare alle tue esigenze.
8. Dopo aver inserito la policy, seleziona Salva modifiche.

Usando il AWS CLI

Per aggiungere o aggiornare una bucket policy, usa il comando di esempio seguente e sostituiscila *user input placeholders* con le tue informazioni.

```
aws s3vectors put-vector-bucket-policy \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --policy '{"Version": "2012-10-17", "Statement": [{"Effect": "Allow", "Principal": {"AWS": "arn:aws:iam::111122223333:root"}, "Action": "s3vectors:*", "Resource": "arn:aws:s3vectors:region:111122223333:bucket/amzn-s3-demo-vector-bucket"}]}'
```

Visualizzazione di una policy di bucket vettoriale

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Scegli Vector bucket e seleziona il nome del bucket vettoriale di cui desideri visualizzare la policy.
4. Scegli la scheda Autorizzazioni.

Usando il AWS CLI

Per recuperare una bucket policy, utilizzate il seguente comando di esempio e sostituirla *user input placeholders* con le vostre informazioni.

```
aws s3vectors get-vector-bucket-policy \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket"
```

Eliminazione di una policy di bucket vettoriale

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, seleziona Amazon S3.
3. Scegli Vector bucket e seleziona il nome del bucket vettoriale per cui desideri eliminare la policy.
4. Scegli la scheda Autorizzazioni.
5. Nella politica del bucket vettoriale, scegli Elimina.

Usando il AWS CLI

Per eliminare una bucket policy, utilizzate il seguente comando di esempio e sostituitela *user input placeholders* con le vostre informazioni.

```
aws s3vectors delete-vector-bucket-policy \  
--vector-bucket-name "amzn-s3-demo-vector-bucket"
```

Per informazioni dettagliate sulla creazione e sulla gestione delle policy di bucket, incluse policy di esempio e best practice, consulta [Esempi di policy basate sulle risorse di S3 Vectors](#).

Utilizzo di tag con bucket vettoriali S3

Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso i bucket vettoriali Amazon S3. Puoi etichettare i bucket vettoriali S3 quando li crei o gestire i tag sui bucket vettoriali esistenti. Per informazioni generali sui tag, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

Note

Non sono previsti costi aggiuntivi per l'utilizzo dei tag nei bucket vettoriali oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Modi comuni per utilizzare i tag con bucket vettoriali

Usa i tag sui tuoi bucket vettoriali S3 per:

- **Attribute-based controllo degli accessi (ABAC):** ridimensiona le autorizzazioni di accesso e concedi l'accesso ai bucket vettoriali S3 in base ai relativi tag. Per ulteriori informazioni, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

ABAC per bucket vettoriali S3

I bucket vettoriali Amazon S3 supportano il controllo degli accessi basato sugli attributi (ABAC) tramite tag. Utilizza le chiavi di condizione basate su tag nelle policy dei bucket vettoriali della tua AWS organizzazione, IAM e S3. Per le aziende, ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle tue policy IAM, puoi controllare l'accesso ai bucket vettoriali S3 in base ai tag del bucket vettoriale utilizzando le seguenti chiavi di condizione globali:

`aws:ResourceTag/key-name`

Utilizzare questa chiave per confrontare la coppia chiave-valore del tag specificata nella policy con la coppia chiave-valore associata alla risorsa. Ad esempio, puoi richiedere che l'accesso a una risorsa sia consentito solo se la risorsa dispone di una chiave di tag Dept collegata al valore Marketing. Per ulteriori informazioni, consulta [Controllare l'accesso alle risorse. AWS](#)

`aws:RequestTag/key-name`

Utilizzare questa chiave per confrontare la coppia chiave-valore del tag passata nella richiesta con la coppia del tag specificata nella policy. Ad esempio, è possibile controllare che la richiesta includa la chiave del tag Dept e che abbia il valore Accounting. Per ulteriori informazioni, vedere [Controllo dell'accesso durante AWS le richieste](#). È possibile utilizzare questa chiave di condizione per limitare quali coppie chiave-valore di tag possono essere passate durante le operazioni API TagResource e CreateVectorBucket.

`aws:TagKeys`

Utilizzare questa chiave per confrontare le chiavi dei tag in una richiesta con quelle specificate nella policy. Nell'utilizzo delle policy per controllare gli accessi tramite tag, è consigliabile utilizzare la chiave di condizione `aws:TagKeys` per definire le chiavi di tag ammesse. Per esempi di policy e ulteriori informazioni, consulta [Controllo dell'accesso in base alle chiavi di tag](#). Puoi creare un bucket vettoriale S3 con tag. Per consentire il tagging durante l'operazione API CreateVectorBucket, è necessario creare una policy che comprende entrambe le azioni `s3vectors:TagResource` e `s3vectors:CreateVectorBucket`. È quindi possibile utilizzare

la chiave di condizione `aws:TagKeys` per implementare nella richiesta `CreateVectorBucket` specifici tag.

`s3vectors:VectorBucketTag/tag-key`

Usa questa chiave di condizione per concedere autorizzazioni a dati specifici nei bucket vettoriali utilizzando i tag. Questa chiave di condizione agisce sui tag assegnati al bucket vettoriale per tutte le azioni di S3 Vectors. Anche quando si crea un indice con tag, questa chiave di condizione agisce sui tag applicati al bucket vettoriale che contiene quell'indice. Ad esempio, potresti richiedere che l'accesso a un bucket sia consentito solo se al bucket è associata la chiave tag `Dept` con il valore `Marketing`. Quando si accede agli indici, questa condizione fa riferimento ai tag associati al bucket vettoriale contenente quell'indice, mentre `aws:ResourceTag/tag-key` farà riferimento ai tag dell'indice stesso.

Esempi di politiche ABAC per bucket vettoriali

Guarda il seguente esempio di politiche ABAC per bucket vettoriali Amazon S3.

1.1 - Politica IAM per creare o modificare bucket vettoriali con tag specifici

In questa policy IAM, gli utenti o i ruoli con questa policy possono creare bucket vettoriali S3 solo se etichettano il bucket vettoriale con la chiave `project` e il valore del tag `Trinity` nella richiesta di creazione del bucket vettoriale. Possono anche aggiungere o modificare tag su bucket vettoriali S3 esistenti purché la `TagResource` richiesta includa la coppia chiave-valore del tag `project:Trinity`. Questa policy non concede autorizzazioni di lettura, scrittura o eliminazione sui bucket vettoriali o sui relativi oggetti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateVectorBucketWithTags",
      "Effect": "Allow",
      "Action": [
        "s3vectors:CreateVectorBucket",
        "s3vectors:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
```

```

        "Trinity"
      ]
    }
  }
}
]
}

```

1.2 - Politica del bucket vettoriale per limitare le operazioni sul bucket vettoriale utilizzando i tag

In questa policy del bucket vettoriale, i principali IAM (utenti e ruoli) possono eseguire operazioni utilizzando l'PutVectorBucketPolicyazione sul bucket vettoriale solo se il valore del tag del bucket vettoriale corrisponde al valore del project tag del bucket vettoriale. project

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowObjectOperations",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3vectors:PutVectorBucketPolicy",
      "Resource": "arn:aws:s3vectors:us-west-2:111122223333:bucket/amzn-s3-demo-
vector-bucket",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}

```

1.3 - Politica IAM per modificare i tag sulle risorse esistenti mantenendo la governance dei tag

In questa policy IAM, i principali IAM (utenti o ruoli) possono modificare i tag su un bucket vettoriale solo se il valore del tag del bucket vettoriale corrisponde al valore del project tag del principal. project Per questi bucket project vettoriali sono consentiti solo i quattro tag environmentowner, e cost-center specificati nelle chiavi di aws:TagKeys condizione. Questo

aiuta a far rispettare la governance dei tag, previene modifiche non autorizzate ai tag e mantiene lo schema di tagging coerente nei bucket vettoriali.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3vectors:TagResource"
      ],
      "Resource": "arn:aws::s3vectors:us-west-2:111122223333:bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",
            "owner",
            "cost-center"
          ]
        }
      }
    }
  ]
}
```

1.4 - Utilizzo della chiave s3vectors: condition **VectorBucketTag**

In questa policy IAM, l'istruzione condition consente l'accesso alle operazioni del bucket vettoriale e dell'indice vettoriale solo se il bucket vettoriale ha la chiave del tag e il valore del tag. Environment Production

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToTaggedBucket",
      "Effect": "Allow",
      "Action": "*",
```

```
"Resource": "arn:aws::s3vectors:us-west-2:111122223333:bucket/*",
"Condition": {
  "StringEquals": {
    "s3vectors:VectorBucketTag/Environment": "Production"
  }
}
}
```

Gestione dei tag per i bucket vettoriali

Puoi aggiungere o gestire tag per i bucket vettoriali S3 utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o utilizzando le API S3:, e. [TagResource](#) [UntagResource](#) [ListTagsForResource](#) Per ulteriori informazioni, consulta:

Creazione di bucket vettoriali con tag

Puoi etichettare i bucket vettoriali Amazon S3 quando li crei. Non è previsto alcun costo aggiuntivo per l'utilizzo dei tag nei bucket vettoriali oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sull'etichettatura dei bucket vettoriali, consulta. [Utilizzo di tag con bucket vettoriali S3](#)

Permissions

Per creare un bucket vettoriale con tag, devi disporre delle seguenti autorizzazioni:

- s3vectors:CreateVectorBucket
- s3vectors:TagResource

Risoluzione degli errori

Se riscontri un errore durante il tentativo di creare un bucket vettoriale con tag, puoi fare quanto segue:

- Verifica di disporre delle [autorizzazioni necessarie](#) per creare il bucket vettoriale e aggiungervi un tag.
- Controllare la policy dell'utente IAM per eventuali condizioni del controllo degli accessi basato su attributi (ABAC). Potrebbe esserti richiesto di etichettare i bucket vettoriali solo con chiavi e valori di tag specifici. Per ulteriori informazioni, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

Fasi

Puoi creare un bucket vettoriale con tag applicati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per creare un bucket vettoriale con tag utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli **bucket vettoriali**.
3. Scegli **crea bucket vettoriale** per creare un nuovo bucket vettoriale.
4. Crea un bucket vettoriale come faresti normalmente; vedi. [Creazione di un bucket vettoriale](#)
5. Nella pagina **Crea bucket vettoriale**, **Tags** è un'opzione per creare un nuovo bucket vettoriale.
6. Inserisci un nome per il bucket vettoriale.
7. Scegli **Aggiungi nuovo tag** per aprire l'editor di tag e inserisci una coppia chiave-valore di tag. La chiave di tag è obbligatoria, mentre il valore è facoltativo.
8. Per aggiungere un altro tag, scegli nuovamente **Aggiungi nuovo tag**. È possibile inserire fino a 50 coppie chiave-valore di tag.
9. Dopo aver specificato le opzioni per il nuovo bucket vettoriale, scegli **Crea bucket vettoriale**.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la creazione di un bucket vettoriale con tag, consulta la seguente sezione nel riferimento alle API **Amazon S3 Vectors**:

[CreateVectorBucket](#)

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come creare un bucket vettoriale con tag utilizzando. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Quando si crea un bucket vettoriale è necessario fornire i dettagli di configurazione e utilizzare la seguente convenzione di denominazione: `example-vector-bucket`

```
aws s3vector create-vector-bucket --vector-bucket-name acc-bucket \  
--tags Department=Accounting,Stage=Prod
```

Aggiungere un tag a un bucket vettoriale

Puoi aggiungere tag ai bucket vettoriali Amazon S3 e modificare questi tag. Non sono previsti costi aggiuntivi per l'utilizzo dei tag nei bucket vettoriali oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sull'etichettatura dei bucket vettoriali, consulta. [Utilizzo di tag con bucket vettoriali S3](#)

Permissions

Per aggiungere un tag a un bucket vettoriale, è necessario disporre delle seguenti autorizzazioni:

- `s3vectors:TagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di aggiungere un tag a un bucket vettoriale, è possibile effettuare le seguenti operazioni:

- Verifica di disporre delle [autorizzazioni necessarie](#) per aggiungere un tag a un bucket vettoriale.
- Se hai tentato di aggiungere una chiave tag che inizia con il prefisso AWS riservato `aws:`, modifica la chiave del tag e riprova.

Fasi

Puoi aggiungere tag ai bucket vettoriali utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per aggiungere tag a un bucket vettoriale utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli `bucket vettoriali`.
3. Scegli il nome del bucket vettoriale.

4. Scegliere la scheda Properties (Proprietà).
5. Scorri la sezione Tag e scegli Aggiungi nuovo tag.
6. Viene visualizzata la pagina Aggiungi tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
7. Se si aggiunge un nuovo tag con lo stesso nome di chiave di un tag esistente, il valore del nuovo tag sovrascrive il valore del tag esistente.
8. In questa pagina è anche possibile modificare i valori dei tag esistenti.
9. Dopo aver aggiunto i tag, scegli Salva le modifiche.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'aggiunta di tag a un bucket vettoriale, consulta la seguente sezione nell'Amazon S3 Vectors API Reference:

[TagResource](#)

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come aggiungere tag a un bucket vettoriale utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3vectors tag-resource \  
--resource-arn arn:aws:s3vectors:us-east-1:012345678900:bucket/acc-bucket \  
--tags Stage=Prod, CostCenter=Marketing
```

Visualizzazione dei bucket tag vettoriali

Puoi visualizzare o elencare i tag applicati ai bucket vettoriali Amazon S3. Per ulteriori informazioni sull'etichettatura dei bucket vettoriali, consulta [Utilizzo di tag con bucket vettoriali S3](#)

Permissions

Per visualizzare i tag applicati a un bucket vettoriale, è necessario disporre delle seguenti autorizzazioni:

- `s3vectors:ListTagsForResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di elencare o visualizzare i tag di un bucket vettoriale, è possibile effettuare le seguenti operazioni:

- Verifica di disporre delle [autorizzazioni necessarie](#) per visualizzare o elencare i tag del bucket vettoriale.

Fasi

Puoi visualizzare i tag applicati ai bucket vettoriali utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare i tag applicati a un bucket vettoriale utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli bucket vettoriali.
3. Scegli il nome del bucket vettoriale.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag per visualizzare tutti i tag applicati al bucket vettoriale.
6. La sezione Tag mostra i User-defined tag per impostazione predefinita. Puoi selezionare la scheda dei tag AWS generati per visualizzare i tag applicati al tuo bucket vettoriale dai AWS servizi.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la visualizzazione dei tag applicati a un bucket vettoriale, consulta la seguente sezione nell'Amazon Simple Vectors API Reference:

[ListTagsforResource](#)

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio CLI mostra come visualizzare i tag applicati a un bucket vettoriale. Per utilizzare il comando, sostituiscili *user input placeholders* con le tue informazioni.

```
aws s3vectors list-tags-for-resource \  
--resource-arn arn:aws:s3vectors:us-east-1:012345678900:bucket/acc-bucket
```

Eliminazione di un tag da un bucket vettoriale

È possibile rimuovere i tag dai bucket vettoriali S3. Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso i bucket vettoriali Amazon S3. Per ulteriori informazioni sull'etichettatura dei bucket vettoriali, consulta [Utilizzo di tag con bucket vettoriali S3](#)

Note

Se elimini un tag e in seguito scopri che è stato utilizzato per tenere traccia dei costi o per il controllo degli accessi, puoi aggiungere nuovamente il tag al bucket vettoriale.

Permissions

Per eliminare un tag da un bucket vettoriale, devi disporre della seguente autorizzazione:

- `s3vectors:UntagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di eliminare un tag da un bucket vettoriale, è possibile effettuare le seguenti operazioni:

- Verifica di disporre delle [autorizzazioni necessarie](#) per eliminare un tag da un bucket vettoriale.

Fasi

Puoi eliminare i tag dai bucket vettoriali utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK AWS.

Utilizzo della console S3

Per eliminare i tag da un bucket vettoriale utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli bucket vettoriali.
3. Scegli il nome del bucket vettoriale.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag e seleziona la casella di controllo accanto al tag o ai tag che desideri eliminare.
6. Scegliere Elimina.
7. Viene visualizzato il pop-up Elimina tag definiti dall'utente che chiede di confermare l'eliminazione del tag o dei tag selezionati.
8. Seleziona Elimina per confermare.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'eliminazione di tag da un bucket vettoriale, consulta la seguente sezione nell'Amazon S3 Vectors API Reference:

[UntagResource](#)

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di nella Guida per l'utente AWS CLI](#). AWS Command Line Interface

Il seguente esempio CLI mostra come eliminare i tag da un bucket vettoriale utilizzando. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3vectors untag-resource \  
--resource-arn arn:aws:s3vectors:us-east-1:012345678900:bucket/acc-bucket \  
--tag-keys CostCenter Department
```

Indici vettoriali

Note

Scegli con attenzione i parametri di configurazione dell'indice vettoriale. Dopo aver creato un indice vettoriale, non è possibile aggiornare il nome dell'indice vettoriale, la dimensione, la metrica della distanza o le chiavi di metadati non filtrabili. Per modificare uno di questi valori, occorre creare un nuovo indice vettoriale.

Gli indici vettoriali sono risorse all'interno di un bucket vettoriale che archiviano e organizzano i dati vettoriali per eseguire operazioni di ricerca per similarità in modo efficiente. Quando si crea un indice vettoriale, si specifica la metrica della distanza (Cosine o Euclidean), il numero di dimensioni che un vettore deve avere e, facoltativamente, un elenco di campi di metadati da escludere dal filtro durante le query di somiglianza.

Per ulteriori informazioni sui limiti di indici vettoriali per bucket, sui limiti di vettori per indice e sui limiti di dimensione per vettore, consulta [Limitazioni e restrizioni](#).

Ogni indice vettoriale dispone di un nome della risorsa Amazon (ARN) univoco. Gli ARN degli indici vettoriali adottano il seguente formato:

```
arn:aws:s3vectors:region:account-id:bucket/bucket-name/index/index-name
```

Requisiti per la denominazione degli indici vettoriali

- I nomi degli indici vettoriali devono essere univoci all'interno del bucket vettoriale.
- I nomi degli indici vettoriali devono essere composti da un numero di caratteri compreso tra 3 e 63.
- I caratteri validi sono lettere minuscole (a-z), numeri (0-9), trattini (-) e punti (.).
- I nomi degli indici vettoriali devono iniziare e terminare con una lettera o un numero.

Requisiti per la dimensione

Una dimensione è il numero di valori presenti in un vettore. Tutti i vettori aggiunti all'indice devono avere esattamente questo numero di valori.

- Una dimensione deve essere un numero intero compreso tra 1 e 4096.

- Una dimensione più grande richiede più spazio di archiviazione.

Opzioni di metrica della distanza

La metrica della distanza specifica come viene calcolata la somiglianza tra i vettori. Quando si creano embedding vettoriali, si sceglie la metrica della distanza consigliata dal modello di embedding per ottenere risultati più accurati.

- Coseno: misura il coseno dell'angolo tra i vettori. Ideale per vettori normalizzati e quando la direzione è più importante della grandezza.
- Euclideo: misura la distanza in linea retta tra i vettori. Ideale quando sia la direzione sia la grandezza sono importanti.

Non-filterable chiavi di metadati

Le chiavi di metadati consentono di collegare informazioni aggiuntive ai vettori come coppie chiave-valore durante l'archiviazione e il recupero. Per impostazione predefinita, tutti i metadati sono filtrabili, quindi possono essere utilizzati per filtrare i risultati delle query. Tuttavia, è possibile designare chiavi di metadati specifiche come non filtrabili per archiviare le informazioni con vettori senza utilizzarle per il filtro.

A differenza delle chiavi di metadati predefinite, queste chiavi non possono essere utilizzate come filtri di interrogazione. Non-filterable le chiavi di metadati possono essere recuperate ma non possono essere ricercate, interrogate o filtrate. È possibile accedervi solo dopo aver individuato l'indice.

Non-filterable le chiavi di metadati consentono di arricchire i vettori con un contesto aggiuntivo che si desidera recuperare con i risultati della ricerca ma non è necessario filtrare. Un esempio comune di chiave di metadati non filtrabili è quando si incorpora un testo nei vettori e si desidera includere il testo originale come metadati non filtrabili. Ciò consente di restituire il testo di origine insieme ai risultati della ricerca vettoriale senza aumentare i limiti di dimensione dei metadati filtrabili. Altri esempi includono la memorizzazione dei timestamp di creazione, degli URL di origine o delle informazioni descrittive puramente di riferimento. Non-filterable È possibile accedere alle chiavi di metadati durante il recupero dei vettori ma, a differenza delle chiavi di metadati predefinite, queste chiavi non possono essere utilizzate come filtri di interrogazione.

Di seguito sono riportati i requisiti per le chiavi di metadati non filtrabili.

- Non-filterable le chiavi di metadati devono essere univoche all'interno dell'indice vettoriale.

- Non-filterable le chiavi di metadati devono contenere da 1 a 63 caratteri.
- Non-filterable le chiavi dei metadati non possono essere modificate dopo la creazione dell'indice vettoriale.
- S3 Vectors supporta fino a 10 chiavi di metadati non filtrabili per indice.

Per ulteriori informazioni sulle chiavi di metadati non filtrabili, consulta [Metadati non filtrabili](#).

Argomenti

- [Creazione di un indice vettoriale in un bucket vettoriale](#)
- [Elenco degli indici vettoriali](#)
- [Eliminazione di un indice vettoriale](#)
- [Utilizzo di tag con indici vettoriali S3](#)

Creazione di un indice vettoriale in un bucket vettoriale

Note

Scegli con attenzione i parametri di configurazione dell'indice vettoriale. Dopo aver creato un indice vettoriale, non è possibile aggiornare il nome dell'indice vettoriale, la dimensione, la metrica della distanza o le chiavi di metadati non filtrabili. Per modificare uno di questi valori, occorre creare un nuovo indice vettoriale.

Un indice vettoriale è una risorsa all'interno di un bucket vettoriale che archivia e organizza i dati vettoriali per eseguire ricerche per similarità efficienti. Quando si crea un indice vettoriale, si definiscono le caratteristiche che tutti i vettori di tale indice devono condividere, ad esempio la dimensione, la metrica della distanza utilizzata per i calcoli della similarità e, facoltativamente, le chiavi di metadati non filtrabili. È inoltre possibile configurare impostazioni e tag di crittografia dedicati per l'indice vettoriale al momento della creazione dell'indice. Per ulteriori informazioni sui requisiti di denominazione degli indici vettoriali, sui requisiti delle dimensioni, sulle opzioni di metrica della distanza e sulle chiavi di metadati non filtrabili, consulta [Limitazioni e restrizioni](#). Per ulteriori informazioni sull'impostazione della configurazione della crittografia per gli indici vettoriali, vedere. [Protezione e crittografia dei dati in S3 Vectors](#) Per ulteriori informazioni sull'impostazione dei tag, vedere. [Utilizzo di tag con bucket vettoriali S3](#)

Gli indici vettoriali devono essere creati all'interno di un bucket vettoriale esistente e richiedono parametri di configurazione specifici che non possono essere modificati dopo la creazione.

Utilizzo della console S3

Come creare un indice vettoriale

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione, scegli Bucket di vettori.
3. Nell'elenco dei bucket vettoriali, seleziona il nome del bucket in cui desideri creare un indice vettoriale.
4. Scegli Crea indice di vettore.
5. Per Nome dell'indice di vettore, inserisci un nome per l'indice vettoriale.

I nomi degli indici vettoriali devono essere univoci all'interno del bucket vettoriale. Il nome dell'indice deve essere composto da un numero di caratteri compreso tra 3 e 63. I caratteri validi sono lettere minuscole (a-z), numeri (0-9), trattini (-) e punti (.). Per ulteriori informazioni sui requisiti di denominazione dell'indice vettoriale, consulta [Limitazioni e restrizioni](#).

6. Per Dimensione, inserisci il numero di valori in ogni vettore.

Note

- Il valore per Dimensione determina quanti valori numerici conterrà ogni vettore.
- Tutti i vettori aggiunti a questo indice devono avere esattamente questo numero di valori.
- La dimensione deve essere compresa tra 1 e 4096.
- Una dimensione più grande richiede più spazio di archiviazione.
- Scegli in base alle dimensioni di output del modello di embedding.

Per ulteriori informazioni sui requisiti di dimensione, consulta [Limitazioni e restrizioni](#).

7. Per Metrica della distanza, scegli una delle seguenti opzioni:
 - Coseno: misura il coseno dell'angolo tra i vettori. Ideale per vettori normalizzati e quando la direzione è più importante della grandezza
 - Euclideo: misura la distanza in linea retta tra i vettori. Ideale quando sia la direzione sia la grandezza sono importanti.

8. (Facoltativo) Nella sezione **Non-filterable metadati**, configura le chiavi di metadati che verranno archiviate ma non utilizzate per il filtraggio:

Per aggiungere chiavi di metadati non filtrabili:

- Scegliere **Add key** (Aggiungi chiave).
- Inserisci un nome per la chiave (da 1 a 63 caratteri e univoco all'interno dell'indice vettoriale).
- Ripeti l'operazione per aggiungere altre chiavi (al massimo 10 chiavi).

 Note

È possibile collegare a ciascun vettore i metadati filtrabili come coppie chiave-valore quando si inseriscono dati vettoriali dopo aver creato l'indice vettoriale. Per impostazione predefinita, tutte le chiavi di metadati collegate ai vettori sono filtrabili e possono essere utilizzate come filtri in una query di somiglianza. Solo le chiavi di metadati specificate come non filtrabili durante la creazione dell'indice vettoriale non possono essere utilizzate come filtro. Per ulteriori informazioni sui limiti di dimensione dei metadati per vettore, inclusi i vincoli dei metadati filtrabili e totali, consulta [Limitazioni e restrizioni](#).

9. Esamina attentamente la configurazione.

 Note

Queste impostazioni non possono essere modificate dopo la creazione.

- 10In **Crittografia** scegli **Specifica il tipo di crittografia**. È possibile utilizzare le impostazioni del bucket per la crittografia o sovrascrivere le impostazioni di crittografia per l'indice vettoriale. Se sostituisci le impostazioni a livello di bucket, hai la possibilità di specificare il tipo di crittografia per l'indice vettoriale come **Server-side crittografia con AWS chiavi di Key Management Service (SSE-KMS)** o **Server-side crittografia con chiavi gestite da Amazon S3 ()**. **SSE-S3** Per ulteriori informazioni sull'impostazione della configurazione della crittografia per gli indici vettoriali, consulta [Protezione e crittografia dei dati in S3 Vectors](#)

- 11In **Tag** (facoltativo), puoi aggiungere tag come coppie chiave-valore per aiutare a tracciare e organizzare i costi degli indici vettoriali utilizzando la AWS fatturazione e la gestione dei costi. Immettere una chiave e un valore. Per aggiungere un altro tag, scegliere **Add Tag** (Aggiungi tag). Puoi inserire fino a 50 tag per un indice vettoriale. Per ulteriori informazioni, consulta [Utilizzo di tag con bucket vettoriali S3](#).

- 12Scegli **Crea indice di vettore**.

Utilizzo di AWS CLI

Per creare un indice vettoriale in un bucket vettoriale, utilizza i seguenti comandi di esempio e sostituisci user input placeholders con le informazioni appropriate.

Esempio 1: creazione di un indice vettoriale con chiavi di metadati non filtrabili

```
aws s3vectors create-index \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --index-name "idx" \  
  --data-type "float32" \  
  --dimension 1 \  
  --distance-metric "cosine" \  
  --metadata-configuration '{"nonFilterableMetadataKeys":["nonFilterableKey1"]}'
```

Esempio 2: creazione di un indice vettoriale senza chiavi di metadati non filtrabili

```
aws s3vectors create-index \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --index-name "idx2" \  
  --data-type "float32" \  
  --dimension 4096 \  
  --distance-metric "euclidean"
```

Inoltre, tutti i metadati (filtrabili e non filtrabili) vengono recuperati allo stesso modo utilizzando le operazioni API GetVectors, ListVectors o QueryVectors. Il seguente comando della CLI mostra come recuperare i vettori con metadati (inclusi i metadati non filtrabili).

Richiesta di esempio:

```
aws s3vectors get-vectors \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --index-name "idx" \  
  --keys '["vec1", "vec3"]' \  
  --return-data \  
  --return-metadata \
```

Risposta di esempio:

```
{
  "vectors": [
    {
      "key": "vec1",
      "data": {
        "float32": [
          0.10000000149011612,
          0.20000000298023224,
          0.30000001192092896,
          0.4000000059604645,
          0.5
        ]
      },
      "metadata": {
        "category": "test",
        "text": "First vector"
      }
    },
    {
      "key": "vec3",
      "data": {
        "float32": [
          0.6000000238418579,
          0.699999988079071,
          0.800000011920929,
          0.8999999761581421,
          1.0
        ]
      },
      "metadata": {
        "text": "Third vector",
        "category": "test"
      }
    }
  ]
}
```

La risposta includerà tutti i metadati associati al vettore, indipendentemente dal fatto che siano stati specificati come filtrabili o non filtrabili durante la creazione dell'indice.

Utilizzo di AWS SDK

SDK for Python

```
import boto3

# Create a S3 Vectors client in the AWS Region of your choice.
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

#Create a vector index "movies" in the vector bucket "media-embeddings" without non-
filterable metadata keys
s3vectors.create_index(
    vectorBucketName="media-embeddings",
    indexName="movies",
    dimension=3,
    distanceMetric="cosine",
    dataType = "float32"
)

#Create a vector index "movies" in the vector bucket "media-embeddings" with non-
filterable metadata keys
s3vectors.create_index(
    vectorBucketName="media-embeddings",
    indexName="movies",
    dimension=3,
    distanceMetric="cosine",
    dataType = "float32",
    metadataConfiguration= {"nonFilterableMetadataKeys":
["nonFilterableMetadataKey1"]}
)
```

Elenco degli indici vettoriali

Puoi visualizzare tutti gli indici vettoriali all'interno di un bucket vettoriale. L'operazione di elenco supporta il filtraggio in base al prefisso per aiutarti a trovare indici specifici quando sono presenti molti indici in un bucket. Per ulteriori informazioni sui `ListIndexes` limiti dei prefissi e sui limiti di risposta, consulta [ListIndexes](#) Amazon Simple Storage Service API Reference.

Funzionalità di ricerca dei prefissi

La ricerca dei prefissi consente di elencare gli indici che iniziano con un prefisso specifico, semplificando l'organizzazione e la ricerca degli indici vettoriali correlati. Questa funzione è particolarmente utile quando utilizzi convenzioni di denominazione che raggruppano indici correlati:

- Per tipo di dati: `text-embeddings-`, `image-features-`, `audio-vectors-`
- Per modello: `model1-embeddings-`, `model2-vectors-`, `custom-model-`
- Per caso d'uso: `search-index-`, `recommendation-`, `similarity-`
- Per ambiente: `prod-vectors-`, `staging-vectors-`, `dev-vectors-`

Utilizzo della console S3

Per elencare gli indici vettoriali

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket di vettori.
3. Nell'elenco dei bucket vettoriali, seleziona il nome del bucket contenente gli indici che desideri visualizzare.
4. La console mostra un elenco completo di tutti gli indici vettoriali nel bucket, tra cui:
 - Nome: il nome di ciascun indice.
 - Data di creazione: quando l'indice è stato creato.
 - Nome della risorsa Amazon (ARN): nome ARN completo per ciascun indice.

Per filtrare l'elenco

1. Inserisci il nome o il prefisso dell'indice nella casella di ricerca sopra l'elenco degli indici. Utilizza i prefissi per trovare gruppi di indici correlati.
2. L'elenco si aggiorna in tempo reale durante la digitazione.

Utilizzo di AWS CLI

Usa i seguenti comandi di esempio e sostituiscili *user input placeholders* con le tue informazioni.

Per elencare gli indici con un prefisso specifico in un bucket vettoriale

Richiesta di esempio:

```
aws s3vectors list-indexes \  
  --vector-bucket-name "amzn-s3-demo-bucket" \  
  --prefix "idx" \  
  --max-results 1
```

Risposta di esempio:

```
{  
  "nextToken":  
    "10bb29ZkzxMGtBXs97Rkbs26xdtKemu4brsnq2jX8DCocADkILv5cRphemXS3PXXFnQBihQBmESgEeKaGA",  
  "indexes": [  
    {  
      "vectorBucketName": "amzn-s3-demo-bucket",  
      "indexName": "idx",  
      "indexArn": "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-  
vector-bucket/index/idx",  
      "creationTime": "2025-06-12T15:50:23+00:00"  
    }  
  ]  
}
```

Per elencare gli indici con impaginazione

Richiesta di esempio:

```
aws s3vectors list-indexes \  
  --vector-bucket-name "amzn-s3-demo-bucket" \  
  --prefix "idx" \  
  --next-token  
  "10bb29ZkzxMGtBXs97Rkbs26xdtKemu4brsnq2jX8DCocADkILv5cRphemXS3PXXFnQBihQBmESgEeKaGA"
```

Risposta di esempio:

```
{  
  "indexes": [  
    {
```



```
{
  "vectorBucketName": "amzn-s3-demo-bucket",
  "indexName": "idx2",
  "indexArn": "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket/index/idx2",
  "creationTime": "2025-06-12T15:45:37+00:00"
}
```

Utilizzo di AWS SDK

SDK for Python

```
import boto3

# Create a S3 Vectors client in the AWS Region of your choice.
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

#List vector indexes in your vector bucket
response = s3vectors.list_indexes(vectorBucketName="media-embeddings")
indexes = response["indexes"]
print(indexes)
```

Eliminazione di un indice vettoriale

Puoi eliminare un indice vettoriale quando non è più necessario. Questa operazione rimuove definitivamente l'indice e tutti i vettori che sono memorizzati al suo interno.

Important

Quando elimini un indice vettoriale, è importante tenere in considerazione quanto segue:

- È possibile eliminare gli indici vettoriali anche quando contengono vettori
- Tutti i vettori memorizzati nell'indice vengono eliminati definitivamente
- Tutti i metadati associati a tali vettori vengono definitivamente persi
- Questa operazione non può essere annullata
- Qualsiasi operazione in corso sull'indice non andrà a buon fine
- Le applicazioni che interrogano l'indice riceveranno errori

- Il nome dell'indice può essere riutilizzato all'interno del bucket

Utilizzo di AWS CLI

Prima di eliminare un indice vettoriale, verifica l'indice stesso. Per ulteriori informazioni su come controllare i dettagli dell'indice, consulta [GetIndex](#) Amazon S3 API Reference. Per ulteriori informazioni su come elencare i vettori all'interno dell'indice per vedere cosa verrà eliminato, consulta [Elenco degli indici vettoriali](#).

Per eliminare un indice vettoriale, utilizza i seguenti comandi di esempio. Sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors delete-index --vector-bucket-name "amzn-s3-demo-vector-bucket" \
    --index-name "idx2"
```

Per ulteriori informazioni su come verificare se l'indice viene eliminato, consulta [Elenco degli indici vettoriali](#).

Utilizzo di AWS SDK

SDK for Python

```
import boto3

# Create a S3 Vectors client in the AWS Region of your choice.
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

#Delete a vector index
response = s3vectors.delete_index(
    vectorBucketName="media-embeddings",
    indexName="movies")
```

Utilizzo di tag con indici vettoriali S3

Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso gli indici vettoriali Amazon S3. Puoi etichettare gli indici vettoriali S3 quando li crei o gestire i tag sugli indici vettoriali esistenti. Per informazioni generali sui tag, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

 Note

Non sono previsti costi aggiuntivi per l'utilizzo dei tag sugli indici vettoriali oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Modi comuni per utilizzare i tag con indici vettoriali

Usa i tag sui tuoi indici vettoriali S3 per:

- **Allocazione dei costi:** tieni traccia dei costi di archiviazione tramite tag di indice vettoriale in AWS Fatturazione e gestione dei costi. Per ulteriori informazioni, consulta [Utilizzo dei tag per l'allocazione dei costi](#).
- **Attribute-based controllo degli accessi (ABAC):** ridimensiona le autorizzazioni di accesso e concedi l'accesso agli indici vettoriali S3 in base ai relativi tag. Per ulteriori informazioni, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

 Note

È possibile utilizzare gli stessi tag sia per l'allocazione dei costi che per il controllo degli accessi.

ABAC per indici vettoriali S3

Gli indici vettoriali Amazon S3 supportano il controllo degli accessi basato sugli attributi (ABAC) tramite tag. Utilizza le chiavi di condizione basate su tag nelle politiche di indicizzazione vettoriale delle tue AWS organizzazioni, IAM e S3. Per le aziende, ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle tue policy IAM, puoi controllare l'accesso agli indici vettoriali S3 in base ai tag dell'indice vettoriale utilizzando le seguenti chiavi di condizione globali:

`aws:ResourceTag/key-name`

Utilizzare questa chiave per confrontare la coppia chiave-valore del tag specificata nella policy con la coppia chiave-valore associata alla risorsa. Ad esempio, puoi richiedere che l'accesso a una risorsa sia consentito solo se la risorsa dispone di una chiave di tag Dept collegata al valore Marketing. Per ulteriori informazioni, consulta [Controllare l'accesso alle risorse. AWS](#)

aws:RequestTag/key-name

Utilizzare questa chiave per confrontare la coppia chiave-valore del tag passata nella richiesta con la coppia del tag specificata nella policy. Ad esempio, è possibile controllare che la richiesta includa la chiave del tag Dept e che abbia il valore Accounting. Per ulteriori informazioni, vedere [Controllo dell'accesso durante AWS le richieste](#). È possibile utilizzare questa chiave di condizione per limitare quali coppie chiave-valore di tag possono essere passate durante le operazioni API TagResource e CreateIndex.

aws:TagKeys

Utilizzare questa chiave per confrontare le chiavi dei tag in una richiesta con quelle specificate nella policy. Nell'utilizzo delle policy per controllare gli accessi tramite tag, è consigliabile utilizzare la chiave di condizione aws:TagKeys per definire le chiavi di tag ammesse. Per esempi di policy e ulteriori informazioni, consulta [Controllo dell'accesso in base alle chiavi di tag](#). È possibile creare un indice vettoriale S3 con tag. Per consentire il tagging durante l'operazione API CreateVectorBucket, è necessario creare una policy che comprende entrambe le azioni s3vectors:TagResource e s3vectors:CreateVectorBucket. È quindi possibile utilizzare la chiave di condizione aws:TagKeys per implementare nella richiesta CreateVectorBucket specifici tag.

Esempi di politiche ABAC per indici vettoriali

Guarda il seguente esempio di politiche ABAC per gli indici vettoriali Amazon S3.

1.1 - Politica IAM per creare o modificare indici vettoriali con tag specifici

In questa policy IAM, gli utenti o i ruoli con questa policy possono creare indici vettoriali S3 solo se etichettano l'indice vettoriale con la chiave project e il valore del tag Trinity nella richiesta di creazione dell'indice vettoriale. Possono anche aggiungere o modificare tag su indici vettoriali S3 esistenti, purché la TagResource richiesta includa la coppia chiave-valore del tag. project:Trinity Questa policy non concede autorizzazioni di lettura, scrittura o cancellazione sugli indici vettoriali o sui relativi oggetti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateVectorIndexWithTags",
      "Effect": "Allow",
```

```

    "Action": [
      "s3vectors:CreateIndex",
      "s3vectors:TagResource"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/project": [
          "Trinity"
        ]
      }
    }
  }
}

```

1.2 - Politica IAM per modificare i tag sulle risorse esistenti mantenendo la governance dei tag

In questa policy IAM, i responsabili IAM (utenti o ruoli) possono modificare i tag su un indice vettoriale solo se il valore del `project` tag dell'indice vettoriale corrisponde al valore del tag del `project` principale. Solo i quattro tag `project`, `environmentowner`, e `cost-center` specificati nelle chiavi di `aws:TagKeys` condizione sono consentiti per questi indici vettoriali. Questo aiuta a far rispettare la governance dei tag, previene modifiche non autorizzate ai tag e mantiene lo schema di tagging coerente in tutti gli indici vettoriali.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3vectors:TagResource"
      ],
      "Resource": "arn:aws::s3vectors:us-west-2:111122223333:bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",

```

```
        "owner",  
        "cost-center"  
    ]  
}  
}  
]  
}
```

Gestione dei tag per gli indici vettoriali

Puoi aggiungere o gestire tag per gli indici vettoriali S3 utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o utilizzando le API S3:., e. [TagResource](#) [UntagResource](#) [ListTagsForResource](#) Per ulteriori informazioni, consulta:

Argomenti

- [Creazione di indici vettoriali con tag](#)
- [Aggiungere un tag a un indice vettoriale](#)
- [Visualizzazione dei tag di indice vettoriali](#)
- [Eliminazione di un tag da un indice vettoriale](#)

Creazione di indici vettoriali con tag

Puoi etichettare gli indici vettoriali Amazon S3 quando li crei. Non sono previsti costi aggiuntivi per l'utilizzo di tag su indici vettoriali oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sull'etichettatura degli indici vettoriali, consulta. [Utilizzo di tag con indici vettoriali S3](#)

Permissions

Per creare un indice vettoriale con tag, è necessario disporre delle seguenti autorizzazioni:

- `s3vectors:CreateIndex`
- `s3vectors:TagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di creare un indice vettoriale con tag, è possibile effettuare le seguenti operazioni:

- Verifica di disporre delle [autorizzazioni necessarie](#) per creare l'indice vettoriale e aggiungervi un tag.
- Controllare la policy dell'utente IAM per eventuali condizioni del controllo degli accessi basato su attributi (ABAC). Potrebbe esserti richiesto di etichettare i tuoi indici vettoriali solo con chiavi e valori di tag specifici. Per ulteriori informazioni, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

Fasi

Puoi creare un indice vettoriale con tag applicati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per creare un indice vettoriale con tag utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli indici vettoriali.
3. Scegli [Crea indice vettoriale](#) per creare un nuovo indice vettoriale.
4. Crea un indice vettoriale come faresti normalmente; vedete [Creazione di un indice vettoriale in un bucket vettoriale](#).
5. Nella pagina [Crea indice vettoriale](#), [Tags](#) è un'opzione per creare un nuovo indice vettoriale.
6. Inserite un nome per l'indice vettoriale.
7. Scegli [Aggiungi nuovo tag](#) per aprire l'editor di tag e inserisci una coppia chiave-valore di tag. La chiave di tag è obbligatoria, mentre il valore è facoltativo.
8. Per aggiungere un altro tag, scegli nuovamente [Aggiungi nuovo tag](#). È possibile inserire fino a 50 coppie chiave-valore di tag.
9. Dopo aver completato la specificazione delle opzioni per il nuovo indice vettoriale, scegliete [Crea indice vettoriale](#).

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la creazione di un indice vettoriale con tag, consulta la seguente sezione nell'Amazon S3 Vectors API Reference:

[CreateIndex](#)

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio CLI mostra come creare un indice vettoriale con tag utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Quando si crea un indice vettoriale è necessario fornire i dettagli di configurazione e utilizzare la seguente convenzione di denominazione: `example-vector-index`

```
aws s3vectors create-index --vector-bucket-name acc-bucket --data-type "float32" \  
--index-name accounts-index --dimension 1024 --distance-metric euclidean \  
--tags Department=Accounting,Stage=Prod
```

Aggiungere un tag a un indice vettoriale

Puoi aggiungere tag agli indici vettoriali Amazon S3 e modificare questi tag. Non sono previsti costi aggiuntivi per l'utilizzo di tag su indici vettoriali oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sull'etichettatura degli indici vettoriali, consulta [Utilizzo di tag con indici vettoriali S3](#)

Permissions

Per aggiungere un tag a un indice vettoriale, è necessario disporre delle seguenti autorizzazioni:

- `s3vectors:TagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di aggiungere un tag a un indice vettoriale, è possibile effettuare le seguenti operazioni:

- Verifica di disporre delle [autorizzazioni necessarie](#) per aggiungere un tag a un indice vettoriale.
- Se hai tentato di aggiungere una chiave tag che inizia con il prefisso AWS riservato `aws :`, modifica la chiave del tag e riprova.

Fasi

Puoi aggiungere tag agli indici vettoriali utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK AWS.

Utilizzo della console S3

Per aggiungere tag a un indice vettoriale utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli indici vettoriali.
3. Scegli il nome dell'indice vettoriale.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri la sezione Tag e scegli Aggiungi nuovo tag.
6. Viene visualizzata la pagina Aggiungi tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
7. Se si aggiunge un nuovo tag con lo stesso nome di chiave di un tag esistente, il valore del nuovo tag sovrascrive il valore del tag esistente.
8. In questa pagina è anche possibile modificare i valori dei tag esistenti.
9. Dopo aver aggiunto i tag, scegli Salva le modifiche.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'aggiunta di tag a un indice vettoriale, consulta la seguente sezione nell'Amazon S3 Vectors API Reference:

[TagResource](#)

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio CLI mostra come aggiungere tag a un indice vettoriale utilizzando il AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3vectors tag-resource \  
--resource-arn arn:aws:s3vectors:us-east-1:012345678900:bucket/acc-bucket/  
index/accounts-index \  
--tags Stage=Prod, CostCenter=Marketing
```

Visualizzazione dei tag di indice vettoriali

Puoi visualizzare o elencare i tag applicati agli indici vettoriali Amazon S3. Per ulteriori informazioni sull'etichettatura degli indici vettoriali, consulta [Utilizzo di tag con indici vettoriali S3](#)

Permissions

Per visualizzare i tag applicati a un indice vettoriale, è necessario disporre delle seguenti autorizzazioni:

- `s3vectors:ListTagsForResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di elencare o visualizzare i tag di un indice vettoriale, è possibile effettuare le seguenti operazioni:

- Verificate di disporre delle [autorizzazioni necessarie](#) per visualizzare o elencare i tag dell'indice vettoriale.

Fasi

Puoi visualizzare i tag applicati agli indici vettoriali utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare i tag applicati a un indice vettoriale utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli indici vettoriali.
3. Scegli il nome dell'indice vettoriale.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag per visualizzare tutti i tag applicati all'indice vettoriale.
6. La sezione Tag mostra i User-defined tag per impostazione predefinita. Puoi selezionare la scheda dei tag AWS generati per visualizzare i tag applicati al tuo indice vettoriale dai AWS servizi.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la visualizzazione dei tag applicati a un indice vettoriale, consulta la seguente sezione nell'Amazon Simple Vectors API Reference:

[ListTagsforResource](#)

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio CLI mostra come visualizzare i tag applicati a un indice vettoriale. Per utilizzare il comando, sostituiscili *user input placeholders* con le tue informazioni.

```
aws s3vectors list-tags-for-resource \  
  --resource-arn arn:aws:s3vectors:us-east-1:012345678900:bucket/acc-bucket/  
  index/accounts-index
```

Eliminazione di un tag da un indice vettoriale

È possibile rimuovere i tag dagli indici vettoriali S3. Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso gli indici vettoriali Amazon S3. Per ulteriori informazioni sull'etichettatura degli indici vettoriali, consulta. [Utilizzo di tag con indici vettoriali S3](#)

Note

Se elimini un tag e in seguito scopri che è stato utilizzato per tenere traccia dei costi o per il controllo degli accessi, puoi aggiungere nuovamente il tag all'indice vettoriale.

Permissions

Per eliminare un tag da un indice vettoriale, è necessario disporre delle seguenti autorizzazioni:

- `s3vectors:UntagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di eliminare un tag da un indice vettoriale, è possibile effettuare le seguenti operazioni:

- Verifica di disporre delle [autorizzazioni necessarie](#) per eliminare un tag da un indice vettoriale.

Fasi

Puoi eliminare i tag dagli indici vettoriali utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per eliminare tag da un indice vettoriale utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli indici vettoriali.
3. Scegli il nome dell'indice vettoriale.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag e seleziona la casella di controllo accanto al tag o ai tag che desideri eliminare.
6. Scegliere Elimina.
7. Viene visualizzato il pop-up Elimina tag definiti dall'utente che chiede di confermare l'eliminazione del tag o dei tag selezionati.
8. Seleziona Elimina per confermare.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'eliminazione di tag da un indice vettoriale, consulta la seguente sezione nell'Amazon S3 Vectors API Reference:

[UntagResource](#)

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come eliminare i tag da un indice vettoriale utilizzando il AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
aws s3vectors untag-resource \
```

```
--resource-arn arn:aws:s3vectors:us-east-1:012345678900:bucket/acc-bucket/  
index/accounts-index \  
--tag-keys CostCenter Department
```

Vettori

Ogni vettore è costituito da una chiave, che lo identifica in modo univoco in un indice vettoriale. Inoltre, è possibile collegare a ciascun vettore i metadati (ad esempio anno, autore, genere, posizione) come coppie chiave-valore.

Le operazioni sui dati vettoriali includono l'inserimento, l'elenco, l'esecuzione di query e l'eliminazione di vettori. Per generare nuovi incorporamenti vettoriali dei tuoi dati non strutturati, puoi utilizzare l'operazione [InvokeModel](#) API di Amazon Bedrock per specificare l'ID del modello di incorporamento che desideri utilizzare. Inoltre, lo strumento open source della CLI di Amazon S3 Vectors Embed offre un modo semplificato per generare embedding ed eseguire ricerche semantiche dalla riga di comando. Per ulteriori informazioni su questo strumento open source che automatizza sia la generazione di embedding vettoriali con i modelli di fondazione di Amazon Bedrock sia le operazioni di ricerca semantica all'interno degli indici vettoriali S3, consulta [Creazione di embedding vettoriali ed esecuzione di ricerche semantiche con s3vectors-embed-cli](#).

Concetti sui vettori

Chiavi del vettore: ogni vettore è identificato da una chiave univoca all'interno dell'indice. Le chiavi del vettore possono contenere fino a 1.024 caratteri e devono essere univoche all'interno dell'indice vettoriale. Le chiavi fanno distinzione tra maiuscole e minuscole e possono contenere qualsiasi carattere UTF-8.

Dimensione vettoriale: una dimensione è il numero di valori presenti in un vettore. Le dimensioni più grandi richiedono più spazio di archiviazione. Tutti i vettori di un indice devono avere lo stesso numero di dimensioni, specificato al momento della creazione dell'indice. Una dimensione deve essere un numero intero compreso tra 1 e 4096.

Metadati: è possibile collegare i metadati ai vettori come coppie chiave-valore per fornire un contesto aggiuntivo e abilitare il filtro durante le query. I metadati includono chiavi di metadati filtrabili e non filtrabili. I metadati filtrabili vengono utilizzati per il filtro delle query. Le chiavi di metadati non filtrabili vengono specificate durante la creazione di un indice vettoriale e forniscono un contesto aggiuntivo, ma non possono essere utilizzate per il filtro. I metadati supportano i dati di tipo stringa, numerico e booleano. Per ulteriori informazioni sui metadati filtrabili e non filtrabili, consulta [Filtro dei metadati](#).

Per ulteriori informazioni sui limiti dei metadati, inclusi i limiti di dimensione per vettore e il numero massimo di chiavi di metadati per vettore, consulta [Limitazioni e restrizioni](#).

Argomenti

- [Inserimento di vettori in un indice vettoriale](#)
- [Elenco dei vettori](#)
- [Query sui vettori](#)
- [Eliminazione dei vettori da un indice vettoriale](#)
- [Filtro dei metadati](#)

Inserimento di vettori in un indice vettoriale

È possibile aggiungere vettori a un indice vettoriale con l'operazione API [PutVectors](#). Ogni vettore è costituito da una chiave, che lo identifica in modo univoco in un indice vettoriale. Se si inserisce un vettore con una chiave già esistente nell'indice, il vettore esistente verrà completamente sovrascritto, rendendo il vettore precedente non più ricercabile. Per massimizzare la velocità di scrittura e ottimizzare i costi, si consiglia di inserire i vettori in batch di grandi dimensioni, fino alla dimensione massima del batch per `PutVectors`. Tuttavia, per i carichi di lavoro che richiedono l'utilizzo di batch più piccoli, ad esempio quando sono attivi, i dati vettoriali in entrata devono diventare immediatamente ricercabili, puoi ottenere un throughput di scrittura più elevato utilizzando un numero maggiore di `PutVectors` richieste simultanee, fino al limite massimo consentito di richieste al secondo. Per ulteriori informazioni sulla dimensione massima del batch per `PutVectors`, ovvero il limite di vettori per chiamata `PutVectors` API, e il limite massimo di richieste e vettori per secondo, consulta [Limitazioni e restrizioni](#). Inoltre, è possibile collegare a ciascun vettore i metadati (ad esempio anno, autore, genere, posizione) come coppie chiave-valore. Per impostazione predefinita, tutte le chiavi di metadati collegate ai vettori sono filtrabili e possono essere utilizzate come filtri in una query di somiglianza. Solo le chiavi di metadati specificate come non filtrabili durante la creazione dell'indice vettoriale non possono essere utilizzate come filtro. Gli indici vettoriali S3 supportano i metadati di tipo stringa, numerico, booleano ed elenco. Per ulteriori informazioni sul limite della dimensione totale dei metadati per vettore e sul limite della dimensione dei metadati filtrabili per vettore, consulta [Limitazioni e restrizioni](#). Se la dimensione dei metadati supera questi limiti, l'operazione API `PutVectors` restituirà un errore `400 Bad Request`.

Prima di aggiungere dati vettoriali all'indice vettoriale con l'operazione API `PutVectors`, è necessario convertire i dati non elaborati in embedding vettoriali, che sono rappresentazioni numeriche dei contenuti sotto forma di array di numeri a virgola mobile. Gli embedding vettoriali

acquisiscono il significato semantico dei contenuti, consentendo le ricerche per similarità una volta archiviati nell'indice vettoriale tramite l'operazione `PutVectors`. È possibile generare embedding vettoriali utilizzando vari metodi a seconda del tipo di dati e del caso d'uso. Questi metodi includono l'utilizzo di framework di machine learning, librerie di embedding specializzate o servizi AWS come Amazon Bedrock. Ad esempio, se utilizzi Amazon Bedrock, puoi generare incorporamenti con l'operazione [InvokeModelAPI](#) e il tuo modello di incorporamento preferito.

Inoltre, Amazon Bedrock Knowledge Bases fornisce un flusso di lavoro end-to-end RAG completamente gestito in cui Amazon Bedrock recupera automaticamente i dati dalla fonte di dati S3, converte i contenuti in blocchi di testo, genera incorporamenti e li archivia nel tuo indice vettoriale. È quindi possibile eseguire query sulla knowledge base e ottenere risposte basate sui blocchi recuperati dai dati di origine.

Inoltre, lo strumento open source della CLI di Amazon S3 Vectors Embed offre un modo semplificato per generare embedding ed eseguire ricerche semantiche dalla riga di comando. Per ulteriori informazioni su questo strumento open source che automatizza sia la generazione di embedding vettoriali con i modelli di fondazione di Amazon Bedrock sia le operazioni di ricerca semantica all'interno degli indici vettoriali S3, consulta [Creazione di embedding vettoriali ed esecuzione di ricerche semantiche con s3vectors-embed-cli](#).

Note

Quando inserisci dati vettoriali nell'indice vettoriale, è necessario fornire i dati vettoriali come valori `float32` (in virgola mobile a 32 bit). Se passi valori ad alta precisione a un AWS SDK, S3 Vectors converte i valori in virgola mobile a 32 bit prima di archivarli e, e le operazioni restituiscono i valori. [GetVectorsListVectorsQueryVectors](#)`float32` Diversi AWS SDKs possono avere diversi tipi numerici predefiniti, quindi assicurati che i vettori siano formattati correttamente come valori indipendentemente dall'SDK che stai utilizzando. `float32` Ad esempio, in Python utilizza `numpy.float32` o converti in modo esplicito i valori.

Usando il AWS SDKs

SDK for Python

```
# Populate a vector index with embeddings from Amazon Titan Text Embeddings V2.
import boto3
import json
```

```
# Create Bedrock Runtime and S3 Vectors clients in the AWS Region of your choice.
bedrock = boto3.client("bedrock-runtime", region_name="us-west-2")
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

# Texts to convert to embeddings.
texts = [
    "Star Wars: A farm boy joins rebels to fight an evil empire in space",
    "Jurassic Park: Scientists create dinosaurs in a theme park that goes wrong",
    "Finding Nemo: A father fish searches the ocean to find his lost son"
]

# Generate vector embeddings.
embeddings = []
for text in texts:
    response = bedrock.invoke_model(
        modelId="amazon.titan-embed-text-v2:0",
        body=json.dumps({"inputText": text})
    )

    # Extract embedding from response.
    response_body = json.loads(response["body"].read())
    embeddings.append(response_body["embedding"])

# Write embeddings into vector index with metadata.
s3vectors.put_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    vectors=[
        {
            "key": "Star Wars",
            "data": {"float32": embeddings[0]},
            "metadata": {"source_text": texts[0], "genre": "scifi"}
        },
        {
            "key": "Jurassic Park",
            "data": {"float32": embeddings[1]},
            "metadata": {"source_text": texts[1], "genre": "scifi"}
        },
        {
            "key": "Finding Nemo",
            "data": {"float32": embeddings[2]},
            "metadata": {"source_text": texts[2], "genre": "family"}
        }
    ]
]
```


)

Elenco dei vettori

Puoi elencare i vettori in un indice vettoriale con l'operazione API. [ListVectors](#). Per ulteriori informazioni sul numero massimo di vettori che possono essere restituiti per pagina, consulta [Limitazioni e restrizioni](#). La risposta include un token di impaginazione quando i risultati vengono troncati. Per ulteriori informazioni sugli elementi di risposta di `ListVectors`, consulta [ListVectors](#) Amazon S3 API Reference. Puoi anche utilizzare `ListVectors` per esportare dati vettoriali da un indice vettoriale specifico. `ListVectors` è molto coerente. Dopo un'operazione di scrittura, è possibile elencare immediatamente i vettori con tutte le modifiche implementate.

Utilizzo di AWS CLI

Per elencare i vettori, utilizza i seguenti comandi di esempio. Sostituisci *user input placeholders* con le informazioni appropriate.

I parametri `segment-index` e `segment-count` consentono di partizionare le operazioni di elenco su più richieste parallele. Quando si specifica un valore `segment-count` (ad es. 2), si divide l'indice in altrettanti segmenti. Il parametro `segment-index` (a partire da 0) determina il segmento da elencare. Questo approccio aiuta a migliorare le prestazioni quando si elencano indici vettoriali di grandi dimensioni abilitando l'elaborazione parallela. Per ulteriori informazioni su `segment-count` e `segment-index`, consulta [ListVectors](#) Amazon S3 API Reference.

Per elencare tutti i vettori in un indice

Richiesta di esempio:

```
aws s3vectors list-vectors \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --index-name "idx" \
  --segment-count 2 \
  --segment-index 0 \
  --return-data \
  --return-metadata
```

Risposta di esempio:

```
{
  "vectors": [
```

```

    {
      "key": "vec3",
      "data": {
        "float32": [0.40000000059604645]
      },
      "metadata": {
        "nonFilterableKey": "val4",
        "filterableKey": "val2"
      }
    }
  ]
}

```

Per elencare i vettori con impaginazione

Richiesta di esempio:

```

aws s3vectors list-vectors \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --index-name "idx" \
  --segment-count 2 \
  --segment-index 0 \
  --return-data \
  --return-metadata \
  --next-token
"zWfh7e57H2jBfBtRRmC70fMw1209G9dg3j2qM6kM4t0rps6ClYzJykgM0i19eGqU5nhf_gTq53IfoUdTnsg"

```

Risposta di esempio:

```

{
  "vectors": [
    {
      "key": "vec1",
      "data": {
        "float32": [0.5]
      },
      "metadata": {
        "nonFilterableKey": "val2",
        "filterableKey": "val1"
      }
    }
  ]
}

```

Utilizzo di AWS SDK

SDK for Python

Esempio: elenca i vettori in un indice vettoriale

```
import boto3

# Create a S3 Vectors client in the AWS Region of your choice.
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

#List vectors in your vector index

response = s3vectors.list_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    maxResults = 600,
    returnData = True,
    returnMetadata = True
)

vectors = response["vectors"]

print(vectors)
```

Esempio: elenca tutti i vettori in un indice vettoriale in parallelo

```
import boto3

# Create a S3 Vectors client in the AWS Region of your choice.
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

#List vectors in the 1st half of vectors in the index.
response = s3vectors.list_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    segmentCount=2,
    segmentIndex=1,
    maxResults = 600,
    returnData = True,
    returnMetadata = True
)
```

```
vectors = response["vectors"]

#List vectors starting from the 2nd half of vectors in the index.
# This can be ran in parallel with the first `list_vectors` call.
response = s3vectors.list_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    segmentCount=2,
    segmentIndex=1,
    maxResults = 600,
    returnData = True,
    returnMetadata = True
)

vectors = response["vectors"]

print(vectors)
```

Query sui vettori

È possibile eseguire una query di similarità con l'operazione [QueryVectorsAPI](#), in cui si specifica il vettore di query, il numero di risultati pertinenti da restituire (i primi K vicini più vicini) e l'indice ARN. Inoltre, si possono utilizzare i filtri di metadati in una query per cercare solo i vettori che corrispondono al filtro. Se si effettua una richiesta di filtro in base a un campo di metadati non filtrabili, la richiesta restituirà un errore 400 Bad Request. Per ulteriori informazioni sul filtro dei metadati, consulta [Filtro dei metadati](#).

Nella risposta, per impostazione predefinita vengono restituite le chiavi del vettore. Facoltativamente, è possibile includere nella risposta la distanza e i metadati. Quando topK supera la dimensione della pagina, i risultati vengono restituiti su più pagine. La risposta include un messaggio nextToken che viene utilizzato per recuperare la pagina successiva. Continua a fare QueryVectors richieste con gli stessi filter parametri queryVectortopK, e, passando il nextToken da ogni risposta, finché non nextToken è più presente. In alternativa, puoi utilizzare gli impaginatori integrati negli SDK AWS per iterare automaticamente su tutte le pagine senza gestirle manualmente. nextToken I token di paginazione rimangono validi per diversi minuti dopo l'esecuzione della query. Se un token di impaginazione scade, emetti nuovamente la query originale per iniziare una nuova sessione. Le scritture sull'indice vettoriale tra i recuperi di pagina non si rifletteranno in quella sessione di interrogazione. Per i limiti specifici relativi alle topK dimensioni della pagina, consulta. [Limitazioni e restrizioni](#)

Quando si genera il vettore di query, è necessario utilizzare lo stesso modello di embedding vettoriale utilizzato per generare i vettori iniziali archiviati nell'indice vettoriale. Ad esempio, se si utilizza il modello Embedding di testo Amazon Titan V2 in Amazon Bedrock per generare embedding vettoriali dei documenti, è necessario utilizzare lo stesso modello di embedding per convertire una domanda in un vettore di query. Inoltre, Knowledge Base per Amazon Bedrock fornisce un flusso di lavoro RAG end-to-end completamente gestito in cui Amazon Bedrock recupera automaticamente i dati dall'origine dati S3, converte i contenuti in blocchi di testo, genera embedding e li archivia nell'indice vettoriale. È quindi possibile eseguire query sulla knowledge base e ottenere risposte basate sui blocchi recuperati dai dati di origine. Per ulteriori informazioni su come eseguire query sui vettori da una knowledge base per Amazon Bedrock nella console, consulta [\(Facoltativo\) Integrazione di S3 Vectors con Knowledge Base per Amazon Bedrock](#).

Inoltre, lo strumento open source della CLI di Amazon S3 Vectors Embed offre un modo semplificato per eseguire ricerche semantiche dalla riga di comando. Questo strumento open source semplifica il processo di query gestendo sia la generazione di embedding vettoriali con i modelli di fondazione di Amazon Bedrock sia l'esecuzione di operazioni di ricerca semantica sugli indici vettoriali S3. Per ulteriori informazioni sull'utilizzo di questo strumento per effettuare query sui dati vettoriali, consulta [Creazione di embedding vettoriali ed esecuzione di ricerche semantiche con s3vectors-embed-cli](#).

S3 Vectors offre tempi di risposta inferiori al secondo per le cold query, sfruttando il throughput elastico di Amazon S3 per eseguire ricerche efficienti tra miliardi di vettori. Ciò lo rende estremamente conveniente per i carichi di lavoro con richieste poco frequenti. Per le query più frequenti, S3 Vectors è in grado di fornire tempi di risposta di appena 100 ms, a vantaggio dei carichi di lavoro con modelli di query ripetuti o frequenti. Quando i risultati delle query vengono restituiti su più pagine, è possibile accedere immediatamente alle pagine successive.

Per l'esecuzione di query di somiglianza per gli embedding vettoriali, diversi fattori possono influire sulle prestazioni di richiamata medie, tra cui il modello di embedding vettoriale, la dimensione del set di dati vettoriali (il numero di vettori e le dimensioni) e la distribuzione delle query. S3 Vectors offre una richiamata media superiore al 90% per la maggior parte dei set di dati. La richiamata media misura la qualità dei risultati delle query. Una richiamata media del 90% significa che la risposta contiene il 90% dei vettori effettivi più vicini (dati acquisiti) archiviati nell'indice vettoriale relativo al vettore di query. Tuttavia, poiché le prestazioni effettive possono variare a seconda dei casi d'uso specifici, è consigliabile eseguire test personalizzati con dati e query rappresentativi per verificare che S3 Vectors soddisfi i requisiti di richiamata.

Utilizzo di AWS SDK

SDK for Python

```
# Query a vector index with an embedding from Amazon Titan Text Embeddings V2.
import boto3
import json

# Create Bedrock Runtime and S3 Vectors clients in the AWS Region of your choice.
bedrock = boto3.client("bedrock-runtime", region_name="us-west-2")
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

# Query text to convert to an embedding.
input_text = "adventures in space"

# Generate the vector embedding.
response = bedrock.invoke_model(
    modelId="amazon.titan-embed-text-v2:0",
    body=json.dumps({"inputText": input_text})
)

# Extract embedding from response.
model_response = json.loads(response["body"].read())
embedding = model_response["embedding"]

# Query vector index.
response = s3vectors.query_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=3,
    returnDistance=True,
    returnMetadata=True
)
print(json.dumps(response["vectors"], indent=2))

# Query vector index with a metadata filter.
response = s3vectors.query_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=3,
    filter={"genre": "scifi"},
    returnDistance=True,
```

```

        returnMetadata=True
    )
print(json.dumps(response["vectors"], indent=2))

# Paginated query with manual nextToken handling.
query_params = dict(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=500,
    returnDistance=True,
    returnMetadata=True,
)
response = s3vectors.query_vectors(**query_params)
for vector in response["vectors"]:
    print(vector)
while response.get("nextToken") is not None:
    response = s3vectors.query_vectors(**query_params,
    nextToken=response["nextToken"])
    for vector in response["vectors"]:
        print(vector)

# Use the built-in paginator to automatically iterate through all pages.
paginator = s3vectors.get_paginator("query_vectors")

for page in paginator.paginate(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=500,
    returnDistance=True,
    returnMetadata=True,
):
    for vector in page["vectors"]:
        print(vector)

```

Eliminazione dei vettori da un indice vettoriale

È possibile eliminare vettori specifici da un indice vettoriale specificando le relative chiavi vettoriali utilizzando l'[DeleteVectors](#) API. Questa operazione è utile per rimuovere dati obsoleti o errati, preservando il resto dei dati vettoriali.

Utilizzo di AWS CLI

Per eliminare i vettori, utilizza i seguenti comandi di esempio. Sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors delete-vectors \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --index-name "idx" \  
  --keys '["vec2","vec3"]'
```

Utilizzo di AWS SDK

SDK for Python

```
import boto3  
  
# Create a S3 Vectors client in the AWS Region of your choice.  
s3vectors = boto3.client("s3vectors", region_name="us-west-2")  
  
#Delete vectors in a vector index  
response = s3vectors.delete_vectors(  
    vectorBucketName="media-embeddings",  
    indexName="movies",  
    keys=["Star Wars", "Finding Nemo"])
```

Filtro dei metadati

Il filtro dei metadati consente di filtrare i risultati delle query in base ad attributi specifici associati ai vettori. È possibile utilizzare i filtri dei metadati con le operazioni di query per trovare vettori che soddisfino sia i criteri di somiglianza sia le condizioni specifiche dei metadati.

S3 Vectors supporta due tipi di metadati: filtrabili e non filtrabili. La differenza fondamentale è che i metadati filtrabili possono essere utilizzati nei filtri di query ma hanno limiti di dimensione più rigorosi, mentre i metadati non filtrabili non possono essere utilizzati nei filtri ma possono archiviare grandi quantità di dati entro i limiti di dimensione. Per ulteriori informazioni sui limiti dei metadati, inclusi i limiti di dimensione per vettore e il numero massimo di chiavi di metadati per vettore, consulta [Limitazioni e restrizioni](#).

S3 Vectors esegue la ricerca vettoriale e la valutazione dei filtri contemporaneamente. S3 Vectors cerca i vettori candidati nell'indice per trovare i primi K vettori simili e contemporaneamente verifica se

ogni vettore candidato soddisfa le condizioni di filtro dei metadati. Ad esempio, se cerchi embedding di film simili e filtri per `genre='mystery'`, S3 Vectors restituisce solo embedding di film simili in cui i metadati di genere corrispondono a `'mystery'`. A differenza dell'utilizzo del filtro dei metadati dopo la ricerca vettoriale, questo approccio di filtro ha maggiori probabilità di trovare risultati corrispondenti. Nota: le query con filtri possono restituire un numero inferiore ai primi K risultati quando l'indice vettoriale contiene pochissimi risultati corrispondenti.

Argomenti

- [Metadati filtrabili](#)
- [Esempi di metadati filtrabili validi](#)
- [Metadati non filtrabili](#)

Metadati filtrabili

I metadati filtrabili consentono di filtrare i risultati delle query in base a valori di metadati specifici. Per impostazione predefinita, tutti i campi di metadati sono filtrabili in una query di somiglianza, a meno che non siano stati esplicitamente specificati come non filtrabili durante la creazione dell'indice vettoriale. S3 Vectors supporta i metadati di tipo stringa, numerico, booleano ed elenco con un limite di dimensione per vettore. Il tipo di metadati è ideale per definire gli attributi in base ai quali si desidera filtrare, come categorie, timestamp o valori di stato.

Se la dimensione dei metadati supera i limiti supportati, l'operazione [PutVectors](#) API restituirà un `400 Bad Request` errore. Per ulteriori informazioni sul limite di dimensione dei metadati filtrabili per vettore, consulta [Limitazioni e restrizioni](#).

Con i metadati filtrabili si possono utilizzare le operazioni indicate di seguito.

Operatore	Tipi di input validi	Description
<code>\$eq</code>	Stringa, numero, booleano	Confronto delle corrispondenze esatte per singoli valori. Quando si confronta con un valore di metadati di un'array, restituisce <code>true</code> se il valore di input corrisponde a un elemento dell'array.

Operatore	Tipi di input validi	Description
		y. Ad esempio, {"category": {"\$eq": "documentary"}} corrisponde un vettore con metadati "category": ["documentary", "romance"] .
\$ne	Stringa, numero, booleano	Confronto non uguale
\$gt	Numero	Confronto maggiore di
\$gte	Numero	Confronto maggiore di o uguale a
\$lt	Numero	Confronto minore di
\$lte	Numero	Confronto minore di o uguale a
\$in	Array di primitivi non vuota	Corrispondenza con un valore dell'array
\$nin	Array di primitivi non vuota	Corrispondenza con nessun valore dell'array
\$exists	Booleano	Controllo dell'esistenza del campo
\$and	Array di filtri non vuota	AND logico di più condizioni
\$or	Array di filtri non vuota	OR logico di più condizioni

Esempi di metadati filtrabili validi

Uguaglianza semplice

```
{"genre": "documentary"}
```

Questo filtro corrisponde i vettori in cui la chiave di metadati `genre` è uguale a `"documentary"`.

Quando non si specifica un operatore, S3 Vectors utilizza automaticamente l'operatore `$eq`.

Uguaglianza esplicita

```
// Example: Exact match
{"genre": {"$eq": "documentary"}}
```

```
// Example: Not equal to
{"genre": {"$ne": "drama"}}
```

Confronto numerico

```
{"year": {"$gt": 2019}}
```

```
{"year": {"$gte": 2020}}
```

```
{"year": {"$lt": 2020}}
```

```
{"year": {"$lte": 2020}}
```

Operazioni sugli array

```
{"genre": {"$in": ["comedy", "documentary"]}}
```

```
{"genre": {"$nin": ["comedy", "documentary"]}}
```

Controllo dell'esistenza

```
{"genre": {"$exists": true}}
```

Il filtro `$exists` corrisponde i vettori che hanno la chiave di metadati `"genre"`, indipendentemente dal valore archiviato per la chiave di metadati.

Operazioni logiche

```
{"$and": [{"genre": {"$eq": "drama"}}, {"year": {"$gte": 2020}]}
```

```
{"$or": [{"genre": {"$eq": "drama"}}, {"year": {"$gte": 2020}}]}
```

Intervallo di prezzo (più condizioni sullo stesso campo)

```
{"price": {"$gte": 10, "$lte": 50}}
```

Per ulteriori informazioni su come eseguire query sui vettori con il filtro dei metadati, consulta [Filtro dei metadati](#).

Metadati non filtrabili

I metadati non filtrabili non possono essere utilizzati nei filtri di query, ma possono archiviare quantità maggiori di dati contestuali rispetto ai metadati filtrabili. Sono l'ideale per archiviare blocchi di testo di grandi dimensioni, descrizioni dettagliate o altre informazioni contestuali che non devono necessariamente essere ricercabili ma possono essere restituiti con i risultati delle query. Ad esempio, è possibile archiviare il testo completo di un documento, le descrizioni di immagini o le specifiche dettagliate del prodotto come metadati non filtrabili.

Le chiavi di metadati non filtrabili devono essere configurate in modo esplicito durante la creazione dell'indice vettoriale. Una volta che una chiave di metadati è stata definita come non filtrabile durante la creazione dell'indice, non può essere modificata in un secondo momento per renderla filtrabile. Per ogni indice vettoriale è possibile configurare più chiavi di metadati come non filtrabili, con ciascun nome di chiave di metadati limitato a 63 caratteri. Per ulteriori informazioni sul numero massimo di chiavi di metadati non filtrabili consentite per indice vettoriale, consulta [Limitazioni e restrizioni](#).

Sebbene non sia possibile filtrare i metadati non filtrabili, è possibile recuperarli insieme ai risultati delle query utilizzando il parametro `return-metadata`. È possibile utilizzare i metadati non filtrabili per alcuni casi d'uso, come descritto di seguito.

- Per fornire un contesto all'applicazione senza analizzare origini dati separate.
- Per archiviare grandi blocchi di testo che supererebbero i limiti di dimensione dei metadati filtrabili.
- Includilo nelle esportazioni vettoriali utilizzando l'operazione [ListVectors](#) API.

Per ulteriori informazioni sulla configurazione dei metadati non filtrabili, consulta [Creazione di un indice vettoriale in un bucket vettoriale](#).

Limitazioni e restrizioni

Amazon S3 Vectors presenta alcune limitazioni e restrizioni di cui dovresti essere a conoscenza quando pianifichi le tue applicazioni di ricerca e archiviazione vettoriale.

- Bucket vettoriali per AWS regione in un account: 10.000
- Indici vettoriali per bucket vettoriale: 10.000
- Vettori per indice vettoriale: fino a 2 miliardi
- Valore della dimensione per vettore: da 1 a 4.096
- Metadati totali per vettore: fino a 40 KB (filtrabili + non filtrabili)
- Chiavi di metadati totali per vettore: fino a 50
- Metadati filtrabili per vettore: fino a 2 KB
- Non-filterable chiavi di metadati per indice vettoriale: fino a 10
- DeleteVectors Combinazioni PutVectors e richieste al secondo per indice vettoriale: fino a 1.000
- Vettori combinati inseriti ed eliminati al secondo per indice vettoriale: fino a 2.500
- Dimensione del payload della richiesta: fino a 20 MiB
- Vettori per chiamata [PutVectors](#)API: fino a 500
- Vettori per chiamata [DeleteVectors](#)API: fino a 500
- Vettori per chiamata [GetVectors](#)API: fino a 100
- Top-K risultati per [QueryVectors](#)richiesta: fino a 10.000
- Risultati per pagina in una [QueryVectors](#)risposta: fino a 100
- Vettori elencati per pagina in una [ListVectors](#)risposta: fino a 1.000
- Bucket vettoriali elencati per pagina in una [ListVectorBuckets](#)risposta: fino a 500.
- Indici vettoriali elencati per pagina in una [ListIndexes](#)risposta: fino a 500.
- Numero di segmenti per l'elenco parallelo in una chiamata ListVectors API: fino a 16

Best practice per S3 Vectors

Amazon S3 Vectors offre un'archiviazione vettoriale personalizzata e ottimizzata in termini di costi per le applicazioni abilitate per l'intelligenza artificiale e la ricerca semantica dei contenuti archiviati in Amazon S3. Progettato per fornire elasticità e durata a livello S3 per l'archiviazione di set di dati vettoriali con prestazioni di query inferiori al secondo per le query fredde e fino a 100 millisecondi per le query calde, S3 Vectors è ideale per le applicazioni che devono creare e far crescere indici vettoriali. Con S3 Vectors è possibile utilizzare un set dedicato di operazioni API per archiviare, accedere ed eseguire query di somiglianza su dati vettoriali senza dover allocare alcuna infrastruttura. Per ulteriori informazioni, consulta [Utilizzo di S3 Vectors e bucket vettoriali](#).

Per ottenere il massimo vantaggio da S3 Vectors, è consigliabile eseguire le best practice riportate di seguito.

Inserimento ed eliminazione di vettori

L'applicazione può ottenere fino a mille [PutVectorsDeleteVectors](#) richieste al secondo per indice vettoriale oppure può inserire o eliminare fino a duemilacinquecento vettori al secondo per indice vettoriale, a seconda del limite raggiunto per primo. Se si supera la frequenza di richiesta, potrebbe essere generato un errore 429 `TooManyRequestsException`.

Per ottimizzare i costi, consigliamo di inserire ed eliminare i vettori in batch di grandi dimensioni, fino alla dimensione massima del batch di 500 vettori per richiesta API. Se il carico di lavoro richiede batch più piccoli, puoi inviare richieste simultanee fino al limite di 1.000 richieste al secondo. Per raggiungere la velocità massima di 2.500 vettori al secondo, puoi inviare 5 batch al secondo con 500 vettori ciascuno o 1.000 batch al secondo con una media di 2,5 vettori ciascuno.

Accesso e query sui vettori in un indice vettoriale S3

La tua applicazione può raggiungere centinaia di [ListVectors](#) richieste al secondo per [QueryVectors](#) indice [GetVectors](#) vettoriale S3. Se si supera la frequenza di richiesta, potrebbe essere generato un errore 429 `TooManyRequestsException`. È consigliabile utilizzare un meccanismo di tentativi e di configurare l'applicazione per inviare meno richieste.

Dimensionamento tra indici vettoriali

Per migliorare le prestazioni delle query per indice vettoriale, si può considerare la possibilità di configurare l'applicazione in modo da dividere i vettori tra più indici vettoriali, ove possibile. Ad esempio, se sono presenti carichi di lavoro multi-tenant e l'applicazione esegue query su ciascun tenant in modo indipendente, è possibile archiviare i vettori di ciascun tenant in un indice vettoriale separato. Per ulteriori informazioni, consulta [Indici vettoriali](#).

Implementazione della multi-tenancy con indici vettoriali separati

È possibile ottenere la multi-tenancy organizzando i dati vettoriali con un unico indice vettoriale per ogni tenant. È possibile utilizzare le policy di bucket e IAM per limitare l'accesso di ogni tenant al solo indice vettoriale designato. Questo approccio aiuta a mantenere l'isolamento dei dati e semplifica la gestione eliminando la necessità di creare bucket separati per ogni tenant. Per ulteriori informazioni, consulta [Identity and Access Management in S3 Vectors](#).

Configurazione di campi di metadati non filtrabili per indici vettoriali

Quando si crea un indice vettoriale, i campi di metadati che non richiedono il filtro si configurano come chiavi di metadati non filtrabili. Ad esempio, è possibile archiviare i blocchi di testo per gli embedding vettoriali come campi di metadati non filtrabili se sono necessari solo come riferimento. Per ulteriori informazioni, consulta [Metadati non filtrabili](#).

Creazione di embedding vettoriali ed esecuzione di ricerche semantiche con **s3vectors-embed-cli**

Amazon S3 Vectors fornisce uno strumento open source autonomo chiamato la CLI di Amazon S3 Vectors Embed (`s3vectors-embed-cli`) che semplifica il lavoro con i dati vettoriali combinando la generazione di embedding con le operazioni vettoriali in singoli comandi. Questo strumento la CLI ti aiuta a iniziare rapidamente a utilizzare S3 Vectors automatizzando la generazione degli embedding vettoriali tramite i modelli di fondazione di Amazon Bedrock e le operazioni di ricerca semantica all'interno degli indici vettoriali.

S3 Vectors Embed CLI fornisce due comandi principali per l'integrazione dei modelli di embedding di Amazon Bedrock con le operazioni di S3 Vectors:

- `s3vectors-embed put`: genera e inserisce embedding vettoriali in un indice vettoriale. Nello specifico, converte testo e immagini in embedding vettoriali tramite modelli di Amazon Bedrock e li archivia automaticamente nell'indice vettoriale.
- `s3vectors-embed query`: genera embedding vettoriali dall'input delle query tramite modelli di Amazon Bedrock e vettori di query nell'indice vettoriale.

[L'Amazon S3 Vectors Embed CLI è disponibile nel repository Amazon Web Services - Labs. GitHub](#)

Per istruzioni di installazione dettagliate, parametri di comando, esempi e best practice, consulta il repository CLI di [Amazon S3 Vectors Embed](#). GitHub

Per le operazioni API S3 Vectors di livello inferiore che offrono maggiore controllo e personalizzazione, consulta [Amazon S3 Vectors](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di S3 Vectors con altri servizi AWS

S3 Vectors si integra con altri AWS servizi per migliorare le capacità di elaborazione vettoriale e fornire soluzioni complete per carichi di lavoro di intelligenza artificiale e apprendimento automatico. Queste integrazioni consentono di sfruttare lo storage conveniente di S3 Vectors insieme alle funzionalità specializzate di altri servizi. AWS

Integrazioni disponibili

S3 Vectors fornisce integrazioni native con i seguenti servizi: AWS

- [Amazon OpenSearch Service](#)- Puoi esportare un'istantanea di un indice vettoriale in Amazon OpenSearch Service per query ad alta frequenza (QPS) e ricerche vettoriali a bassa latenza. Inoltre, Amazon OpenSearch Service aggiunge Amazon S3 Vectors come nuovo motore a basso costo per i clienti che desiderano ottimizzare i costi continuando a utilizzare le operazioni Amazon OpenSearch Service API per funzionalità di ricerca avanzate tra cui ricerca ibrida, aggregazioni, filtri avanzati, ricerca sfaccettata e altro ancora.
- [Amazon Bedrock Basi di conoscenza](#): usa S3 Vectors come archivio vettoriale per le applicazioni Retrieval Augmented Generation (RAG), riducendo i costi di storage e mantenendo le prestazioni delle query per le operazioni della knowledge base. Puoi accedere a questa integrazione tramite la console Amazon Bedrock o [Amazon SageMaker AI Unified Studio](#).

Vantaggi dell'integrazione

Queste integrazioni offrono numerosi vantaggi:

- **Ottimizzazione dei costi:** archivia set di dati vettoriali di grandi dimensioni in modo conveniente in S3 Vectors utilizzando servizi specializzati per carichi di lavoro specifici, come Amazon per funzionalità di ricerca avanzate. OpenSearch
- **Flessibilità delle prestazioni:** scegli l'integrazione giusta per i tuoi requisiti prestazionali, con S3 Vectors per l'archiviazione a un throughput più basso e query sporadiche, e altri servizi per operazioni ad alto throughput e bassa latenza.

- Integrazione del flusso di lavoro: integra senza problemi le operazioni vettoriali nelle pipeline di intelligenza artificiale e ML esistenti. AWS
- Gestione semplificata: riduci la complessità operativa utilizzando integrazioni gestite anziché creare soluzioni personalizzate.

Argomenti

- [Utilizzo di vettori S3 con servizio OpenSearch](#)
- [Utilizzo di S3 Vectors con Knowledge Base per Amazon Bedrock](#)

Utilizzo di vettori S3 con servizio OpenSearch

Amazon S3 Vectors si integra con OpenSearch per fornire funzionalità di ricerca e archiviazione vettoriale flessibili. Questa integrazione consente di ottimizzare i costi archiviando i vettori in S3 Vectors e sfruttando al contempo le funzionalità di ricerca avanzate di OpenSearch.

Esistono due integrazioni tra S3 Vectors e OpenSearch. Una consiste nell'esportare i dati vettoriali da S3 Vectors a Serverless per funzionalità di ricerca ad OpenSearch alte prestazioni. L'altro utilizza S3 Vectors come motore di archiviazione economico, pur mantenendo l'accesso alle funzionalità OpenSearch.

OpenSearch Esporta in formato Serverless

Puoi esportare indici vettoriali da S3 Vectors a raccolte OpenSearch Serverless per operazioni di ricerca ad alte prestazioni, ricerca ibrida, aggregazioni, filtri avanzati e ricerca sfaccettata. Quando esporti, i dati vengono copiati su OpenSearch Serverless rimanendo in S3 Vectors, il che significa che pagherai per entrambi i servizi durante questo periodo.

Quando utilizzare questa integrazione

Prendi in considerazione l'esportazione in OpenSearch Serverless da S3 Vectors quando hai bisogno di quanto segue:

- Funzionalità di ricerca ibrida che combinano la somiglianza vettoriale con la ricerca per parole chiave.
- Elevato throughput delle query per carichi di lavoro impegnativi.
- Risposte a bassa latenza per applicazioni in tempo reale che richiedono tempi di risposta nell'ordine di millisecondi.

- Analisi avanzate che includono aggregazioni, ricerca con facet e filtri complessi.

Prerequisiti

Prima di utilizzare S3 Vectors con OpenSearch, assicurati di disporre di quanto segue:

- Un bucket vettoriale S3 esistente con indici vettoriali contenenti i dati.
- Autorizzazioni IAM appropriate sia per S3 Vectors che per Service. OpenSearch
- Una comprensione dei requisiti prestazionali per scegliere il metodo di integrazione appropriato.

Nozioni di base

Usando il Console di gestione AWS

Per esportare dati vettoriali in OpenSearch

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket di vettori.
3. Nell'elenco dei bucket vettoriali, scegli il nome del bucket contenente i dati vettoriali che desideri esportare.
4. Per Indici vettoriale, scegli il pulsante di opzione accanto all'indice vettoriale che desideri esportare.
5. Scegli Esporta ricerca avanzata, quindi scegli Esporta in OpenSearch.

Important

- Point-in-time esportazione: L'esportazione acquisisce i dati fino all'inizio dell'esportazione. Se aggiorni i tuoi dati vettoriali durante l'inserimento di OpenSearch, non tutti gli aggiornamenti si rifletteranno. OpenSearch
- Operazione una tantum: si tratta di un'esportazione una tantum che non viene sincronizzata con i dati di S3 Vectors. È necessario ripetere manualmente l'esportazione per acquisire eventuali modifiche successive.

Quindi, per configurare e gestire l'integrazione di S3 Vectors con Amazon OpenSearch Service, lavorerai principalmente tramite la OpenSearch console.

Per visualizzare le esportazioni in OpenSearch

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket di vettori.
3. Nell'elenco dei bucket vettoriali, scegli il nome del bucket contenente i dati vettoriali che desideri esportare.
4. Per gli indici vettoriali, scegli Esportazione di ricerca avanzata, quindi scegli Visualizza esportazioni in. OpenSearch

Quindi, visualizzerai le esportazioni OpenSearch tramite la console. OpenSearch

Per ulteriori informazioni sulla creazione e la gestione di raccolte OpenSearch Serverless, consulta [Creazione e gestione di raccolte Serverless di Amazon OpenSearch Service](#) nella Amazon OpenSearch Service Developer Guide.

OpenSearch con motore S3 Vectors

Puoi utilizzare S3 Vectors come motore di storage sottostante per i [cluster Amazon OpenSearch Managed](#), fornendo storage vettoriale ottimizzato in termini di costi pur mantenendo la funzionalità. OpenSearch

Quando utilizzare questa integrazione

Prendi in considerazione l'utilizzo OpenSearch con il motore S3 Vectors quando hai bisogno di quanto segue:

- Funzionalità di ricerca ibrida che combinano la somiglianza vettoriale con la ricerca per parole chiave.
- Riduzione del throughput delle query con modelli di utilizzo meno frequenti o sporadici.
- Maggiore tolleranza di latenza per le applicazioni in grado di accettare tempi di risposta più lunghi in cambio di costi più contenuti.
- Analisi avanzate che includono aggregazioni, ricerca con facet e filtri complessi.
- OpenSearch Flussi di lavoro esistenti che desideri estendere con uno storage vettoriale conveniente.

Prerequisiti

Prima di utilizzarlo OpenSearch con il motore S3 Vectors, assicurati di avere:

- Un dominio OpenSearch gestito esistente. Per ulteriori informazioni, consulta [Creazione e gestione di domini Amazon OpenSearch Service](#) nella Amazon OpenSearch Service Developer Guide.
- Una comprensione dei requisiti prestazionali per scegliere il metodo di integrazione appropriato.

Nozioni di base

Per utilizzarlo OpenSearch con il motore S3 Vectors, imposta il motore su `S3_Vectors` durante la creazione dell'indice in OpenSearch. Per ulteriori informazioni sul modello utilizzato per la creazione di un indice in OpenSearch Service, incluso dove specificare il tipo di motore, consulta [Metodi e motori](#). Per ulteriori informazioni sull'integrazione tra OpenSearch e il motore S3 Vectors, consulta Funzionalità di [ricerca avanzate con un motore S3 Vectors nella](#) Amazon OpenSearch Service Developer Guide.

Utilizzo di S3 Vectors con Knowledge Base per Amazon Bedrock

S3 Vectors si integra con [Amazon Bedrock Knowledge Bases e Amazon SageMaker AI Unified Studio](#) per semplificare e ridurre il costo dello storage vettoriale per le applicazioni RAG (Retrieval Augmented Generation).

Per ulteriori informazioni sui comandi CLI di alto livello che integrano i modelli di incorporamento di Amazon Bedrock con le operazioni di S3 Vectors, consulta. [Creazione di embedding vettoriali ed esecuzione di ricerche semantiche con `s3vectors-embed-cli`](#)

Argomenti

- [Panoramica dell'integrazione](#)
- [Quando utilizzare questa integrazione](#)
- [Modelli di embedding supportati](#)
- [Prerequisiti e autorizzazioni](#)
- [Creazione di una knowledge base con S3 Vectors](#)
- [Gestione e interrogazione della knowledge base](#)
- [Limitazioni](#)

Panoramica dell'integrazione

Quando crei una knowledge base in Amazon Bedrock, puoi selezionare S3 Vectors come archivio vettoriale. Questa integrazione offre i seguenti vantaggi:

- Risparmio sui costi per le applicazioni RAG con set di dati vettoriali di grandi dimensioni.
- Perfetta integrazione con il flusso di lavoro RAG completamente gestito di Amazon Bedrock.
- Gestione vettoriale automatica tramite il servizio Amazon Bedrock.
- Sub-second latenza delle query a freddo e latenza delle query a caldo di soli 100 millisecondi per le operazioni di recupero della knowledge base.

Knowledge Base per Amazon Bedrock fornisce un flusso di lavoro RAG end-to-end completamente gestito. Quando crei una knowledge base con S3 Vectors, Amazon Bedrock recupera automaticamente i dati dall'origine dati S3, converte i contenuti in blocchi di testo, genera gli embedding e li archivia nell'indice vettoriale. È quindi possibile eseguire query sulla knowledge base e ottenere risposte basate sui blocchi recuperati dai dati di origine.

Quando utilizzare questa integrazione

Valuta di utilizzare S3 Vectors con Knowledge Base per Amazon Bedrock quando hai bisogno di quanto segue:

- Cost-effective archiviazione vettoriale per set di dati di grandi dimensioni in cui una latenza di query inferiore al secondo soddisfa i requisiti dell'applicazione.
- Recupero di documenti in base a testo e immagini per casi d'uso come la ricerca tra manuali, policy e contenuti visivi.
- Applicazioni RAG che danno priorità all'ottimizzazione dei costi di archiviazione rispetto alle risposte a latenza ultrabassa.
- Operazioni vettoriali gestite senza la necessità di imparare direttamente le operazioni API di S3 Vectors (puoi continuare a utilizzare le interfacce di Amazon Bedrock che già conosci).
- Long-term storage vettoriale con la durabilità e la scalabilità di Amazon S3

Questa integrazione è ideale per le organizzazioni che sviluppano applicazioni RAG e che devono cercare ed estrarre informazioni da contenuti di testo e immagini, laddove i vantaggi in termini di costo offerti da S3 Vectors siano in linea con requisiti di prestazioni delle query considerati accettabili.

Modelli di embedding supportati

Consulta i [modelli supportati per gli incorporamenti vettoriali](#) nella Amazon Bedrock User Guide.

Prerequisiti e autorizzazioni

Prima di creare una knowledge base con S3 Vectors, assicurati di disporre di quanto segue:

- Autorizzazioni IAM appropriate per entrambi i servizi S3 Vectors e Amazon Bedrock. Per ulteriori informazioni sulle autorizzazioni IAM per S3 Vectors, consulta [the section called “Identity and Access Management in S3 Vectors”](#). Per ulteriori informazioni sulle autorizzazioni IAM relative al tuo ruolo di servizio per Knowledge Base per Amazon Bedrock per accedere a S3 Vectors, consulta [Autorizzazioni per accedere all'archivio vettoriale in Amazon S3 Vectors](#) nella Guida per l'utente di Amazon Bedrock.
- Documenti di origine pronti per essere importati nella knowledge base.
- Conoscenza dei requisiti del modello di embedding.

Quando configuri le configurazioni di sicurezza, puoi scegliere un ruolo IAM che fornisce l'autorizzazione ad Amazon Bedrock per accedere ai servizi richiesti AWS . Puoi lasciare che Amazon Bedrock crei il ruolo di servizio o utilizzi un ruolo personalizzato. Se utilizzi un ruolo personalizzato, configura una policy di bucket vettoriale che limiti l'accesso al bucket vettoriale e all'indice vettoriale al solo ruolo personalizzato.

Per informazioni dettagliate sulle autorizzazioni richieste e sui ruoli IAM, consulta [Creazione di un ruolo di servizio per Knowledge Base per Amazon Bedrock](#) nella Guida per l'utente di Amazon Bedrock. Il ruolo di servizio deve inoltre disporre delle autorizzazioni per S3 Vectors e le operazioni API. AWS KMS

Creazione di una knowledge base con S3 Vectors

Esistono due metodi per creare una knowledge base che utilizza S3 Vectors.

Metodo 1: utilizzando la console Amazon Bedrock

Quando crei una knowledge base nella console Amazon Bedrock, puoi selezionare “Bucket vettoriale S3” come opzione di archiviazione vettoriale. Sono disponibili due opzioni di configurazione:

- Creazione rapida di un nuovo archivio vettoriale: Amazon Bedrock crea un bucket vettoriale S3 e un indice vettoriale, configurandoli con le impostazioni richieste. Per impostazione predefinita,

il bucket vettoriale viene crittografato utilizzando la crittografia lato server con chiavi gestite di Amazon S3 (). SSE-S3 Facoltativamente, puoi crittografare il bucket utilizzando AWS KMS Per ulteriori informazioni sulla creazione rapida di un nuovo archivio vettoriale nella console, consulta [Creazione di una knowledge base collegandosi a un'origine dati in Knowledge Base per Amazon Bedrock](#) nella Guida per l'utente di Amazon Bedrock.

- Selezione di un archivio vettoriale già creato: seleziona un bucket vettoriale S3 e un indice vettoriale esistenti dall'account che hai creato in precedenza. Per ulteriori informazioni sulla creazione di un bucket vettoriale S3 e di un indice vettoriale nella console di Knowledge Base per Amazon Bedrock, vedi la scheda S3 Vectors in [Prerequisiti per l'utilizzo di un archivio vettoriale creato per una knowledge base](#) nella Guida per l'utente di Amazon Bedrock.

Per istruzioni dettagliate, consulta [Creazione di una knowledge base collegandosi a un'origine dati in Knowledge Base per Amazon Bedrock](#) nella Guida per l'utente di Amazon Bedrock.

Metodo due: usare Amazon SageMaker Unified Studio

Puoi anche creare e gestire basi di conoscenza con S3 Vectors tramite Amazon Bedrock in [Amazon SageMaker AI Unified Studio](#). che consiste in un ambiente di sviluppo unificato per creare e testare applicazioni di intelligenza artificiale che utilizzano basi di conoscenza.

[Amazon Bedrock in SageMaker AI Unified Studio](#) è progettato per gli utenti che necessitano di funzionalità notebook integrate e lavorano su più servizi di AWS ML e analisi. Puoi creare rapidamente un bucket vettoriale S3 e configurarlo come archivio vettoriale per le tue knowledge base quando crei applicazioni di IA generativa.

Per informazioni sull'uso di S3 Vectors con Amazon Bedrock in SageMaker AI Unified Studio, consulta [Aggiungere una fonte di dati alla tua app Amazon Bedrock](#) nella Guida per l'utente di SageMaker AI Unified Studio.

Gestione e interrogazione della knowledge base

Sincronizzazione e gestione dei dati

Knowledge Base per Amazon Bedrock offre operazioni basate su processi di acquisizione per garantire la sincronizzazione tra l'origine dati e gli embedding vettoriali. Quando sincronizzi l'origine dati, Amazon Bedrock scansiona ogni documento e verifica se è stato indicizzato nell'archivio vettoriale. Puoi anche indicizzare direttamente i documenti nell'archivio vettoriale utilizzando l'operazione. [IngestKnowledgeBaseDocuments](#) Al fine di garantire la sincronizzazione dei dati, è buona prassi creare un archivio vettoriale separato per ogni knowledge base.

Quando elimini una knowledge base o una risorsa di origine dati, Amazon Bedrock offre due policy di eliminazione dei dati: `Delete` (predefinita) e `Retain`. Se scegli la policy `Delete`, i vettori nell'indice vettoriale e nel bucket vettoriale vengono eliminati automaticamente.

Interrogazione e recupero

Dopo aver configurato la knowledge base, è possibile:

- Recuperare i blocchi dai dati di origine utilizzando l'operazione [Retrieve](#) dell'API.
- Genera risposte basate sui blocchi recuperati utilizzando l'operazione API. [RetrieveAndGenerate](#)
- Provare le query direttamente nella console Amazon Bedrock.

Le risposte vengono restituite con citazioni che rimandano ai dati di origine.

Limitazioni

Quando usi S3 Vectors con Knowledge Base per Amazon Bedrock, è importante conoscere le seguenti limitazioni:

- Solo ricerca semantica: S3 Vectors supporta la ricerca semantica, ma non le funzionalità di ricerca ibrida.
- Limiti delle dimensioni in S3 Vectors: ogni vettore presenta sia un limite sulle dimensioni totali dei metadati sia un limite sulle dimensioni dei metadati filtrabili. Ciò potrebbe ridurre la quantità di metadati personalizzati e le opzioni di filtraggio disponibili. Quando usi S3 Vectors come archivio vettoriale con Amazon Bedrock Knowledge Bases, puoi allegare fino a 1 KB di metadati personalizzati e 35 chiavi di metadati per vettore.
- Vincoli della strategia di suddivisione in blocchi: quando utilizzi un numero di token molto elevato con suddivisione in blocchi gerarchici nelle Knowledge Base di Amazon Bedrock, puoi superare i limiti massimi di dimensione dei metadati poiché le relazioni tra blocchi padre-figlio e il contesto gerarchico vengono archiviati come metadati non filtrabili in S3 Vectors. Per ulteriori informazioni sui limiti di [Limitazioni e restrizioni](#) dimensione dei metadati per vettore, consulta.
- Floating-point solo vettori: gli incorporamenti vettoriali binari non sono supportati.

Per una guida completa su come lavorare con Knowledge Base per Amazon Bedrock, consulta [Recupero dei dati e generazione di risposte basate su IA con Knowledge Base per Amazon Bedrock](#) nella Guida per l'utente di Amazon Bedrock.

Regioni AWS, endpoint e quote per S3 Vectors

Le seguenti sezioni includono le AWS regioni supportate e le quote di servizio per Amazon S3 Vectors.

S3 Vectors AWS Regioni ed endpoint

Amazon S3 Vectors è attualmente disponibile nelle seguenti regioni. AWS Per connetterti in modo programmatico a un AWS servizio, utilizzi un endpoint. Per ulteriori informazioni sugli endpoint AWS del servizio, vedere gli endpoint del [AWS servizio nella Guida](#) generale. AWS Per ulteriori informazioni sugli endpoint di Amazon S3, consulta gli endpoint e le quote di [Amazon S3 nella Guida generale](#). AWS

Gli endpoint di S3 Vectors sono endpoint dual-stack che supportano le richieste tramite protocollo IPv6 e IPv4.

S3 Vectors supporta la connettività privata con endpoint di interfaccia. AWS PrivateLink Per ulteriori informazioni, consulta [Endpoint VPC per S3 Vectors](#).

S3 Vectors AWS Regioni ed endpoint

Nome della region	Regione	Endpoint	Protocollo	Supporto versioni di firma
Africa (Città del Capo)	af-south-1	s3vectors.af-south-1.api.aws	HTTPS	4
Asia Pacific (Hong Kong)	ap-east-1	s3vectors.ap-east-1.api.aws	HTTPS	4
Asia Pacific (Hyderabad)	ap-south-2	s3vectors.ap-south-2.api.aws	HTTPS	4

Nome della regione	Regione	Endpoint	Protocollo	Supporto versioni di firma
Asia Pacific (Giappone)	ap-southeast-3	s3vectors.ap-southeast-3.api.aws	HTTPS	4
Asia Pacific (Malesia)	ap-southeast-5	s3vectors.ap-southeast-5.api.aws	HTTPS	4
Asia Pacific (Melbourne)	ap-southeast-4	s3vectors.ap-southeast-4.api.aws	HTTPS	4
Asia Pacific (Mumbai)	ap-south-1	s3vectors.ap-south-1.api.aws	HTTPS	4
Asia Pacific (Nuova Zelanda)	ap-southeast-6	s3vectors.ap-southeast-6.api.aws	HTTPS	4
Asia Pacific (Osaka-Local)	ap-northeast-3	s3vectors.ap-northeast-3.api.aws	HTTPS	4
Asia Pacific (Seoul)	ap-northeast-2	s3vectors.ap-northeast-2.api.aws	HTTPS	4

Nome della regione	Regione	Endpoint	Protocollo	Supporto versioni di firma
Asia Pacific (Singapore)	ap-southeast-1	s3vectors.ap-southeast-1.api.aws	HTTPS	4
Asia Pacific (Sydney)	ap-southeast-2	s3vectors.ap-southeast-2.api.aws	HTTPS	4
Asia Pacific (Taipei)	ap-east-2	s3vectors.ap-east-2.api.aws	HTTPS	4
Asia Pacific (Thailandia)	ap-southeast-7	s3vectors.ap-southeast-7.api.aws	HTTPS	4
Asia Pacific (Tokyo)	ap-northeast-1	s3vectors.ap-northeast-1.api.aws	HTTPS	4
AWS Europe Sovereign Cloud (Germania)	eusc-de-east-1	s3vectors.eusc-de-east-1.api.amazonaws.eu	HTTPS	4
AWS GovCloud (US-East)	us-gov-east-1	s3vectors.us-gov-east-1.api.aws	HTTPS	4

Nome della regione	Regione	Endpoint	Protocollo	Supporto versioni di firma
AWS GovCloud (US-West)	us-gov-west-1	s3vectors.us-gov-west-1.api.aws	HTTPS	4
Canada (Centro)	ca-central-1	s3vectors.ca-central-1.api.aws	HTTPS	4
Canada (Occidentale) (Calgary)	ca-west-1	s3vectors.ca-west-1.api.aws	HTTPS	4
Europa (Francoforte)	eu-central-1	s3vectors.eu-central-1.api.aws	HTTPS	4
Europa (Irlanda)	eu-west-1	s3vectors.eu-west-1.api.aws	HTTPS	4
Europa (Londra)	eu-west-2	s3vectors.eu-west-2.api.aws	HTTPS	4
Europa (Milano)	eu-south-1	s3vectors.eu-south-1.api.aws	HTTPS	4
Europa (Parigi)	eu-west-3	s3vectors.eu-west-3.api.aws	HTTPS	4
Europa (Spagna)	eu-south-2	s3vectors.eu-south-2.api.aws	HTTPS	4

Nome della regione	Regione	Endpoint	Protocollo	Supporto versioni di firma
Europa (Stoccolma)	eu-north-1	s3vectors.eu-north-1.api.aws	HTTPS	4
Europa (Zurigo)	eu-central-2	s3vectors.eu-central-2.api.aws	HTTPS	4
Messico (Centro)	mx-central-1	s3vectors.mx-central-1.api.aws	HTTPS	4
Sud America (San Paolo)	sa-east-1	s3vectors.sa-east-1.api.aws	HTTPS	4
US East (N. Virginia)	us-east-1	s3vectors.us-east-1.api.aws	HTTPS	4
Stati Uniti orientali (Ohio)	us-east-2	s3vectors.us-east-2.api.aws	HTTPS	4
Stati Uniti occidentali (California settentrionale)	us-west-1	s3vectors.us-west-1.api.aws	HTTPS	4

Nome della region	Regione	Endpoint	Protocollo	Supporto versioni di firma
Stati Uniti occidentali (Oregon)	us-west-2	s3vectors.us-west-2.api.aws	HTTPS	4

Quote di servizio di S3 Vectors

Le quote, note anche come limiti, sono il numero massimo di risorse o operazioni di servizio per l'account dell'utente. AWS I limiti sono le quote di servizio per le risorse di S3 Vectors.

Per i limiti dettagliati che si applicano a S3 Vectors, consulta [Limitazioni e restrizioni](#).

Salvo diversa indicazione, ogni quota è per AWS regione. Se per alcune quote è possibile richiedere aumenti, per altre non è possibile. Per ulteriori informazioni su come richiedere un aumento della quota, consulta [Come richiedere un aumento della quota](#) nella Guida per l'utente alle quote di servizio. Per ulteriori informazioni sulle quote di Amazon S3, consulta [Endpoint e quote di Amazon S3](#) nella Guida di riferimento generale di AWS .

Sicurezza in S3 Vectors

Amazon S3 Vectors fornisce un'archiviazione vettoriale con elevata durabilità. I dati scritti su S3 Vectors vengono archiviati su S3, che è progettato per garantire una durabilità dei dati del 99,999999999%.

S3 Vectors adotta un approccio alla sicurezza che include la crittografia dei dati inattivi e la trasmissione sicura dei dati. Che tu stia archiviando milioni di vettori per applicazioni di machine learning o sviluppando sistemi di ricerca semantica, S3 Vectors fornisce i controlli di sicurezza necessari per soddisfare i requisiti dell'organizzazione in materia di conformità e protezione dei dati.

Argomenti

- [Identity and Access Management in S3 Vectors](#)
- [Protezione e crittografia dei dati in S3 Vectors](#)

- [Endpoint VPC per S3 Vectors](#)

Identity and Access Management in S3 Vectors

La gestione degli accessi in S3 Vectors segue le migliori pratiche di AWS sicurezza, fornendo più livelli di controllo per garantire che solo gli utenti e le applicazioni autorizzati possano accedere ai dati vettoriali. Il servizio si integra con IAM e supporta le policy basate su identità e risorse, fornendo flessibilità nel modo in cui si strutturano e gestiscono le autorizzazioni all'interno dell'organizzazione.

Autenticazione e autorizzazione delle richieste

S3 Vectors utilizza meccanismi di autenticazione e autorizzazione AWS standard per proteggere l'accesso ai bucket vettoriali e ai relativi contenuti. Ogni richiesta a S3 Vectors deve essere autenticata utilizzando AWS credenziali valide e il servizio valuta le autorizzazioni in base alla combinazione di politiche basate sull'identità, politiche basate sulle risorse e qualsiasi politica di controllo del servizio applicabile.

Il processo di autenticazione inizia quando un client effettua una richiesta a S3 Vectors utilizzando AWS credenziali (chiavi di accesso, credenziali temporanee o ruoli IAM). AWS STS Il servizio convalida queste credenziali e quindi valuta le autorizzazioni associate all'identità autenticata in relazione all'azione richiesta e alla risorsa di destinazione. Questo processo di valutazione prende in considerazione diversi tipi di policy e applica il principio del privilegio minimo per determinare se consentire o rifiutare la richiesta.

L'autorizzazione in S3 Vectors funziona a più livelli di granularità. È possibile controllare l'accesso a livello di bucket vettoriale, a livello di indice vettoriale individuale o anche operazioni specifiche all'interno di un indice. Questo modello di autorizzazione gerarchico consente di implementare sofisticati schemi di controllo degli accessi in linea con la struttura organizzativa e i requisiti di governance dei dati.

Tipi di risorsa definiti per i bucket vettoriali

S3 Vectors definisce tipi di risorse specifici a cui è possibile fare riferimento nelle policy IAM e nelle policy basate su risorse. La comprensione di questi tipi di risorse è essenziale per creare policy di controllo degli accessi efficaci che forniscano il livello di accesso appropriato agli utenti e alle applicazioni corretti.

La tabella seguente descrive i tipi di risorsa disponibili in S3 Vectors.

Tipi di risorsa disponibili nei vettori S3

Tipo di risorsa	Formato ARN	Description
VectorBucket	<i>region</i> 123456789 012 arn:aws:s3vectors: ::bucket/ <i>bucket-name</i>	Rappresenta un bucket vettoriale e viene utilizzato per operazioni a livello di bucket come la creazione, l'eliminazione o la configurazione del bucket
Indice	arn:aws:s3vectors: ::bucket/ / index/ <i>region</i> 123456789 012 <i>bucket-name</i> <i>index-name</i>	Rappresenta un indice vettoriale all'interno di un bucket e viene utilizzato per operazioni specifiche dell'indice, come l'esecuzione di query sui vettori o la gestione del contenuto dell'indice

Azioni di policy per bucket vettoriali

S3 Vectors fornisce un set completo di azioni di policy che corrispondono alle varie operazioni che è possibile eseguire su bucket vettoriali e indici vettoriali. Queste azioni sono progettate per fornire un controllo granulare su chi può eseguire operazioni specifiche, consentendo di implementare efficacemente il principio del privilegio minimo.

La tabella seguente elenca tutte le azioni di policy disponibili per le risorse S3 Vectors.

Azioni di policy per risorse S3 Vectors

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
Account	ListVectorBuckets	vettori s3: ListVectorBuckets	Fornisce l'autorizzazione per elencare tutti i bucket	List	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
			vettoriali nell'account e nella Regione		
VectorBucket	CreateVectorBucket	vettori s3: CreateVectorBucket	Fornisce l'autorizzazione per creare un nuovo bucket vettoriale con la configurazione specificata	Scrittura	Vettori S3: tipo SSE, vettori s3: kmsKeyArn
VectorBucket	GetVectorBucket	vettori s3: GetVectorBucket	Fornisce l'autorizzazione per recuperare gli attributi e la configurazione del bucket vettoriale	Lettura	
VectorBucket	DeleteVectorBucket	vettori s3: DeleteVectorBucket	Fornisce l'autorizzazione per eliminare un bucket vettoriale vuoto	Scrittura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
VectorBucket	ListIndexes	vettori s3: ListIndexes	Fornisce l'autorizzazione per elencare tutti gli indici all'interno di un bucket vettoriale	List	
VectorBucket	PutVectorBucketPolicy	vettori s3: PutVectorBucketPolicy	Fornisce l'autorizzazione per applicare o aggiornare una policy basata su risorse di un bucket vettoriale	Gestione delle autorizzazioni	
VectorBucket	GetVectorBucketPolicy	vettori s3: GetVectorBucketPolicy	Fornisce l'autorizzazione per recuperare una policy basata su risorse collegata a un bucket vettoriale	Lettura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
VectorBucket	DeleteVectorBucketPolicy	vettori s3: DeleteVectorBucketPolicy	Fornisce l'autorizzazione per rimuovere la policy basata su risorse da un bucket vettoriale	Gestione delle autorizzazioni	
Indice	CreateIndex	vettori s3: CreateIndex	Fornisce l'autorizzazione per creare un nuovo indice vettoriale con dimensioni e configurazione dei metadati specificate	Scrittura	
Indice	GetIndex	vettori s3: GetIndex	Fornisce l'autorizzazione per recuperare gli attributi e la configurazione dell'indice vettoriale	Lettura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
Indice	DeleteIndex	vettori s3: DeleteIndex	Fornisce l'autorizzazione per eliminare un indice vettoriale e tutto il relativo contenuto	Scrittura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
Indice	QueryVectors	(Obbligatorie) s3vectors: QueryVectors	<p>Fornisce l'autorizzazione a eseguire query di somiglianza sui vettori di un indice.</p> <p>Solo con s3vectors:QueryVectors, è possibile recuperare e le chiavi dei vettori dei vicini più prossimi approssimativi e le relative distanze calcolate dal vettore di query. Questa autorizzazione è sufficiente solo quando non imposti alcun filtro</p>	Lettura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
			per i metadati e non richiedi i metadati (mantenendo il returnMetadata parametro impostato su false o non specificato).		

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
		(Condizionalmente richiesto): s3vector:GetVectors	<p>Obbligatorio se si impostano i filtri per i metadati, si imposta <code>returnMetadata</code> su <code>true</code> nella richiesta.</p> <p>Con s3vector:QueryVectors e s3vector:GetVectors, è possibile filtrare i risultati utilizzando i criteri di metadati e recuperare le chiavi di vettore insieme ai dati associati, ai metadati e alle distanze calcolate del</p>	Lettura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
			vettore di query.		
Indice	PutVectors	vettori s3: PutVectors	Fornisce l'autorizzazione per aggiungere o aggiornare vettori in un indice	Scrittura	
Indice	GetVectors	vettori s3: GetVectors	Fornisce l'autorizzazione per recuperare vettori specifici e i relativi metadati tramite la chiave di vettore	Lettura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
Indice	ListVectors	(Obbligatori) s3vectors: ListVectors	<p>Fornisce l'autorizzazione a elencare le chiavi di vettore in un indice.</p> <p>Solo con s3vectors:ListVectors, è possibile elencare le chiavi di vettore quando entrambi i parametri <code>returnData</code> e <code>returnMetadata</code> sono falsi o non sono specificati.</p>	Lettura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
		(Condizionalmente richiesto): s3vectors: GetVectors	<p>Obbligatorio se nella richiesta è impostato su true uno dei due parametri <code>returnData</code> e <code>returnMetadata</code>.</p> <p>Con s3vectors:ListVectors e s3vectors:GetVectors, è possibile recuperare le chiavi di vettore insieme ai dati e ai metadati associati impostando <code>returnData</code> e <code>returnMetadata</code> su true.</p>	Lettura	

Tipo di risorsa	operazioni API	Azioni di policy	Descrizione delle azioni delle policy	Livello di accesso	Chiavi di condizione
Indice	DeleteVectors	vettori s3: DeleteVectors	Fornisce l'autorizzazione a eliminare vettori specifici da un indice	Scrittura	

Queste azioni possono essere combinate in vari modi per creare policy che soddisfino i requisiti di accesso specifici. Ad esempio, è possibile creare una policy di sola lettura che includa le azioni `s3vectors:GetVectorBucket`, `s3vectors:ListIndexes`, `s3vectors:QueryVectors` e `s3vectors:GetVectors` oppure una policy che includa le autorizzazioni di query e recupero di vettori ma escluda le azioni amministrative come la creazione o l'eliminazione di indici.

Chiavi di condizione per bucket vettoriali

Chiavi di condizione per bucket vettoriali

	Chiavi di condizione	Descrizione	Tipo
1	<code>s3vectors:sseType</code>	Filtra l'accesso tramite il tipo di crittografia lato server. Valori validi: <code>AES256</code> <code>aws:kms</code>	Stringa
2	<code>vettori s3: kmsKeyArn</code>	Filtra l'accesso tramite la AWS AWS KMS chiave ARN per la chiave utilizzata per crittografare un bucket vettoriale	ARN

Esempi di policy basate sull'identità di S3 Vectors

Le policy IAM basate sull'identità sono documenti JSON che si collegano a utenti, gruppi o ruoli IAM per definire le operazioni che possono eseguire sulle risorse di S3 Vectors. Queste politiche vengono valutate nel contesto dell'identità che effettua la richiesta e forniscono un modo centralizzato per gestire le autorizzazioni in tutto l'ambiente. AWS Le policy basate sull'identità forniscono un chiaro audit trail delle autorizzazioni assegnate e possono essere aggiornate con facilità al variare delle esigenze di accesso.

Nel predisporre le policy basate sull'identità per S3 Vectors, è importante tenere in considerazione le varie tipologie di utenti e applicazioni che interagiranno con i dati vettoriali. Tra i modelli più comuni vi sono i data scientist che devono eseguire query sui vettori, i data engineer che devono caricare e gestire i dati vettoriali, gli amministratori che necessitano del pieno controllo della configurazione del bucket e le applicazioni che richiedono specifici permessi di accesso in lettura o scrittura su particolari indici vettoriali.

Policy di esempio

Policy di accesso amministrativa

Questa policy fornisce l'accesso amministrativo completo alle risorse S3 Vectors, adatta agli amministratori o ai team di piattaforma: DevOps

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAdministrativeAccess",
      "Effect": "Allow",
      "Action": [
        "s3vectors:CreateVectorBucket",
        "s3vectors:PutVectorBucketPolicy",
        "s3vectors>DeleteVectorBucket",
        "s3vectors>DeleteVectorBucketPolicy",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListVectorBuckets",
        "s3vectors>CreateIndex",
        "s3vectors>DeleteIndex",
        "s3vectors:GetIndex",
        "s3vectors:ListIndexes",

```

```

        "s3vectors:DeleteVectors",
        "s3vectors:GetVectors",
        "s3vectors:ListVectors",
        "s3vectors:PutVectors",
        "s3vectors:QueryVectors"
    ],
    "Resource": "*"
}
]
}

```

Policy di accesso specifica per l'applicazione

Questa policy è progettata per le applicazioni che devono eseguire operazioni specifiche su indici vettoriali designati:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowApplicationVectorAccess",
      "Effect": "Allow",
      "Action": [
        "s3vectors:QueryVectors",
        "s3vectors:GetVectors",
        "s3vectors:PutVectors",
        "s3vectors:ListVectors"
      ],
      "Resource": [
        "arn:aws:s3vectors:aws-region:123456789012:bucket/amzn-s3-demo-vector-bucket/index/product-recommendations",
        "arn:aws:s3vectors:aws-region:123456789012:bucket/amzn-s3-demo-vector-bucket/index/content-similarity"
      ]
    },
    {
      "Sid": "AllowGetIndex",
      "Effect": "Allow",
      "Action": "s3vectors:GetIndex",
      "Resource": "arn:aws:s3vectors:aws-region:123456789012:bucket/amzn-s3-demo-vector-bucket/index/*"
    },
    {

```

```
        "Sid": "AllowIndexInspection",
        "Effect": "Allow",
        "Action": "s3vectors:ListIndexes",
        "Resource": "arn:aws:s3vectors:aws-region:123456789012:bucket/amzn-s3-demo-
vector-bucket"
    }
  ]
}
```

Esempi di policy basate sulle risorse di S3 Vectors

Le policy basate su risorse sono collegate a una risorsa. È possibile creare policy basate sulle risorse per i bucket vettoriali. Le politiche basate sulle risorse per S3 Vectors utilizzano il formato di AWS policy standard in JSON che si collega direttamente ai bucket vettoriali per controllare l'accesso al bucket e al suo contenuto.

A differenza delle politiche basate sull'identità associate a utenti, gruppi o ruoli, le politiche basate sulle risorse sono collegate alla risorsa stessa (il bucket vettoriale) e possono concedere autorizzazioni ai principali di altri account. AWS Ciò le rende ideali per scenari in cui è necessario condividere dati vettoriali tra diversi ambiti organizzativi oppure implementare controlli di accesso granulari basati sulla specifica risorsa a cui si sta accedendo.

Le policy basate sulle risorse vengono valutate in combinazione con le policy basate sull'identità e le autorizzazioni effettive sono determinate dall'unione di tutte le policy applicabili. Ciò significa che un principale ha bisogno dell'autorizzazione sia dalla policy basata sull'identità (associata al suo utente/ruolo) sia dalla policy basata sulle risorse (associata al bucket) per eseguire un'azione, a meno che la policy basata sulle risorse non conceda esplicitamente tale autorizzazione.

Esempio 1: policy di accesso multi-account

Questa policy dimostra come concedere autorizzazioni specifiche agli utenti di account AWS diversi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountBucketAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam:123456789012:role/Admin"
      },

```

```

    "Action": [
      "s3vectors:CreateIndex",
      "s3vectors:ListIndexes",
      "s3vectors:QueryVectors",
      "s3vectors:PutVectors",
      "s3vectors>DeleteIndex"
    ],
    "Resource": [
      "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket/*",
      "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket"
    ]
  }
]
}

```

Esempio 2: negare le azioni a livello di indice vettoriale

Questa policy dimostra come negare azioni specifiche a livello di indice vettoriale a un ruolo IAM:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIndexLevelActions",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam:123456789012:role/External-Role-Name"
      },
      "Action": [
        "s3vectors:QueryVectors",
        "s3vectors:PutVectors",
        "s3vectors>DeleteIndex",
        "s3vectors:GetVectors",
        "s3vectors:GetIndex",
        "s3vectors>DeleteVectors",
        "s3vectors>CreateIndex",
        "s3vectors:ListVectors"
      ],
      "Resource": "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket/*"
    }
  ]
}

```

}

Esempio 3: negare le operazioni di modifica sia a livello di indice vettoriale che a livello di bucket

Questa policy dimostra come negare le richieste di modifica sia per l'indice vettoriale che per le azioni a livello di bucket specificando più risorse:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModificationActionsAtBucketandIndexLevels",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam:123456789012:role/External-Role-Name"
      },
      "Action": [
        "s3vectors:CreateVectorBucket",
        "s3vectors>DeleteVectorBucket",
        "s3vectors:PutVectorBucketPolicy",
        "s3vectors>DeleteVectorBucketPolicy",
        "s3vectors>CreateIndex",
        "s3vectors>DeleteIndex",
        "s3vectors:PutVectors",
        "s3vectors>DeleteVectors"
      ],
      "Resource": [
        "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket/*",
        "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket"
      ]
    }
  ]
}
```

Protezione e crittografia dei dati in S3 Vectors

Amazon S3 Vectors offre una durabilità del 99,999999999% (11 nove) per i dati vettoriali, garantendo un'affidabilità eccezionale per le esigenze di archiviazione vettoriale. Questa durabilità è supportata dall'infrastruttura collaudata di Amazon S3, progettata per mantenere l'integrità e la disponibilità dei dati anche in caso di guasti hardware o altre interruzioni.

La protezione dei dati in S3 Vectors comprende controlli di sicurezza a più livelli per proteggere i dati vettoriali sia a riposo sia in transito.

Per impostazione predefinita, tutti i nuovi bucket vettoriali di Amazon S3 Vectors utilizzano la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3). Quando crei un bucket vettoriale con crittografia SSE-S3, tutte le operazioni successive sul bucket utilizzano automaticamente questa crittografia.

S3 Vectors si integra anche con AWS Key Management Service (KMS) per fornire opzioni flessibili di gestione delle chiavi di crittografia, che consentono di scegliere chiavi gestite dal cliente per il controllo delle autorizzazioni e la verificabilità.

Quando si crea un indice vettoriale all'interno di un bucket vettoriale, è possibile opzionalmente sovrascrivere le impostazioni di crittografia a livello di bucket vettoriale e fornire una configurazione di crittografia (SSE-S3 o KMS) a livello di indice vettoriale. Se non viene specificata una crittografia specifica al momento della creazione dell'indice vettoriale, l'indice erediterà la configurazione di crittografia dal bucket vettoriale a cui appartiene.

Impostazione del comportamento di crittografia lato server per bucket e indici vettoriali Amazon S3

La configurazione della crittografia in S3 Vectors è un'impostazione di sicurezza fondamentale che si specifica quando si crea un bucket vettoriale. Questo approccio garantisce che tutti i dati vettoriali archiviati nel bucket siano crittografati sin dal momento della creazione. Per impostazione predefinita, la configurazione di crittografia si applica a tutti i vettori, gli indici vettoriali e i metadati all'interno del bucket, garantendo una protezione uniforme sull'intero set di dati vettoriali in un bucket vettoriale. È inoltre possibile sovrascrivere le impostazioni di crittografia a livello di bucket vettoriale e fornire una configurazione di crittografia dedicata (SSE-S3 o) a livello di indice vettoriale. AWS KMS

Important

Le impostazioni di crittografia di un bucket vettoriale non possono essere modificate dopo la creazione del bucket vettoriale. È necessario considerare con attenzione i requisiti di crittografia durante il processo di creazione del bucket, inclusi i requisiti di conformità, le preferenze di gestione delle chiavi e l'integrazione con l'infrastruttura di sicurezza esistente.

Quando si imposta il tipo di crittografia SSE-S3 o SSE-KMS a livello di bucket vettoriale, per impostazione predefinita si applica a tutti gli indici vettoriali e i vettori all'interno del bucket. La

configurazione della crittografia si applica non solo ai dati vettoriali, ma anche a tutti i metadati associati.

È inoltre possibile sovrascrivere le impostazioni di crittografia a livello di bucket vettoriale e fornire una configurazione di crittografia dedicata (SSE-S3 o KMS) a livello di indice vettoriale. Le impostazioni di crittografia per un indice vettoriale non possono essere modificate dopo la creazione dell'indice vettoriale.

Utilizzo della crittografia SSE-S3

La crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3) offre una soluzione di crittografia semplice ed efficace per bucket AWS vettoriali in cui gestisce tutti gli aspetti del processo di crittografia. Questo metodo di crittografia utilizza la crittografia AES-256 ed è progettato per fornire un elevato livello di sicurezza con un sovraccarico operativo minimo, offrendo alle organizzazioni una crittografia robusta senza la complessità delle esigenze di gestione delle chiavi di crittografia.

Con SSE-S3, Amazon S3 gestisce automaticamente la generazione, la rotazione e la gestione delle chiavi di crittografia. SSE-S3 offre una sicurezza avanzata senza richiedere altre operazioni di configurazione o una gestione continua. I processi di crittografia e decrittografia vengono gestiti automaticamente dal servizio e non sono previsti costi aggiuntivi per l'utilizzo della crittografia SSE-S3, oltre ai prezzi standard di S3 Vectors.

Utilizzo della crittografia SSE-KMS

La crittografia lato server con chiavi del servizio di gestione delle AWS chiavi (SSE-KMS) offre un controllo avanzato sulle chiavi di crittografia e consente una registrazione dettagliata dell'utilizzo delle chiavi. Questo metodo di crittografia è ideale per le organizzazioni con requisiti di conformità rigorosi, per quelle che devono implementare policy di rotazione delle chiavi personalizzate o per ambienti in cui sono richiesti audit trail dettagliati per l'accesso ai dati.

SSE-KMS consente di utilizzare chiavi gestite dal cliente (CMKs) per crittografare i dati vettoriali. Le chiavi gestite dal cliente offrono il massimo livello di controllo, consentendo di definire politiche chiave, abilitare o disabilitare le chiavi e monitorarne l'utilizzo. AWS CloudTrail Questo livello di controllo rende SSE-KMS particolarmente adatto per i settori regolamentati o le organizzazioni con requisiti specifici di governance dei dati.

Quando si utilizza SSE-KMS con chiavi gestite dal cliente, si ha il controllo completo su chi può utilizzare le chiavi per crittografare e decrittografare i dati. È possibile creare policy della chiave dettagliate che specificano quali utenti, ruoli o servizi possono accedere alle chiavi.

Considerazioni importanti per SSE-KMS

- Requisiti del formato della chiave KMS: S3 Vectors richiede di specificare le chiavi KMS utilizzando il formato del nome della risorsa Amazon (ARN) completo. Le chiavi IDs o gli alias delle chiavi non sono supportati.
- Autorizzazioni per il principale del servizio: quando si utilizzano le chiavi gestite dal cliente con S3 Vectors, è necessario fornire esplicitamente le autorizzazioni al principale del servizio S3 Vectors per utilizzare la chiave KMS. Questo requisito garantisce che il servizio possa crittografare e decrittografare i dati automaticamente. Il principale del servizio che richiede l'accesso è `indexing.s3vectors.amazonaws.com`.

Esempio: policy della chiave KMS per S3 Vectors

Per utilizzare una chiave KMS gestita dal cliente con S3 Vectors, è necessario aggiornare la policy della chiave in modo da includere le autorizzazioni per il principale del servizio S3 Vectors. Di seguito è riportato un esempio completo di policy della chiave.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3VectorsServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "indexing.s3vectors.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3vectors:aws-region:123456789012:bucket/"
        }
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ForAnyValue:StringEquals": {
        "kms:EncryptionContextKeys": ["aws:s3vectors:arn",
          "aws:s3vectors:resource-id"]
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "AllowApplicationAccess",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam:123456789012:role/VectorApplicationRole",
        "arn:aws:iam:123456789012:user/DataScientist"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "s3vectors.aws-region.amazonaws.com"
      },
      "ForAnyValue:StringEquals": {
        "kms:EncryptionContextKeys": ["aws:s3vectors:arn",
"aws:s3vectors:resource-id"]
      }
    }
  }
]
}

```

- Autorizzazioni KMS richieste:
 - Autorizzazione del principale del servizio S3 Vectors:
 - kms:Decrypt: richiesta dal principale del servizio S3 Vectors (indexing.s3vectors.amazonaws.com) sulla chiave gestita dal cliente per mantenere e ottimizzare l'indice nelle operazioni in background
 - Autorizzazioni del principale IAM:
 - kms:Decrypt— Obbligatorio per tutte le operazioni a livello vettoriale ([PutVectors](#),[GetVectors](#),[QueryVectorsDeleteVectorsListVectors](#))
 - kms:GenerateDataKey: richiesta per creare un bucket vettoriale utilizzando la chiave gestita dal cliente

- Considerazioni sull'accesso multi-account: quando si implementano modelli di accesso multi-account con SSE-KMS, è necessario assicurarsi che la policy della chiave KMS consenta l'accesso dai principali appropriati in altri account. Il formato dell'ARN della chiave diventa particolarmente importante negli scenari multi-account, in quanto fornisce un riferimento inequivocabile alla chiave indipendentemente dal contesto dell'account da cui si accede.

Impostazione della crittografia in S3 Vectors

Questo argomento spiega come impostare la configurazione di crittografia per i bucket e gli indici vettoriali S3.

Prima di iniziare, assicurati di disporre di:

- Autorizzazioni appropriate per visualizzare le proprietà del bucket e dell'indice.

Utilizzo della console S3

Come configurare la crittografia per un bucket vettoriale

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket di vettori.
3. Scegli Crea bucket di vettore.
4. In Nome bucket, immettere il nome del bucket.

Il nome del bucket deve:

- Sii unico all'interno del tuo account per questa regione AWS
 - Deve contenere un numero di caratteri compreso tra 3 a 63.
 - Essere costituito solo da lettere minuscole, numeri e trattini (-).
5. Per la crittografia, scegli
 - Specifica il tipo di crittografia: scegli un metodo di crittografia specifico:
 - Crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3): con SSE-S3, Amazon S3 gestisce automaticamente la generazione, la rotazione e la gestione delle chiavi di crittografia.
 - Crittografia lato server con chiavi del servizio di gestione delle AWS chiavi (SSE-KMS): simile a SSE-S3, ma utilizza chiavi gestite dal cliente () in KMS, offrendoti un maggiore

controllo sulle chiavi. CMKs AWS Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente](#) nella Guida per gli sviluppatori di Servizio AWS di gestione delle chiavi.

Se selezioni questa opzione, per Chiave AWS KMS scegli una delle seguenti opzioni:

- Scegli tra le tue chiavi KMS: seleziona una chiave AWS KMS esistente dall'elenco a discesa
- Inserisci l'ARN della chiave AWS KMS: inserisci l'Amazon Resource Name (ARN) di una chiave KMS
- Crea una chiave KMS: crea una nuova chiave gestita dal cliente nella console KMS. AWS Per ulteriori informazioni, consulta [Creazione di chiavi simmetriche gestite dal cliente](#) nella Guida per gli sviluppatori del Servizio AWS di gestione delle chiavi.

Note

Alla chiave KMS si applicano i seguenti requisiti:

- AWS L'ID della chiave KMS non deve essere vuoto
- La chiave KMS deve trovarsi nella stessa Regione in cui viene creato il bucket.
- AWS L'ARN della chiave KMS deve iniziare con «arn:aws:kms:»

Important

Le impostazioni di crittografia non possono essere modificate dopo la creazione del bucket vettoriale.

6. Se hai scelto Inserisci la chiave AWS KMS ARN, inserisci l'ARN nel campo di testo fornito.
7. Se hai scelto Crea una chiave KMS, la console apre la console AWS KMS in una nuova scheda. Per istruzioni sulla creazione di una chiave KMS, consulta [Creazione di chiavi simmetriche gestite dal cliente](#) nella Guida per gli sviluppatori del Servizio AWS di gestione delle chiavi.
8. Scegli Crea bucket di vettore.

 Important

Quando utilizzi la crittografia KMS, assicurati che i principali IAM che devono accedere agli oggetti nel bucket dispongano dell'autorizzazione KMS necessaria (kms:Decrypt) per la chiave KMS selezionata.

Per configurare la crittografia per un indice vettoriale

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket di vettori.
3. Nell'elenco dei bucket vettoriali, seleziona il nome del bucket in cui desideri creare un indice vettoriale.
4. Scegli Crea indice di vettore.
5. Per Nome dell'indice di vettore, inserisci un nome per l'indice vettoriale.

I nomi degli indici vettoriali devono essere univoci all'interno del bucket vettoriale. Il nome dell'indice deve essere composto da un numero di caratteri compreso tra 3 e 63. I caratteri validi sono lettere minuscole (a-z), numeri (0-9), trattini (-) e punti (.). Per ulteriori informazioni sui requisiti di denominazione dell'indice vettoriale, consulta [Regole di denominazione dei bucket vettoriali](#).

6. Per Dimensione, inserisci il numero di valori in ogni vettore.

 Note

- Il valore per Dimensione determina quanti valori numerici conterrà ogni vettore.
- Tutti i vettori aggiunti a questo indice devono avere esattamente questo numero di valori.
- La dimensione deve essere compresa tra 1 e 4096.
- Una dimensione più grande richiede più spazio di archiviazione.
- Scegli in base alle dimensioni di output del modello di embedding.

Per ulteriori informazioni sui requisiti di dimensione, consulta [Limitazioni e restrizioni](#).

7. Per Metrica della distanza, scegli una delle seguenti opzioni:
- Coseno: misura il coseno dell'angolo tra i vettori. Ideale per vettori normalizzati e quando la direzione è più importante della grandezza
 - Euclideo: misura la distanza in linea retta tra i vettori. Ideale quando sia la direzione sia la grandezza sono importanti.
8. (Facoltativo) In Metadati non filtrabili, configura le chiavi di metadati che verranno archiviate ma non utilizzate per il filtro:

Per aggiungere chiavi di metadati non filtrabili:

- a. Scegliere Add key (Aggiungi chiave).
- b. Inserisci un nome per la chiave (da 1 a 63 caratteri e univoco all'interno dell'indice vettoriale).
- c. Ripeti l'operazione per aggiungere altre chiavi (al massimo 10 chiavi).

 Note

È possibile collegare a ciascun vettore i metadati filtrabili come coppie chiave-valore quando si inseriscono dati vettoriali dopo aver creato l'indice vettoriale. Per impostazione predefinita, tutte le chiavi di metadati collegate ai vettori sono filtrabili e possono essere utilizzate come filtri in una query di somiglianza. Solo le chiavi di metadati specificate come non filtrabili durante la creazione dell'indice vettoriale non possono essere utilizzate come filtro. Per ulteriori informazioni sui limiti di dimensione dei metadati per vettore, inclusi i vincoli dei metadati filtrabili e totali, consulta [Limitazioni e restrizioni](#).

9. Per Crittografia, scegli Specificare il tipo di crittografia, quindi scegli una delle seguenti opzioni:
- Usa le impostazioni del bucket per la crittografia: Amazon S3 applica le impostazioni di crittografia del bucket vettoriale per crittografare i dati vettoriali nell'indice vettoriale.
 - Sostituisci le impostazioni del bucket per la crittografia: specifica un tipo di crittografia specifico per l'indice vettoriale:
 - Crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3): con SSE-S3, Amazon S3 gestisce automaticamente la generazione, la rotazione e la gestione delle chiavi di crittografia.

- Crittografia lato server con chiavi del servizio di gestione delle AWS chiavi (SSE-KMS): simile a SSE-S3, ma utilizza chiavi gestite dal cliente () in KMS, offrendoti un maggiore controllo sulle chiavi. CMKs AWS Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente](#) nella Guida per gli sviluppatori di Servizio AWS di gestione delle chiavi.

Se selezioni questa opzione, per Chiave AWS KMS scegli una delle seguenti opzioni:

- Scegli tra le tue chiavi KMS: seleziona una chiave AWS KMS esistente dall'elenco a discesa
- Inserisci l'ARN della chiave AWS KMS: inserisci l'Amazon Resource Name (ARN) di una chiave KMS
- Crea una chiave KMS: crea una nuova chiave gestita dal cliente nella console KMS. AWS Per ulteriori informazioni, consulta [Creazione di chiavi simmetriche gestite dal cliente](#) nella Guida per gli sviluppatori del Servizio AWS di gestione delle chiavi.

Note

Alla chiave KMS si applicano i seguenti requisiti:

- AWS L'ID della chiave KMS non deve essere vuoto.
- La tua chiave KMS deve trovarsi nella stessa regione in cui viene creato questo bucket.
- AWS L'ARN della chiave KMS deve iniziare con «arn:aws:kms:»

Important

- Le impostazioni di crittografia non possono essere modificate dopo la creazione dell'indice vettoriale.
- Se hai scelto Inserisci la chiave AWS KMS ARN, inserisci l'ARN nel campo di testo fornito.
- Se hai scelto Crea una chiave KMS, la console apre la console AWS KMS in una nuova scheda. Per istruzioni sulla creazione di una chiave KMS, consulta [Creazione di chiavi simmetriche gestite dal cliente](#) nella Guida per gli sviluppatori del Servizio AWS di gestione delle chiavi.

⚠ Important

Quando utilizzi la crittografia KMS, assicurati che i principali IAM che devono accedere agli oggetti nel bucket dispongano dell'autorizzazione KMS necessaria (kms:Decrypt) per la chiave KMS selezionata.

10. In Tag (facoltativo), puoi aggiungere tag come coppie chiave-valore per monitorare e organizzare i costi degli indici vettoriali utilizzando AWS Billing and Cost Management. Immettere una chiave e un valore. Per aggiungere un altro tag, scegliere Add Tag (Aggiungi tag). Puoi inserire fino a 50 tag per un indice vettoriale. Per ulteriori informazioni, consulta [Utilizzo di tag con bucket vettoriali S3](#).
11. Esamina attentamente la configurazione.

ℹ Note

Queste impostazioni non possono essere modificate dopo la creazione.

12. Scegli Crea indice di vettore.

Usando il AWS CLI

L'esempio seguente mostra come creare un bucket vettoriale con la configurazione di crittografia SSE-S3 utilizzando la AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors create-vector-bucket \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --encryption-configuration '{"sseType": "AES256"}'
```

Gli esempi seguenti mostrano come creare un bucket vettoriale che utilizza la configurazione di crittografia SSE-KMS con una chiave gestita dal cliente. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors create-vector-bucket \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --encryption-configuration '{"sseType": "aws:kms", "kmsKeyArn":
  "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"}'
```

L'esempio seguente mostra come creare un indice vettoriale con la configurazione di crittografia SSE-S3 utilizzando AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors create-index \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --index-name "amzn-s3-demo-vector-index" \  
  --encryption-configuration '{"sseType": "AES256"}'
```

Gli esempi seguenti mostrano come creare un indice vettoriale che utilizza la configurazione di crittografia SSE-KMS con una chiave gestita dal cliente. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors create-index \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --index-name "amzn-s3-demo-vector-index" \  
  --encryption-configuration '{"sseType": "aws:kms",  
  "kmsKeyArn": "arn:aws:kms:us-  
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890abc"}'
```

Gli esempi seguenti mostrano come verrà creato un indice vettoriale utilizzando le impostazioni di crittografia del bucket vettoriale. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors create-index \  
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \  
  --index-name "amzn-s3-demo-vector-index" \  
  --encryption-configuration '{"sseType": "aws:kms",  
  "kmsKeyArn": "arn:aws:kms:us-  
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890abc"}'
```

Visualizzazione della configurazione di crittografia in S3 Vectors

Dopo aver creato il bucket vettoriale, puoi verificare la configurazione della crittografia utilizzando la console. In alternativa, puoi utilizzare le operazioni GetVectorBucket e GetIndex API tramite l'API AWS REST, la AWS CLI o AWS gli SDK.

Utilizzo di AWS CLI

Utilizza il comando `get-vector-bucket` per recuperare informazioni dettagliate sul bucket, inclusa la configurazione della crittografia. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors get-vector-bucket \  
  --vector-bucket-name amzn-s3-demo-vector-bucket
```

Utilizzate il `get-index` comando per recuperare informazioni dettagliate sull'indice vettoriale, inclusa la configurazione della crittografia. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3vectors get-index \  
  --vector-bucket-name amzn-s3-demo-vector-bucket \  
  --index-name amzn-s3-demo-vector-index
```

Endpoint VPC per S3 Vectors

Per accedere a S3 Vectors dal tuo cloud privato virtuale (VPC), Amazon S3 supporta gli endpoint VPC di interfaccia utilizzando (). AWS PrivateLink PrivateLink PrivateLink fornisce una connettività privata tra VPC e S3 Vector senza richiedere un gateway Internet o un dispositivo NAT. Gli endpoint di interfaccia sono rappresentati da una o più interfacce di rete elastiche (ENI) a cui vengono assegnati indirizzi IP privati dalle sottoreti del VPC. Le richieste ai vettori S3 tramite gli endpoint di interfaccia rimangono sulla rete. AWS

Puoi anche accedere agli endpoint di interfaccia nel tuo VPC da applicazioni locali tramite AWS Direct Connect la nostra rete privata AWS virtuale (VPN).AWS Per ulteriori informazioni su come connettere il VPC alla rete locale, consulta la Guida per l'utente [e la Guida per l'AWS Direct Connect utente della VPN](#). [AWS Site-to-Site](#) Per informazioni generali sugli endpoint di interfaccia, consulta [Accedere a un AWS servizio utilizzando un endpoint](#) VPC di interfaccia nella Guida. AWS PrivateLink

Vantaggi dell'utilizzo con PrivateLink S3 Vectors

L'utilizzo PrivateLink con S3 Vectors offre diversi vantaggi operativi e di sicurezza:

- Sicurezza migliorata: il traffico tra il tuo VPC e i vettori S3 rimane all'interno della AWS rete e non attraversa Internet.
- Architettura di rete semplificata: accedi ai vettori S3 senza configurare gateway Internet, dispositivi NAT o connessioni VPN.
- Controllo granulare degli accessi: utilizza le policy degli endpoint VPC per controllare a quali bucket vettoriali e indici vettoriali è possibile accedere tramite l'endpoint.

- Supporto alla conformità: soddisfa i requisiti normativi che impongono la connettività di rete privata per i dati sensibili.

Nomi e risoluzione DNS degli endpoint VPC

Quando si crea un endpoint VPC, S3 Vectors genera due tipi di nomi DNS specifici degli endpoint: regionali e zonali.

I nomi DNS regionali e zonali degli endpoint VPC di interfaccia per S3 Vectors sono i seguenti:

- Nome DNS regionale: `vpce-1a2b3c4d-5e6f.s3vectors.region.vpce.amazonaws.com` - Il nome DNS dell'endpoint VPC regionale. Risolvi sempre con indirizzi IP privati.
- Nome DNS zonale:
`vpce-1a2b3c4d-5e6f-availability_zone_code.s3vectors.region.vpce.amazonaws.com`
- Nomi DNS per endpoint Zone-specific VPC. Risolvi sempre con indirizzi IP privati.

Puoi anche utilizzare il nome DNS dell'endpoint pubblico `s3vectors.region.api.aws` come nome DNS privato del servizio endpoint se hai abilitato il DNS privato per l'endpoint VPC.

Indirizzamento IP per gli endpoint di interfaccia

Gli endpoint DNS regionali, zonali e privati di S3 Vector supportano i tipi di IP IPv4, IPv6 e dualstack per. AWS PrivateLink Per ulteriori informazioni, consulta Tipi [di indirizzo](#) IP e tipo IP di record DNS per i servizi nella Guida. [AWS](#) AWS PrivateLink

Di seguito sono riportate alcune cose che dovresti sapere prima di provare ad accedere agli indici vettoriali e ai bucket vettoriali di S3 Vectors tramite IPv6 nel tuo VPC:

- Il client che usi per accedere ai vettori e il tuo client S3 Vectors devono entrambi avere il dual-stack abilitato.
- Se il tuo gruppo di sicurezza VPC non ha configurato IPv6, dovrai configurare una regola per consentire il traffico IPv6. Per ulteriori informazioni, consulta la [Fase 3: Aggiornamento delle regole del gruppo di sicurezza](#) nella Guida per l'utente di VPC e [Configurazione delle regole del gruppo di sicurezza nella Guida per l'utente di VPC](#).
- Se al VPC non sono assegnati CIDR IPv6, sarà necessario aggiungere manualmente un intervallo CIDR IPv6 al VPC. Per ulteriori informazioni, consulta [Aggiungere il supporto IPv6 per il tuo](#) VPC nella Guida. AWS PrivateLink

- Se utilizzi le policy IAM per il filtraggio degli indirizzi IP, queste devono essere aggiornate per gestire gli indirizzi IPv6. Per ulteriori informazioni sulla gestione delle autorizzazioni di accesso con IAM, consulta [Identity and Access Management in S3 Vectors](#).

Creazione di un endpoint di interfaccia VPC per S3 Vectors

È possibile creare un endpoint di interfaccia VPC per S3 Vectors utilizzando la console VPC, la CLI, gli SDK o l'API. AWS AWS AWS

Utilizzo della console S3

1. Apri <https://console.aws.amazon.com/vpc/> la console VPC all'indirizzo.
2. Nel pannello di navigazione, seleziona Endpoints (Endpoint).
3. Seleziona Crea endpoint.
4. Per Service category (Categoria servizio), scegli AWS services.
5. Per Servizi, cerca `s3vectors` e seleziona `com.amazonaws.region.s3vectors`.
6. Per VPC, seleziona il VPC in cui desideri creare l'endpoint.
7. (Facoltativo) In Impostazioni aggiuntive, per Abilita nome DNS, scegli se abilitare la funzionalità DNS privato. Se abilitata, le richieste che utilizzano l'endpoint del servizio pubblico (`s3vectors.region.api.aws`), ad esempio le richieste effettuate tramite AWS SDK, vengono risolte nell'endpoint VPC anziché nell'endpoint pubblico.
8. Per le sottoreti, seleziona le sottoreti in cui desideri creare le interfacce di rete degli endpoint.
9. Per il tipo di indirizzo IP, scegli il tipo di indirizzo IP per l'endpoint:
 - IPv4: assegna gli indirizzi IPv4 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4.
 - IPv6: assegna gli indirizzi IPv6 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate sono sottoreti solo IPv6.
 - Dualstack: assegna gli indirizzi IPv4 e IPv6 alle interfacce di rete degli endpoint. Questa opzione è supportata solo se tutte le sottoreti selezionate dispongono di intervalli di indirizzi IPv4 e IPv6.
10. Per Security groups (Gruppi di sicurezza), seleziona i gruppi di sicurezza da associare alle interfacce di rete dell'endpoint.
11. (Facoltativo) Per Policy, puoi allegare una policy sugli endpoint VPC per controllare l'accesso ai vettori S3 tramite l'endpoint. Per consentire tutte le operazioni da parte di tutti i principali su tutte

le risorse S3 Vectors tramite l'endpoint dell'interfaccia, scegli Accesso completo. Per limitare l'accesso, scegli Personalizzato e inserisci una policy. Per ulteriori informazioni, consulta [Controllare l'accesso agli endpoint VPC utilizzando le politiche degli endpoint](#) nella Guida. AWS PrivateLink Se non alleggi una policy, la policy predefinita consente l'accesso completo.

12. Seleziona Crea endpoint.

Utilizzo di AWS CLI

Per creare un nuovo endpoint VPC che restituisca sia IPv4 che IPv6 per i vettori S3, usa il seguente comando CLI di esempio. Per ulteriori informazioni, vedere [create-vpc-endpoint](#).

```
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-12345678 \
  --service-name com.amazonaws.region.s3vectors \
  --vpc-endpoint-type Interface \
  --subnet-ids subnet-12345678 subnet-87654321 \
  --security-group-ids sg-12345678 \
  --ip-address-type dualstack \
  --private-dns-enabled
```

Il `--private-dns-enabled` parametro abilita la funzionalità DNS privato. Se abilitata, le richieste `s3vectors.region.api.aws` verranno indirizzate attraverso l'endpoint VPC.

Per ulteriori informazioni sulla creazione di endpoint VPC, consulta [Create a VPC endpoint](#) nella VPC User Guide.

Policy sugli endpoint VPC per S3 Vectors

Analogamente alle policy basate sulle risorse, puoi allegare una policy sugli endpoint al tuo endpoint VPC per controllare l'accesso agli indici vettoriali e ai bucket vettoriali. Per ulteriori informazioni sulle politiche degli endpoint, consulta [Controllare l'accesso agli endpoint VPC utilizzando le politiche degli endpoint nella Guida](#). AWS PrivateLink

Esempi di politiche per gli endpoint VPC

Il seguente esempio di policy sugli endpoint VPC consente l'accesso a tutte le operazioni di S3 Vectors per tutti i principali:

```
{
  "Version": "2012-10-17",
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Principal": "*",  
    "Action": [  
      "s3vectors:*"  
    ],  
    "Resource": "*"   
  }  
]
```

Il seguente esempio di policy sugli endpoint VPC limita l'accesso a un bucket vettoriale specifico:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": [  
        "s3vectors:GetVectorBucket",  
        "s3vectors:ListIndexes",  
        "s3vectors:GetIndex",  
        "s3vectors:QueryVectors",  
        "s3vectors:GetVectors"  
      ],  
      "Resource": [  
        "arn:aws:s3vectors:us-west-2:111122223333:bucket/amzn-s3-demo-vector-bucket",  
        "arn:aws:s3vectors:us-west-2:111122223333:bucket/amzn-s3-demo-vector-bucket/*"  
      ]  
    }  
  ]  
}
```

Il seguente esempio di policy sugli endpoint VPC consente l'accesso solo durante l'orario lavorativo utilizzando la chiave di condizione: `aws:CurrentTime`

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",
```



```
"Principal": "*",
"Action": "s3vectors:*",
"Resource": "*",
"Condition": {
  "DateGreaterThan": {
    "aws:CurrentTime": "08:00Z"
  },
  "DateLessThan": {
    "aws:CurrentTime": "18:00Z"
  }
}
}
```

Configurazione dei client S3 Vectors per gli endpoint VPC

Quando si utilizzano endpoint VPC con S3 Vectors, è possibile configurare i client S3 Vectors in modo che utilizzino il nome DNS del servizio o il nome DNS dell'endpoint VPC.

Utilizzo di AWS SDK

SDK for Python

L'esempio seguente mostra come configurare il client S3 Vectors in SDK for Python (Boto3) per utilizzare un endpoint VPC:

```
import boto3

# Using service DNS name (requires private DNS feature enabled on VPC endpoint)
s3vectors_client = boto3.client(
    's3vectors',
    region_name='us-west-2',
    endpoint_url='https://s3vectors.us-west-2.api.aws'
)

# Using VPC endpoint DNS name
s3vectors_client = boto3.client(
    's3vectors',
    region_name='us-west-2',
    endpoint_url='https://vpce-12345678.s3vectors.us-west-2.vpce.amazonaws.com'
)
```

Risoluzione dei problemi relativi agli endpoint VPC

Se riscontri problemi con il tuo endpoint VPC di interfaccia, considera i seguenti passaggi per la risoluzione dei problemi:

- **Risoluzione DNS:** verifica che le query DNS per l'endpoint si risolvano in indirizzi IP privati compresi nell'intervallo CIDR del tuo VPC quando utilizzi un DNS privato.
- **Gruppi di sicurezza:** assicurati che il gruppo di sicurezza associato all'endpoint VPC consenta il traffico HTTPS in entrata (porta 443) dalle tue risorse VPC.
- **Tabelle di routing:** verifica che le tabelle di routing della tua sottorete non abbiano route in conflitto che potrebbero reindirizzare il traffico lontano dall'endpoint VPC.
- **Politica sugli endpoint VPC:** verifica che la tua policy sugli endpoint VPC consenta le azioni e le risorse S3 Vectors necessarie.
- **Configurazione del client:** se la funzionalità DNS privato è disabilitata, configura il tuo client S3 Vectors in modo che utilizzi il nome DNS dell'endpoint VPC anziché il nome DNS del servizio.

Monitoraggio dell'utilizzo degli endpoint VPC

Puoi monitorare l'utilizzo degli endpoint VPC di S3 Vectors tramite i registri degli eventi. CloudTrail [NetworkActivity](#)

Per ulteriori informazioni sulla registrazione di S3 Vectors, vedere. [Registrazione con AWS CloudTrail per i vettori S3](#)

Registrazione con AWS CloudTrail per i vettori S3

Amazon S3 Vectors è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un servizio. AWS CloudTrail acquisisce tutte le chiamate API per S3 Vectors come eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata fatta a S3 Vectors, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e dettagli aggiuntivi. Quando si verifica un'attività di evento supportata in S3 Vectors, tale attività viene registrata in un evento. CloudTrail Puoi utilizzare CloudTrail trail per registrare gli eventi di gestione e gli eventi relativi ai dati per S3 Vectors.

Per saperne di più CloudTrail, consulta la Guida per l'[CloudTrail utente](#).

Informazioni sui vettori S3 in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in S3 Vectors, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per S3 Vectors, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta [Panoramica sulla creazione di un percorso](#), sulla [configurazione delle notifiche di Amazon SNS](#), sulla [CloudTrail ricezione di file di registro da più regioni](#) e sulla [CloudTrail ricezione di file di registro da più account](#) nella Guida CloudTrail per CloudTrail utente.

[Tutte le azioni dell'API S3 Vectors vengono registrate CloudTrail e sono documentate nell'Amazon S3 Vectors API Reference](#). Ad esempio, le chiamate a [CreateVectorBucketCreateIndex](#), e le [QueryVectors](#) azioni generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'[elemento CloudTrail UserIdentity nella Guida](#) per l'CloudTrail utente.

CloudTrail eventi di gestione per S3 Vectors

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse dell'account. AWS Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Per S3 Vectors, CloudTrail registra i seguenti eventi di gestione:

- [CreateVectorBucket](#)
- [DeleteVectorBucket](#)
- [GetVectorBucket](#)
- [ListVectorBuckets](#)
- [PutVectorBucketPolicy](#)
- [GetVectorBucketPolicy](#)
- [DeleteVectorBucketPolicy](#)
- [CreateIndex](#)
- [DeleteIndex](#)
- [GetIndex](#)
- [ListIndexes](#)

Il valore di eventSource degli eventi di gestione e degli eventi di dati per S3 Vectors è `s3vectors.amazonaws.com`.

Per ulteriori informazioni sugli eventi di gestione, consulta [Registrazione degli eventi di gestione](#) nella Guida per l'utente. CloudTrail

CloudTrail eventi di dati per S3 Vectors

Gli eventi di dati forniscono informazioni sulle operazioni eseguite in una risorsa o al suo interno. Queste operazioni sono definite anche operazioni del piano dei dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati. Tuttavia, è possibile configurare i trail per registrare i log degli eventi di dati per le risorse S3 Vectors.

Quando si configura il trail per la registrazione dei log degli eventi di dati, è possibile specificare il tipo di risorsa S3 Vectors. S3 Vectors supporta i seguenti tipi di risorsa per gli eventi di dati:

- `AWS::S3Vectors::VectorBucket`: registra i log degli eventi di dati per tutti gli indici vettoriali presenti nei bucket vettoriali specificati
- `AWS::S3Vectors::Index`: registra i log degli eventi di dati per indici vettoriali specifici

Per S3 Vectors, CloudTrail registra i seguenti eventi relativi ai dati:

Operazioni su dati vettoriali:

- [PutVectors](#)- Registra quando i vettori vengono aggiunti a un indice vettoriale
- [GetVectors](#)- Registra quando i vettori vengono recuperati da un indice vettoriale
- [DeleteVectors](#)- Registra quando i vettori vengono eliminati da un indice vettoriale
- [ListVectors](#)- Registra quando vengono elencati i vettori in un indice vettoriale
- [QueryVectors](#)- Registra quando vengono eseguite interrogazioni di somiglianza su un indice vettoriale

eventSource per gli eventi di dati di S3 Vectors è `s3vectors.amazonaws.com`.

Abilitazione della registrazione di log degli eventi di dati per S3 Vectors

È possibile abilitare la registrazione degli eventi relativi ai dati per le risorse S3 Vectors quando si crea o si aggiorna un trail. CloudTrail È possibile specificare la registrazione di log per tutti i bucket vettoriali e tutti gli indici vettoriali dell'account oppure per singoli bucket vettoriali o indici vettoriali specificati. Per i passaggi dettagliati sulla creazione di un percorso, consulta [Creazione di un percorso nella Guida](#) per l'CloudTrail utente.

Per abilitare la registrazione di log degli eventi di dati per tutte le risorse S3 Vectors:

- Al momento della creazione o dell'aggiornamento di un trail, scegli Eventi di dati.
- Per Tipo di risorsa scegli `AWS::S3Vectors::VectorBucket`.
- Per Resource ARN, immettete per `arn:aws:s3vectors::_:_:bucket/*` registrare gli eventi per tutti i bucket vettoriali o specificate un bucket ARNs vettoriale individuale (ad esempio,).
`arn:aws:s3vectors:us-east-1:123456789012:bucket/amzn-s3-demo-vector-bucket`

Per abilitare la registrazione dei log degli eventi di dati per indici vettoriali specifici:

- Al momento della creazione o dell'aggiornamento di un trail, scegli Eventi di dati.
- Per Tipo di risorsa scegli `AWS::S3Vectors::Index`.
- Per ARN della risorsa, inserisci l'ARN dell'indice vettoriale specifico, ad esempio
`arn:aws:s3vectors:us-east-1:123456789012:bucket/amzn-s3-demo-vector-bucket/index/my-index`.

Per ulteriori informazioni sugli eventi relativi ai dati, consulta [Registrazione degli eventi relativi ai dati](#) nella Guida per l'utente. CloudTrail

Argomenti

- [CloudTrail esempio di file di registro per S3 Vectors](#)

CloudTrail esempio di file di registro per S3 Vectors

Gli esempi seguenti mostrano le voci di CloudTrail registro per gli eventi relativi ai dati di S3 Vectors. Gli eventi di dati vengono registrati quando si eseguono operazioni sui dati vettoriali all'interno degli indici vettoriali.

Esempio: file di CloudTrail registro per eventi relativi ai dati **GetVectors**

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/myUserName",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "myUserName"
  },
  "eventTime": "2024-11-22T17:12:25Z",
  "eventSource": "s3vectors.amazonaws.com",
  "eventName": "GetVectors",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "[aws-cli/2.18.5]",
  "requestParameters": {
    "vectorBucketName": "amzn-s3-demo-vector-bucket",
    "returnMetadata": "false",
    "indexName": "111aa1111-22bb-33cc-44dd-5555eee66ffff",
    "returnData": "false"
  },
  "responseElements": null,
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256"
  },
}
```

```

"requestID": "07D681123BD12AED",
"eventID": "f2b287f3-0df1-1234-a2f4-c4bdfed47657",
"readOnly": true,
"resources": [{
  "accountId": "123456789012",
  "type": "AWS::S3Vectors::VectorBucket",
  "ARN": "arn:aws:s3vectors:us-east-1:123456789012:bucket/amzn-s3-demo-vector-bucket"
}, {
  "accountId": "123456789012",
  "type": "AWS::S3Vectors::Index",
  "ARN": "arn:aws:s3vectors:us-east-1:123456789012:bucket/amzn-s3-demo-vector-bucket/index/111aa1111-22bb-33cc-44dd-5555eee66ffff"
}],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "444455556666",
"eventCategory": "Data",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "client-host"
}
}

```

Interpretazione delle voci dei file di log di S3 Vectors

CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Le voci di CloudTrail registro di S3 Vectors contengono i seguenti elementi chiave:

- `eventSource`: sempre `s3vectors.amazonaws.com` per gli eventi di S3 Vectors.
- `eventName`: l'operazione API di S3 Vectors che è stata eseguita.
- `eventCategory`: Management per le operazioni del piano di controllo (control-plane) o Data per le operazioni del piano dati.
- `ReadOnly`: `true` per operazioni di lettura (ad esempio, [GetVectorsQueryVectors](#), [ListVectors](#)) e `false` per operazioni di scrittura ([PutVectors](#), [DeleteVectors](#)).

- **resources**: risorse di S3 Vectors interessate dall'operazione, inclusi bucket e indici vettoriali.
- **requestParameters**: parametri inviati insieme alla richiesta.
- **responseElements**: elementi di risposta restituiti dal servizio S3 Vectors.

Lavorare con i file Amazon S3

Argomenti

- [Che cos'è S3 Files?](#)
- [Come funziona S3 Files?](#)
- [Sei il primo utente di S3 Files?](#)
- [Concetti chiave](#)
- [Funzionalità](#)
- [Come viene fatturato il costo di S3 Files?](#)
- [Prerequisiti per i file S3](#)
- [Tutorial: Guida introduttiva a S3 Files](#)
- [Montaggio dei bucket S3 su risorse di elaborazione](#)
- [Creazione e gestione delle risorse S3 Files](#)
- [Comprendere come funziona la sincronizzazione](#)
- [Monitoraggio e controllo dei file S3](#)
- [Specifiche prestazionali](#)
- [Sicurezza per i file S3](#)
- [Come vengono misurati i file S3](#)
- [Le migliori pratiche per i file S3](#)
- [Funzionalità, limiti e quote non supportati](#)
- [Risoluzione dei problemi relativi ai file S3](#)

Che cos'è S3 Files?

S3 Files è un file system condiviso che collega qualsiasi risorsa di AWS elaborazione direttamente con i tuoi dati in Amazon S3. Fornisce un accesso rapido e diretto a tutti i dati S3 sotto forma di file con semantica completa del file system e prestazioni a bassa latenza, senza che i dati escano mai da S3. Ogni applicazione, agente e team basato su file può accedere e utilizzare i dati S3 come file system utilizzando gli strumenti da cui già dipende. Costruito utilizzando Amazon EFS, S3 Files offre le prestazioni e la semplicità di un file system con la scalabilità, la durabilità e l'economicità di S3.

Puoi leggere, scrivere e organizzare i dati utilizzando operazioni su file e directory, mentre S3 Files gestisce la sincronizzazione delle modifiche tra il bucket e il file system.

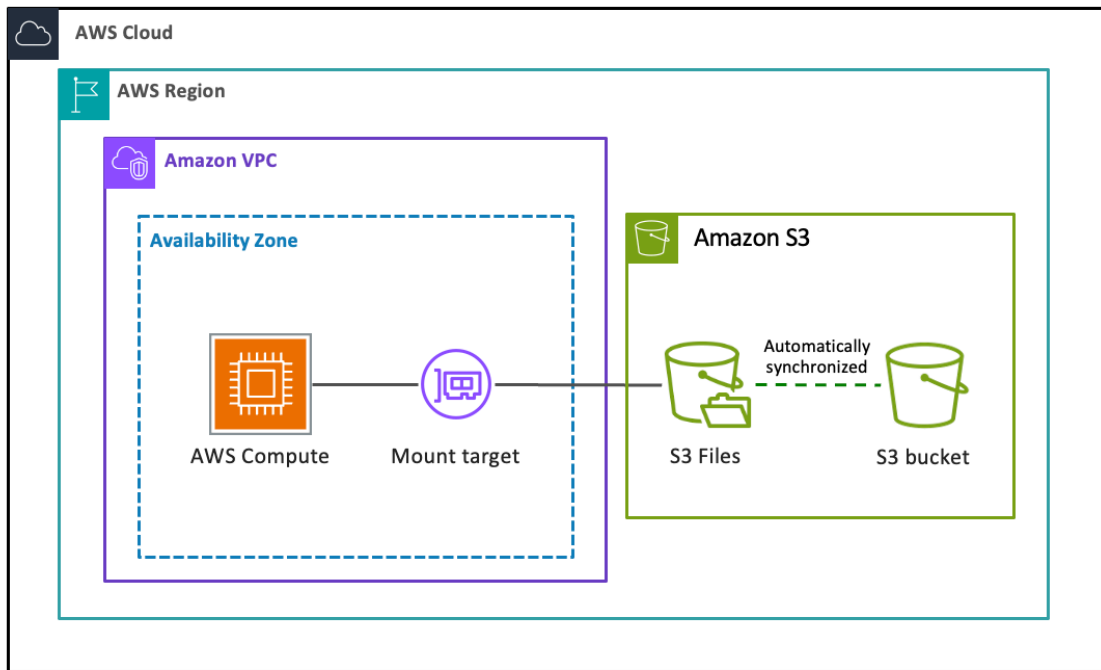
Come funziona S3 Files?

Quando crei un file system S3 collegato al tuo bucket S3 o a un prefisso al suo interno e lo monti su una risorsa di calcolo come un'istanza EC2 o una funzione Lambda, S3 Files presenta innanzitutto una vista attraversabile degli oggetti del bucket come file. Mentre navighi tra le directory e apri i file, i metadati e i contenuti associati vengono inseriti nello storage ad alte prestazioni del file system. Quando leggi i file, S3 Files carica il contenuto dei file sullo storage ad alte prestazioni su richiesta senza duplicare l'intero set di dati. Quando scrivi dati, le tue scritture vengono trasferite nello storage ad alte prestazioni e vengono nuovamente sincronizzate nel tuo bucket S3. S3 Files traduce in modo intelligente le operazioni del file system in richieste S3 efficienti per tuo conto. Molte operazioni di lettura aggirano completamente il file system e i dati vengono forniti direttamente da S3.

È possibile configurare la soglia di dimensione del file per ciò che viene caricato sullo storage ad alte prestazioni (impostazione predefinita <128 KiB), poiché le latenze sono più importanti per i file di piccole dimensioni. S3 Files trasmette le letture dei file direttamente dal bucket S3 in due casi: quando i dati del file non sono archiviati nella memoria ad alte prestazioni del file system e per letture di grandi dimensioni ≥ 1 MiB, anche quando i dati risiedono anche nello storage ad alte prestazioni del file system. Il bucket S3 è ottimizzato per un throughput elevato, mentre il livello di storage ad alte prestazioni del file system è ottimizzato per l'accesso a bassa latenza. S3 Files importa in modo asincrono i dati per file di piccole dimensioni (< 128 KiB per impostazione predefinita) nello storage ad alte prestazioni del file system per l'accesso a bassa latenza nelle letture successive. I dati modificati di recente che non sono ancora stati sincronizzati con S3 vengono sempre forniti dal file system. Per ulteriori informazioni, consulta [Personalizzazione della sincronizzazione per i file S3](#).

I dati che non sono stati letti all'interno di una finestra configurabile (da 1 a 365 giorni, impostazione predefinita 30) scadono automaticamente dallo storage ad alte prestazioni. I tuoi dati autorevoli rimangono sempre in S3 e la sincronizzazione in background mantiene il file system e il bucket coerenti in entrambe le direzioni. Per ulteriori informazioni, consulta [Comprendere come funziona la sincronizzazione](#).

I servizi di elaborazione supportati per montare i file system S3 sono Amazon EC2 AWS Lambda, Amazon EKS e Amazon ECS. Per ulteriori informazioni, consulta [Montaggio dei bucket S3 su risorse di elaborazione](#).



Sei il primo utente di S3 Files?

Se sei un utente alle prime armi di S3 Files, crea il tuo primo file system S3 utilizzando la console S3 o la CLI AWS seguendo il [Tutorial: Guida introduttiva a S3 Files](#)

Concetti chiave

I seguenti termini vengono utilizzati nella documentazione di S3 Files:

File system

Un file system condiviso collegato al tuo bucket S3.

High-performance archiviazione

Il livello di storage a bassa latenza all'interno del file system in cui risiedono i dati e i metadati dei file utilizzati attivamente. S3 Files gestisce automaticamente questo spazio di archiviazione, copiando i dati su di esso quando accedi ai file e rimuovendo i dati che non sono stati letti entro una finestra di scadenza configurabile. Paghi una tariffa di archiviazione per i dati che risiedono nello storage ad alte prestazioni.

Sincronizzazione

Il processo mediante il quale S3 Files mantiene il set di dati di lavoro attivo e le modifiche coerenti tra il file system e il bucket S3. Importazione di copie dei dati dal bucket S3 sul file system.

Esportazione delle copie delle modifiche apportate tramite il file system nel bucket S3. S3 Files esegue la sincronizzazione automaticamente in entrambe le direzioni.

Monta il bersaglio

Una destinazione di montaggio fornisce l'accesso di rete al file system all'interno di una singola zona di disponibilità nel VPC. È necessaria almeno una destinazione di montaggio per accedere al file system dalle risorse di elaborazione ed è possibile creare al massimo una destinazione di montaggio per zona di disponibilità.

Access point

I punti di accesso sono punti di accesso specifici dell'applicazione a un file system che semplificano la gestione dell'accesso ai dati su larga scala per set di dati condivisi. È possibile utilizzare i punti di accesso per applicare le identità e le autorizzazioni degli utenti per tutte le richieste di file system effettuate tramite il punto di accesso. Quando si crea un file system utilizzando la console di AWS gestione, S3 Files crea automaticamente un punto di accesso per il file system.

Funzionalità

Prestazioni elevate senza replica completa dei dati

S3 Files offre un accesso ai file a bassa latenza copiando solo il workset attivo sullo storage ad alte prestazioni del file system, non l'intero set di dati. I file di piccole dimensioni a cui si accede di frequente vengono serviti dallo storage ad alte prestazioni con latenze inferiori al millisecondo o a una singola cifra. Le letture di grandi dimensioni vengono trasmesse in streaming direttamente da S3 fino a terabyte al secondo di throughput aggregato. Ciò significa che ottieni le prestazioni del file system per i carichi di lavoro interattivi e il throughput S3 per i carichi di lavoro in streaming, senza pagare per archiviare o importare dati che non utilizzi o che non traggono vantaggio dalla bassa latenza. Per ulteriori informazioni, consulta [Specifiche prestazionali](#).

Routing di lettura intelligente

S3 Files indirizza automaticamente le richieste di lettura al livello di storage (file system S3 o bucket S3) più adatto a loro, mantenendo al contempo la semantica completa del file system, tra cui coerenza, blocco e autorizzazioni POSIX. Le letture casuali di piccole dimensioni dei file

utilizzati attivamente vengono eseguite dallo storage ad alte prestazioni per una bassa latenza. Le letture sequenziali di grandi dimensioni e le letture di dati non presenti nel file system vengono eseguite direttamente dal bucket S3 per un throughput elevato, senza costi per i dati del file system.

Sincronizzazione automatica

S3 Files mantiene automaticamente il file system e il bucket S3 coerenti in entrambe le direzioni. Le modifiche apportate tramite il file system vengono copiate nuovamente nel bucket S3 e le modifiche apportate direttamente al bucket S3 si riflettono nella visualizzazione del file system. Puoi personalizzare il comportamento di sincronizzazione, compresi quali dati vengono importati e per quanto tempo rimangono nel file system. Per ulteriori informazioni, consulta [Comprendere come funziona la sincronizzazione](#).

Prestazioni scalabili

S3 Files ridimensiona automaticamente la velocità effettiva e gli IOPS in base all'attività del carico di lavoro. Non è necessario fornire o gestire la capacità prestazionale e si paga solo per ciò che si utilizza.

Durabilità a livello regionale

I dati scritti nel livello di storage ad alte prestazioni hanno la stessa durabilità di Amazon S3. Archivia i dati in modo ridondante in più zone di disponibilità geograficamente separate all'interno della stessa AWS regione, garantendo durabilità e disponibilità elevate per i dati.

Encryption (Crittografia)

S3 Files crittografa tutti i dati in transito utilizzando TLS e tutti i dati inattivi utilizzando le chiavi KMS. AWS È possibile utilizzare chiavi AWS di proprietà (impostazione predefinita) o chiavi gestite dal cliente. Per ulteriori informazioni, consulta [Encryption \(Crittografia\)](#).

Semantica del file system

S3 Files supporta i protocolli NFS versione 4.2 e 4.1. Fornisce semantica di accesso al file system, come la coerenza dei dati di lettura dopo la scrittura, il blocco dei file e le autorizzazioni POSIX.

Come viene fatturato il costo di S3 Files?

Paghi una tariffa di storage per la frazione di dati attivi che risiede nello storage ad alte prestazioni e paghi i costi di accesso al file system per la lettura e la scrittura sullo storage ad alte prestazioni

del file system. S3 Files trasmette le letture dei file direttamente dal bucket S3 in due casi: quando i dati del file non sono archiviati nella memoria ad alte prestazioni del file system e per letture di grandi dimensioni ≥ 1 MiB, anche quando i dati risiedono anche nello storage ad alte prestazioni del file system. Il bucket S3 è ottimizzato per un throughput elevato, mentre il livello di storage ad alte prestazioni del file system è ottimizzato per l'accesso a bassa latenza. S3 Files importa in modo asincrono i dati per file di piccole dimensioni (< 128 KiB per impostazione predefinita) nello storage ad alte prestazioni del file system per l'accesso a bassa latenza nelle letture successive. Queste letture comportano solo il costo della richiesta S3 GET standard senza costi di accesso al file system. I costi di accesso al file system si applicano alle operazioni di sincronizzazione: l'importazione dei dati nel file system comporta costi di scrittura, mentre l'esportazione delle modifiche in S3 comporta costi di lettura. Per ulteriori informazioni, consulta [Come vengono misurati i file S3](#). [Per i prezzi correnti, consulta la pagina dei prezzi di S3 Files](#).

Prerequisiti per i file S3

Prima di iniziare a utilizzare S3 Files, assicurati di aver completato i seguenti prerequisiti.

AWS configurazione dell'account e del computer

- Hai un AWS account.
- Hai una risorsa di elaborazione e un bucket S3 generico nella AWS regione desiderata in cui desideri creare il tuo file system. Per ulteriori informazioni, consulta [Creazione di un bucket per uso generico](#).
- Il controllo delle versioni del bucket S3 è abilitato. S3 Files richiede S3 Versioning per sincronizzare le modifiche tra il file system e il bucket S3. Per ulteriori informazioni, consulta [Abilitazione della funzione Controllo delle versioni sui bucket](#).
- Il bucket S3 deve utilizzare uno dei seguenti tipi di crittografia: Server-side crittografia con chiavi gestite Amazon S3 (SSE-S3) o Server-side crittografia con AWS chiavi KMS ().AWS SSE-KMS

Client S3 Files

Per utilizzare S3 Files con Amazon EC2, devi installare il client `amazon-efs-utils`, una raccolta condivisa e open source di strumenti per Amazon EFS e Amazon S3 Files. Per lavorare con S3 Files, è necessaria `amazon-efs-utils` la versione 3.0.0 o successiva. Il client include un programma di supporto al montaggio che semplifica il montaggio dei file system S3 e abilita le CloudWatch metriche di Amazon per monitorare lo stato di montaggio del file system.

Fase 1: Installare il client

- Accedi al terminale per la tua istanza Amazon EC2 tramite Secure Shell (SSH) e accedi con il nome utente appropriato. Per ulteriori informazioni, consulta [Connessione alla tua istanza EC2](#) nella Amazon Elastic Compute Cloud User Guide.
- Per chi utilizza Amazon Linux, procedi come segue per installare efs-utils dai repository di Amazon:

```
sudo yum -y install amazon-efs-utils
```

- Se usi altre distribuzioni Linux supportate, puoi fare quanto segue:

```
curl https://amazon-efs-utils.aws.com/efs-utils-installer.sh | sudo sh -s -- --install
```

- Per altre distribuzioni Linux, consulta [Su altre distribuzioni Linux](#) nel file README di amazon-efs-utils attivo. GitHub

Fase 2: Installa botocore

Il amazon-efs-utils client utilizza botocore per interagire con altri servizi. AWS Ad esempio, devi installare botocore per utilizzare Amazon per CloudWatch monitorare il tuo file system. Per istruzioni sull'installazione e l'aggiornamento di botocore, consulta Installazione di botocore nel file README di [amazon-efs-utils su](#). GitHub

Attivazione della modalità FIPS per i file S3

Se è necessario rispettare i Federal Information Processing Standards (FIPS), è necessario abilitare la modalità FIPS nel client. L'attivazione della modalità FIPS comporta la modifica del s3files-utils.conf file sul sistema operativo.

Segui questi passaggi per abilitare la modalità FIPS nel client per i file S3:

1. Utilizzando un editor di testo a scelta, aprire il file /etc/amazon/efs/s3files-utils.conf.
2. Trova la riga contenente il seguente testo:

```
fips_mode_enabled = false
```

3. Cambia il testo nel modo seguente:

```
fips_mode_enabled = true
```

4. Salvare le modifiche.

Ruoli IAM e policy

Per utilizzare i file S3, è necessario configurare i ruoli IAM e le politiche allegate per due scopi:

- Accesso al bucket dal file system
- Collegare il file system alle risorse di calcolo AWS

Ruolo IAM per accedere al bucket dal file system

Quando crei un file system S3 Files, specifichi un ruolo IAM che S3 Files presume sia in grado di leggere e scrivere nel bucket S3. Questo ruolo concede a S3 Files il permesso di sincronizzare le modifiche tra il file system e il bucket, incluse le regole di Amazon che attivano la sincronizzazione. EventBridge È inoltre necessario assicurarsi che la policy del bucket S3 non neghi l'accesso alle risorse di elaborazione.

S3 Files richiede il controllo delle versioni S3 sul bucket. Utilizza operazioni API specifiche della versione come e in aggiunta a. `s3:GetObjectVersion` `s3:GetObjectVersionTagging` `s3:GetObject` La seguente politica utilizza caratteri jolly (ad esempio, `s3:GetObject*` anziché `s3:GetObject`) per includere sia le azioni con versione che quelle senza versione.

Note

Quando si crea un file system utilizzando la console di AWS gestione, S3 Files crea automaticamente questo ruolo IAM con le autorizzazioni richieste.

Questo ruolo IAM richiede quanto segue:

- Una politica in linea come segue:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```



```

        "Sid": "S3BucketPermissions",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket",
            "s3:ListBucketVersions"
        ],
        "Resource": "arn:aws:s3:::bucket",
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "accountId"
            }
        }
    },
    {
        "Sid": "S3ObjectPermissions",
        "Effect": "Allow",
        "Action": [
            "s3:AbortMultipartUpload",
            "s3:DeleteObject*",
            "s3:GetObject*",
            "s3:List*",
            "s3:PutObject*"
        ],
        "Resource": "arn:aws:s3:::bucket/*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "accountId"
            }
        }
    },
    {
        "Sid": "UseKmsKeyWithS3Files",
        "Effect": "Allow",
        "Action": [
            "kms:GenerateDataKey",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncryptFrom",
            "kms:ReEncryptTo"
        ],
        "Condition": {
            "StringLike": {
                "kms:ViaService": "s3.region.amazonaws.com",
                "kms:EncryptionContext:aws:s3:arn": [

```

```

        "arn:aws:s3:::bucket",
        "arn:aws:s3:::bucket/*"
    ]
}
},
"Resource": "arn:aws:kms:region:accountId:*"
},
{
    "Sid": "EventBridgeManage",
    "Effect": "Allow",
    "Action": [
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Condition": {
        "StringEquals": {
            "events:ManagedBy": "elasticfilesystem.amazonaws.com"
        }
    },
    "Resource": [
        "arn:aws:events:*:*:rule/D0-NOT-DELETE-S3-Files*"
    ]
},
{
    "Sid": "EventBridgeRead",
    "Effect": "Allow",
    "Action": [
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule"
    ],
    "Resource": [
        "arn:aws:events:*:*:rule/*"
    ]
}
]
}

```

Sostituisci i valori segnaposto con i tuoi valori.

#	Placeholder	Description	Esempio
1	<i>bucket</i>	Il nome del tuo bucket S3	il mio secchio
2	<i>region</i>	La AWS regione del tuo secchio	us-east-1
3	<i>accountId</i>	L'ID del tuo AWS account	123456789012

- Una politica di fiducia che consente a S3 Files di assumere il ruolo IAM. Aggiungi la seguente politica di fiducia al ruolo IAM per consentire al servizio S3 Files di assumerlo. Sostituisci *accountId* e *region* con i tuoi valori.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3FilesAssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": "elasticfilesystem.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountId"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3files:region:accountId:file-system/*"
        }
      }
    }
  ]
}
```

Ruolo IAM per collegare il tuo file system a AWS risorse di calcolo

Le risorse di elaborazione su cui si monta un file system S3 devono avere un ruolo IAM associato (ad esempio, un profilo di istanza EC2) con policy che consentano alla risorsa di elaborazione

di interagire con il file system S3 e il bucket S3 di origine. È inoltre necessario assicurarsi che le politiche dei bucket del bucket di origine non neghino l'accesso alla risorsa di elaborazione.

Aggiungi le due politiche seguenti al ruolo IAM associato alla tua risorsa di elaborazione:

- Autorizzazioni per la risorsa di elaborazione per connettersi e interagire con i file system S3

Il ruolo IAM deve includere le autorizzazioni per consentire al mount helper di connettersi e interagire con i file system S3. È possibile allegare una policy AWS gestita, ad esempio `AmazonS3FilesClientFullAccess` managed policy, se si desidera concedere alla risorsa di calcolo l'accesso completo in lettura e scrittura al file system S3 o l'accesso in sola lettura. `AmazonS3FilesClientReadOnlyAccess` Puoi anche allegare la policy `AmazonElasticFileSystemsUtils` gestita se desideri abilitare il monitoraggio di Amazon CloudWatch. Per ulteriori informazioni e un elenco completo delle politiche gestite disponibili per i file S3, consulta le politiche [AWS gestite per Amazon S3 Files](#). Puoi fornire queste autorizzazioni anche aggiungendo autorizzazioni IAM individuali come `s3files:ClientMount` o `s3files:ClientWrite` (non obbligatorio per le connessioni di sola lettura) al ruolo IAM della tua risorsa di calcolo.

- Una policy in linea che concede alla risorsa di calcolo l'accesso in lettura agli oggetti S3

Aggiungi la seguente policy in linea al ruolo IAM. Questa policy concede alle risorse di calcolo le autorizzazioni per leggere direttamente gli oggetti dal bucket S3 collegato nello stesso account per ottimizzare le prestazioni di lettura. Sostituisci *bucket* con il nome del bucket S3 o il nome del bucket con prefisso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3ObjectReadAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::bucket/*"
    },
    {
      "Sid": "S3BucketListAccess",
      "Effect": "Allow",

```

```
{
  "Action": "s3:ListBucket",
  "Resource": "arn:aws:s3:::bucket"
}
```

Gruppi di sicurezza

Una volta creati il file system e le destinazioni di montaggio, è necessario configurare i gruppi di sicurezza corretti per iniziare a utilizzare il file system. I gruppi di sicurezza sia sulla risorsa di calcolo che sulla destinazione di montaggio devono consentire il traffico richiesto, come mostrato nella tabella seguente:

Gruppo di sicurezza	Tipo di regola	Protocollo	Porta	Source/destination
Istanza EC2	In uscita	TCP	2049	Gruppo di sicurezza Mount Target
Destinazione di montaggio	In entrata	TCP	2049	Gruppo di sicurezza dell'istanza EC2

Tutorial: Guida introduttiva a S3 Files

In questo tutorial, crei un file system S3 e lo monti su un'istanza EC2. Quindi testerai le operazioni di base sui file. Puoi usare la console S3 o la AWS CLI per iniziare con S3 Files.

Iniziare con S3 Files utilizzando il AWS Console

Il flusso di lavoro S3 Files sulla console S3 prevede i seguenti passaggi:

- Crea il tuo file system S3.
- Installa il file system sulla tua istanza EC2 ed esegui le operazioni del file system.

Prerequisiti

Prima di iniziare, assicurati di disporre di quanto segue:

- Hai completato il [AWS configurazione dell'account e del computer](#).
- Sei configurato con Amazon EC2 e hai dimestichezza con il lancio di istanze EC2. Per ulteriori informazioni, consulta [Nozioni di base su Amazon VPC](#) nella Guida per l'utente di Amazon EC2. Per questo tutorial, usa il VPC predefinito per la tua istanza EC2.
- Ne hai [Ruolo IAM per collegare il tuo file system a AWS risorse di calcolo](#) collegato uno alla tua istanza EC2 in modo che possa interagire con il tuo file system S3 e il tuo bucket S3.

Passaggio 1: crea il tuo file system S3

- Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
- Nella barra di navigazione, verifica di trovarti nella AWS regione in cui si trovano l'istanza EC2 e il bucket S3.
- Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
- Seleziona il bucket per il quale desideri creare un file system.
- Scegli la scheda File system.
- Scegliere Create file system (Crea file system).
- Controlla e conferma il tuo VPC. Per questo tutorial, usa il tuo VPC predefinito.
- Scegli Create (Crea).

Quando si crea un file system utilizzando la console di AWS gestione, S3 Files crea automaticamente una destinazione di montaggio in ogni zona di disponibilità nel VPC predefinito e un punto di accesso per il file system. Ciò può richiedere alcuni minuti. Il file system sarà disponibile per la fase successiva una volta create tutte le risorse.

Passaggio 2: installa il file system sulla tua istanza EC2

- Nella pagina Panoramica del file system, scegli Allega sotto Allega a un'istanza EC2. Si aprirà una nuova pagina per montare il file system su un'istanza EC2.
- Seleziona l'istanza EC2 desiderata dal menu a discesa Istanze EC2 disponibili.
- Inserisci un percorso sulla tua istanza EC2 in cui desideri montare il file system. Ad esempio, `/mnt/s3files/`.
- Assicurati di aver configurato l'indirizzo giusto [Gruppi di sicurezza](#) sulla tua istanza EC2 e il target di montaggio per consentire il flusso del traffico richiesto.

- Assicurati di avere il ruolo IAM giusto con le autorizzazioni richieste allegate alla tua istanza EC2 in modo che possa interagire con il tuo file system S3 e il tuo bucket S3. Per ulteriori informazioni, consulta [Ruolo IAM per collegare il tuo file system a AWS risorse di calcolo](#). Per questo tutorial, puoi considerare di concedere al client l'accesso completo aggiungendo la policy gestita al ruolo IAM dell'istanza AmazonS3FilesClientFullAccess EC2.
- Segui le istruzioni di allegamento visualizzate sulla pagina per aprire CloudShell, montare il file system ed eseguire le operazioni di base del file system.

Guida introduttiva a S3 Files utilizzando il AWS CLI

Il flusso di lavoro S3 Files su AWS CLI prevede i seguenti passaggi:

1. Creare il file system .
2. Crea obiettivi di montaggio per il tuo file system.
3. Installa il file system sulla tua istanza EC2 utilizzando un target di montaggio.
4. Verifica le operazioni sui file, come elencare una directory, scrivere testo su un file, leggere un file e copiare un file. Quindi verifica che le modifiche si riflettano nel tuo bucket S3.

Prerequisiti

Prima di iniziare, assicurati di avere quanto segue:

- Hai installato e configurato la AWS CLI. Per ulteriori informazioni, consulta [Installing or updating to the latest version of the AWS CLI](#).
- Sono stati completati tutti i prerequisiti descritti in [Prerequisiti per i file S3](#)
- Sei configurato con Amazon EC2 e hai dimestichezza con il lancio di istanze EC2. Hai bisogno di un AWS account, un utente con accesso amministrativo, una key pair e un gruppo di sicurezza. Per ulteriori informazioni, consulta [Nozioni di base su Amazon VPC](#) nella Guida per l'utente di Amazon EC2.

Passaggio 1: crea il tuo file system S3

[Connect alla tua istanza EC2](#). Esegui il create-file-system comando per creare un file system.

```
aws s3files create-file-system --region aws-region --bucket bucket-arn --role-arn iam-role
```

Sostituisci quanto segue con i valori desiderati:

- ***aws-region***: La AWS regione del tuo bucket. Ad esempio, `us-east-1`.
- ***bucket-arn***: L'ARN del tuo bucket S3.
- ***iam-role***: ARN del ruolo IAM che S3 Files assume per leggere e scrivere nel bucket S3. Assicurati di aver aggiunto le autorizzazioni corrette a questo ruolo IAM. Per ulteriori informazioni, consulta [Ruolo IAM per accedere al bucket dal file system](#).

Dopo aver creato correttamente il file system, S3 Files restituisce la descrizione del file system come JSON. Annota l'ID del file system per il passaggio successivo.

Fase 2: Creare obiettivi di montaggio

Una destinazione di montaggio fornisce l'accesso di rete al file system nel VPC all'interno di una singola zona di disponibilità. È necessario un target di montaggio per accedere al file system dalle risorse di calcolo. È possibile creare al massimo un target di montaggio per zona di disponibilità. Ti consigliamo di creare un target di montaggio in ogni zona di disponibilità in cui operi.

Esegui il `create-mount-target` comando seguente per creare una destinazione di montaggio per il tuo file system. Devi assicurarti che ***subnet-id*** si trovi nello stesso VPC dell'istanza EC2. È necessario creare il target di montaggio nella stessa zona di disponibilità dell'istanza EC2.

```
aws s3files create-mount-target --region aws-region --file-system-id file-system-id --  
subnet-id subnet-id
```

file-system-id Ecco l'ID del file system che hai ricevuto nella risposta al `create-file-system` comando. La creazione degli obiettivi di montaggio può richiedere fino a circa 5 minuti.

Passaggio 3: installa il file system sulla tua istanza EC2

Prima di montare il file system, assicurati di aver configurato la giusta [Gruppi di sicurezza](#) risorsa di elaborazione e il target di montaggio per consentire il flusso del traffico richiesto. Per maggiori dettagli sui gruppi di sicurezza, consulta la [guida utente VPC](#).

Esegui i seguenti comandi per montare il tuo file system:

- Crea una directory `/mnt/s3files` che utilizzerai come punto di montaggio del file system usando il seguente comando:


```
sudo mkdir /mnt/s3files
```

- Installa il file system:

```
sudo mount -t s3files file-system-id:/ /mnt/s3files
```

Se non disponi dell'ID del file system, puoi trovarlo eseguendo quanto segue:

```
aws s3files get-file-system --region aws-region --file-system-id file-system-id
```

Passaggio 4: Verifica le operazioni sui file

Verificate le operazioni di base sui file sul file system montato come segue:

- Passate alla directory che avete montato:

```
cd /mnt/s3files
```

- Puoi elencare il contenuto della tua directory per verificare che il contenuto del tuo bucket o prefisso sorgente sia stato importato. La sincronizzazione avviene in genere in pochi secondi, ma può richiedere più tempo, specialmente per il primo file. Se il bucket è vuoto, anche il comando seguente restituirà un risultato vuoto.

```
ls
```

- Puoi anche testare altre operazioni sui file:

- Crea un file:

```
echo "Hello, S3 Files!" > test.txt
```

- Leggi il file:

```
cat test.txt
```

- Crea una cartella:

```
mkdir test-directory
```

- Copia il file nella directory:

```
cp /mnt/s3files/test.txt /mnt/s3files/test-directory/
```

Puoi quindi andare al tuo bucket S3 e verificare che la directory `test-directory` rifletta nel tuo bucket. Tieni presente che potrebbe essere necessario circa 1 minuto per sincronizzare le modifiche nel bucket S3.

Montaggio dei bucket S3 su risorse di elaborazione

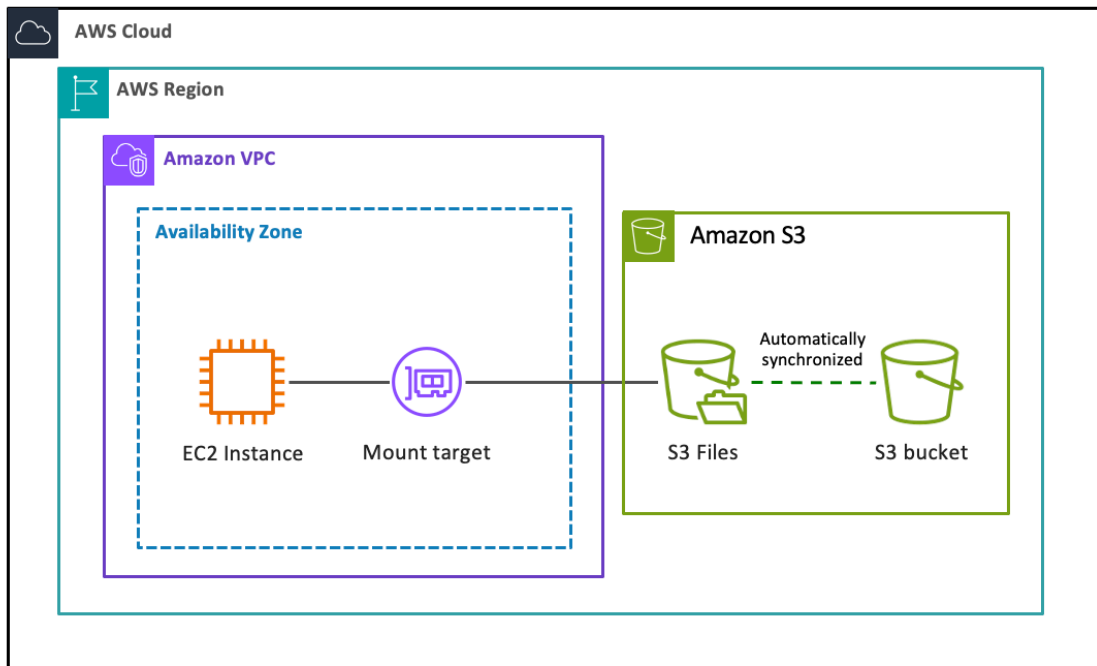
Puoi montare un file system S3 su risorse di calcolo per accedere ai tuoi dati S3 come file. La tua risorsa di elaborazione deve essere eseguita nello stesso Amazon Virtual Private Cloud (Amazon VPC) del file system S3. Tutte le risorse di elaborazione comunicano con il file system tramite target di montaggio sulla porta NFS 2049.

S3 Files supporta i seguenti ambienti di calcolo:

- [Istanze Amazon Elastic Compute Cloud \(Amazon EC2\)](#)
- [AWS Lambda funzioni](#)
- [Cluster Amazon Elastic Kubernetes Service \(Amazon EKS\)](#)
- [Cluster Amazon Elastic Container Service \(Amazon ECS\)](#)

Montaggio di file system S3 su Amazon EC2

Per montare i file system S3 su un'istanza EC2, è necessario utilizzare l'helper di montaggio dei file S3. L'helper di montaggio consente di montare i file system S3 su istanze EC2 che eseguono le distribuzioni supportate. Quando si monta un file system, il mount helper definisce un nuovo tipo di file system di rete, chiamato `s3files`, che è completamente compatibile con il comando standard di Linux. `mount`. Il mount helper supporta anche il montaggio automatico di un file system S3 all'avvio dell'istanza utilizzando le voci nel file di `/etc/fstab` configurazione sulle istanze EC2 Linux. Il mount helper fa parte della raccolta di strumenti open source che viene installata quando si installa il client S3 Files (`amazon-efs-utils`).



Prerequisiti per il montaggio su istanze EC2

- Hai un file system S3 con almeno una destinazione di montaggio disponibile.
- La tua istanza EC2 si trova nella stessa zona di disponibilità della destinazione di montaggio che utilizzerai per montare il tuo file system.
- Un profilo di istanza IAM è collegato all'istanza EC2 con le autorizzazioni richieste per i file S3. Per informazioni dettagliate, vedi [Ruolo IAM per collegare il tuo file system a AWS risorse di calcolo](#).
- Hai configurato i requisiti. [Gruppi di sicurezza](#)
- Hai installato il pacchetto amazon-efs-utils sull'istanza EC2. Per ulteriori informazioni, consulta [Client S3 Files](#).

Come funziona il mount helper?

Quando si emette un comando mount, il mount helper esegue le seguenti azioni:

- Recupera le credenziali IAM dal profilo dell'istanza EC2.
- Inizializza il processo efs-proxy per stabilire una connessione al target di montaggio. TLS-encrypted

- Avvia il processo di supervisione `amazon-efs-mount-watchdog`, che monitora lo stato dei mount TLS. Questo processo viene avviato automaticamente la prima volta che viene montato un file system S3.
- Monta il file system nel punto di montaggio specificato.

L'helper di montaggio utilizza TLS versione 1.2 per comunicare con il file system. L'utilizzo di TLS richiede dei certificati e questi certificati sono firmati da un'autorità di certificazione di Amazon. Per ulteriori informazioni sul funzionamento della crittografia, consultare [Sicurezza per i file S3](#).

L'helper di montaggio utilizza le seguenti opzioni di montaggio ottimizzate per i file S3:

Opzione	Valore	Description
<code>nfsvers</code>	4.2	Versione del protocollo NFS.
<code>rsize</code>	1048576	Imposta il numero massimo di byte di dati che il client NFS può ricevere per ogni richiesta READ di rete a 1048576 (1 MB), il numero massimo disponibile, per evitare una riduzione delle prestazioni.
<code>wsize</code>	1048576	Imposta il numero massimo di byte di dati che il client NFS può inviare per ogni richiesta WRITE di rete a 1048576 (1 MB), il numero massimo disponibile, per evitare una riduzione delle prestazioni.
<code>hard</code>	—	Imposta il comportamento di ripristino del client NFS dopo il timeout di una richiesta NFS, in modo che le richieste NFS vengano ritentate all'infinito fino alla risposta del server, per garantire l'integrità dei dati.
<code>timeo</code>	600	Imposta il valore di timeout utilizzato dal client NFS per attendere una risposta prima di riprovare una richiesta NFS a 600 decisecondi (60 secondi) per evitare una riduzione delle prestazioni.
<code>retrans</code>	2	Imposta il numero di volte in cui il client NFS ritenta una richiesta prima di tentare un'ulteriore azione di ripristino su 2.

Opzione	Valore	Description
<code>noresvport</code>	—	Indica al client NFS di utilizzare una nuova porta sorgente TCP non privilegiata quando viene ristabilita una connessione di rete. L'utilizzo <code>noresvport</code> aiuta a garantire la disponibilità ininterrotta del file system dopo una riconnessione o un evento di ripristino della rete.

Inoltre, il mount helper utilizza `tls` automaticamente le opzioni di montaggio durante il montaggio di un file system S3 poiché S3 Files richiede queste opzioni per stabilire una connessione. `iam` Questo perché S3 Files monta sempre un file system utilizzando la crittografia TLS e l'autenticazione IAM e queste non possono essere disabilitate.

Come montare il file system S3 su un'istanza EC2?

- Connettiti alla tua istanza EC2 tramite Secure Shell (SSH) o EC2 Instance Connect sulla console EC2. Per ulteriori informazioni, consulta [Connessione alla tua istanza EC2](#).
- Crea una directory `/mnt/s3files` che utilizzerai come punto di montaggio del file system usando il seguente comando:

```
sudo mkdir /mnt/s3files
```

- Monta il tuo file system S3:

```
FS="{YOUR_FILE_SYSTEM_ID}"
sudo mount -t s3files $FS:/ /mnt/s3files
```

- Verifica che il file system sia montato.

```
df -h /mnt/s3files
```

Noterai una risposta simile alla seguente:

```
Filesystem      Size  Used Avail Use% Mounted on
{s3files-dns}   8.0E  129M  8.0E   1% {path/to/mount}
```

È inoltre possibile verificare il montaggio del file system e controllare le opzioni di montaggio elencando il contenuto del punto di montaggio locale. Se il montaggio ha esito positivo, questo comando mostra i dettagli di montaggio, incluse le opzioni di montaggio, per la directory specifica.

```
findmnt -T /mnt/s3files
```

Per informazioni dettagliate sui comandi di montaggio, [GitHub consulta la documentazione](#).

È ora possibile leggere e scrivere oggetti S3 come file sul percorso di montaggio locale utilizzando le operazioni standard del file system. Se nel bucket S3 sono presenti oggetti, è possibile visualizzarli come file utilizzando i seguenti comandi.

```
ls /mnt/s3files
```

È possibile monitorare l'archiviazione del file system, le prestazioni, le connessioni client e gli errori di sincronizzazione utilizzando le metriche. [CloudWatch](#)

Come montare il file system S3 su un'istanza EC2 utilizzando i punti di accesso

Quando si monta un file system utilizzando un punto di accesso, il comando mount include l'opzione `access-point-id` mount.

```
sudo mount -t s3files -o accesspoint=access-point-id file-system-id /mnt/s3files
```

dove:

- *access-point-id* è l'ID del punto di accesso.
- *file-system-id* è l'ID del tuo file system S3.

Montaggio automatico dei file system S3 all'avvio dell'istanza EC2

È possibile configurare l'istanza EC2 per montare automaticamente un file system S3 all'avvio o al riavvio dell'istanza aggiornando il file. `/etc/fstab` Il `/etc/fstab` file contiene informazioni sui file system e viene utilizzato dal sistema operativo per determinare quali file system montare all'avvio.

⚠ Warning

In caso di montaggio automatico del file system, utilizzare l'opzione `_netdev`, usata per identificare i file system di rete. Se `_netdev` è mancante, l'istanza EC2 potrebbe smettere di rispondere. Questo risultato è dovuto al fatto che i file system di rete devono essere inizializzati dopo che l'istanza di calcolo ha avviato la sua interfaccia di rete. Per ulteriori informazioni, vedi Il montaggio [automatico non riesce e l'istanza non risponde](#).

Puoi utilizzare il mount helper per configurare un'istanza Amazon EC2 per montare automaticamente un file system S3 all'avvio dell'istanza:

- Aggiorna il `/etc/fstab` file EC2 con una voce per il file system S3.
- Allega un file system S3 quando crei una nuova istanza EC2 utilizzando la procedura guidata di avvio dell'istanza EC2.

Aggiornamento del file `/etc/fstab`

Esegui i passaggi seguenti per aggiornarlo `/etc/fstab` su un'istanza Linux EC2 in modo che l'istanza utilizzi il mount helper per rimontare automaticamente un file system S3 al riavvio dell'istanza.

- [Connettiti alla tua istanza EC2](#).
- Apri il `/etc/fstab` file in un editor e aggiungi la riga seguente al file:

```
file-system-id:/ mount-directory s3files _netdev 0 0
```

Dove:

- *file-system-id* è l'ID del tuo file system S3 (ad esempio, `fs-0123456789abcdef0`).
- *mount-directory* è la directory dei punti di montaggio sulla tua istanza EC2 (ad esempio, `/mnt/s3files`).
- `_netdev` specifica che il file system è un file system di rete, assicurando che l'istanza attenda la disponibilità della rete prima di tentare il montaggio.
- Salva il file e chiudi l'editor.
- Verificate la voce `fstab` montando tutti i file system in `fstab`:

```
sudo mount -a
```

- Verifica che il file system sia montato:

```
findmnt -T mount-directory
```

Utilizzando l'opzione nofail

Consigliamo di aggiungere l'`nofail` opzione alla voce `fstab` negli ambienti di produzione. Questa opzione consente all'istanza di avviarsi anche se il file system non riesce a montare:

```
file-system-id:/ mount-directory s3files _netdev,nofail 0 0
```

Montaggio automatico con un punto di accesso

Per eseguire il montaggio automatico utilizzando un punto di accesso S3 Files, includi l'`accesspoint` opzione:

```
file-system-id:/ mount-directory s3files _netdev,accesspoint=access-point-id 0 0
```

Montaggio automatico con una sottodirectory

Per montare automaticamente una sottodirectory specifica del file system, specificate il percorso:

```
file-system-id:/path/to/directory mount-directory s3files _netdev 0 0
```

Utilizzo della procedura guidata di avvio dell'istanza di EC2

- Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
- Scegliere Launch Instance (Avvia istanza).
- Segui questa documentazione per avviare un'istanza EC2 utilizzando la procedura guidata di avvio dell'istanza nella console. AWS Prima di scegliere Launch Instance, configura la rete e aggiungi il tuo file system S3 come mostrato nei passaggi seguenti.
- Assicurati di selezionare una sottorete nelle impostazioni di rete.
- Seleziona il gruppo di sicurezza predefinito per assicurarti che la tua istanza EC2 possa accedere al tuo file system S3. Non è possibile accedere all'istanza EC2 tramite Secure Shell (SSH) utilizzando questo gruppo di sicurezza. Per l'accesso tramite SSH, successivamente è possibile

modificare la sicurezza predefinita e aggiungere una regola per consentire SSH o un nuovo gruppo di sicurezza che consenta SSH. Puoi utilizzare le seguenti impostazioni:

- Tipo: SSH
- Protocollo: TCP
- Intervallo porte: 22
- Fonte: Anywhere 0.0.0. 0/0
- Nella sezione Archiviazione, scegli File system e scegli S3 Files.
- Nel menu a discesa del file system, vedrai i tuoi file system nella zona di disponibilità in base alla sottorete selezionata in precedenza nelle impostazioni di rete. Scegli il file system S3 che desideri montare. Se non disponi di alcun file system, scegli crea un nuovo file system per crearne uno nuovo.
- Inserisci un percorso di montaggio locale sull'istanza EC2 in cui desideri montare il file system (ad esempio, /mnt/s3files).
- Verrà generato un comando per montare il file system e aggiungerlo a fstab. Puoi scegliere di aggiungere il comando ai dati utente o di eseguirlo manualmente sulla tua istanza EC2 dopo il suo avvio. L'istanza EC2 verrà quindi configurata per montare il file system S3 all'avvio e ogni volta che viene riavviata.
- Scegliere Launch Instance (Avvia istanza).

Montaggio dei file system S3 da un altro VPC

Quando utilizzi una connessione peering VPC o un gateway di transito per connettere i VPC, le istanze Amazon EC2 presenti in un VPC possono accedere ai file system S3 in un altro VPC.

Un Transit Gateway è un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti locali. Per ulteriori informazioni sull'utilizzo di VPC Transit Gateway, consulta l'argomento relativo alle [nozioni di base su Transit Gateway](#) nella Guida di Amazon VPC Transit Gateway. Una connessione di peering VPC è una connessione di rete tra due VPC. Questo tipo di connessione consente di instradare il traffico tra di essi utilizzando indirizzi IPv4 (Internet Protocol version 4) o IPv6 (Internet Protocol version 6) privati. Puoi utilizzare il peering VPC per connettere i VPC all'interno della stessa regione o tra regioni. AWS Per ulteriori informazioni sul peering VPC, vedi [Cos'è il peering VPC?](#) nella Amazon VPC User Guide.

Quando si monta un file system da un VPC diverso, è necessario risolvere manualmente la destinazione di montaggio. È necessario utilizzare l'indirizzo IP delle destinazioni di montaggio nella

zona di disponibilità corrispondente come segue e sostituire *mount-target-ip-address**file-system-id*, e *mount-directory* con i propri valori.

```
sudo mount -t s3files -o mounttargetip=mount-target-ip-address file-system-id mount-directory
```

Per garantire un'elevata disponibilità del file system, si consiglia di utilizzare sempre un indirizzo IP di destinazione di montaggio che si trovi nella stessa zona di disponibilità del client NFS.

In alternativa, puoi utilizzare Amazon Route 53 come servizio DNS. In Route 53, puoi risolvere gli indirizzi IP di destinazione del montaggio da un altro VPC creando una zona ospitata privata e un set di record di risorse. Per ulteriori informazioni su come eseguire questa operazione, consulta [Lavorare con zone ospitate private](#) nella Amazon Route 53 Developer Guide.

Per maggiori dettagli sul montaggio da un altro VPC, visita il [GitHub ReadMe](#).

Montaggio di file system S3 da un altro AWS Region

Se stai montando il tuo file system S3 da un altro VPC che si trova in una AWS regione diversa da quella del file system, dovrai modificare il file. `s3files-utils.conf` in `/etc/amazon/efs/s3files-utils.conf` individua le righe seguenti:

```
#region = us-east-1
```

Rimuovi il commento dalla riga e sostituisci il valore dell'ID della regione in cui si trova il file system, se non è in `us-east-1`.

Quindi, è necessario specificare l'IP di destinazione del montaggio nel comando `mount` dopo aver modificato la regione nella configurazione:

```
sudo mount -t s3files -o mounttargetip=mount-target-ip-address file-system-id mount-directory
```

Smontaggio del file system S3

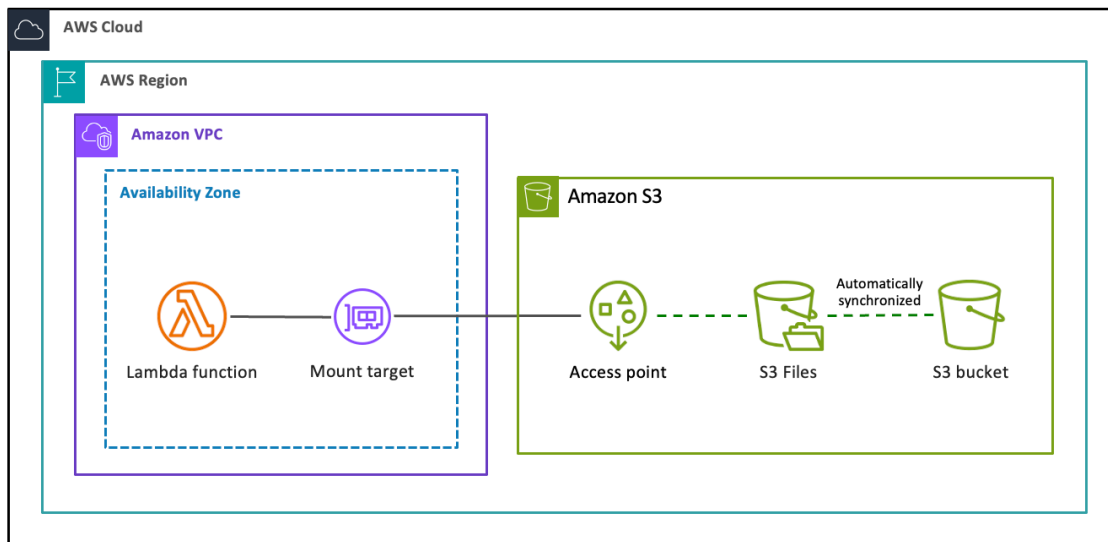
Per smontare un file system S3 connesso a un'istanza EC2 che esegue Linux, usa il comando come segue: `umount`

```
umount mount-directory
```

È consigliabile non specificare nessun'altra opzione di `umount`. Evitare di impostare qualsiasi altra opzione di `umount` differente da quelle di default. Puoi verificare che il tuo file system S3 sia stato smontato eseguendo il comando `findmnt`. Se lo smontaggio è andato a buon fine, il `findmnt` comando nella directory di montaggio non produrrà alcun output.

Montaggio di file system S3 su AWS Lambda funzioni

Sebbene AWS Lambda le funzioni forniscano uno storage locale temporaneo disponibile durante l'esecuzione, molti carichi di lavoro serverless, come l'inferenza dell'apprendimento automatico, l'elaborazione dei dati e la gestione dei contenuti, richiedono l'accesso a set di dati di riferimento di grandi dimensioni, file condivisi o archiviazione persistente. Collegando un file system S3 alla funzione Lambda, è possibile condividere facilmente i dati tra chiamate di funzioni, leggere file di dati di riferimento di grandi dimensioni e scrivere l'output delle funzioni in un archivio persistente e condiviso, il tutto tramite un percorso di montaggio locale.



Prerequisiti

Prima di montare un file system S3 su una funzione Lambda, assicurati di avere quanto segue:

- File system, destinazioni di montaggio e punto di accesso: devono essere disponibili il file system S3, almeno una destinazione di montaggio e un punto di accesso. Se si crea un file system utilizzando la console di AWS gestione, S3 Files crea automaticamente una destinazione di montaggio in ogni zona di disponibilità nel VPC predefinito e un punto di accesso UID/GID 1000/1000 (/Lambdae come ambito del punto di accesso) per il file system.

- Funzione Lambda: una funzione Lambda con un ruolo di esecuzione che ha accesso al montaggio del file system. Vedi [Ruolo di esecuzione e autorizzazioni utente nella Guida](#) per l'AWS Lambda utente.
- VPC: la funzione Lambda deve trovarsi nello stesso VPC del target di montaggio. Le sottoreti assegnate alla funzione Lambda devono trovarsi nella zona di disponibilità con una destinazione di montaggio.
- Hai configurato il necessario. [Gruppi di sicurezza](#)

Come montare il file system S3 su una funzione Lambda

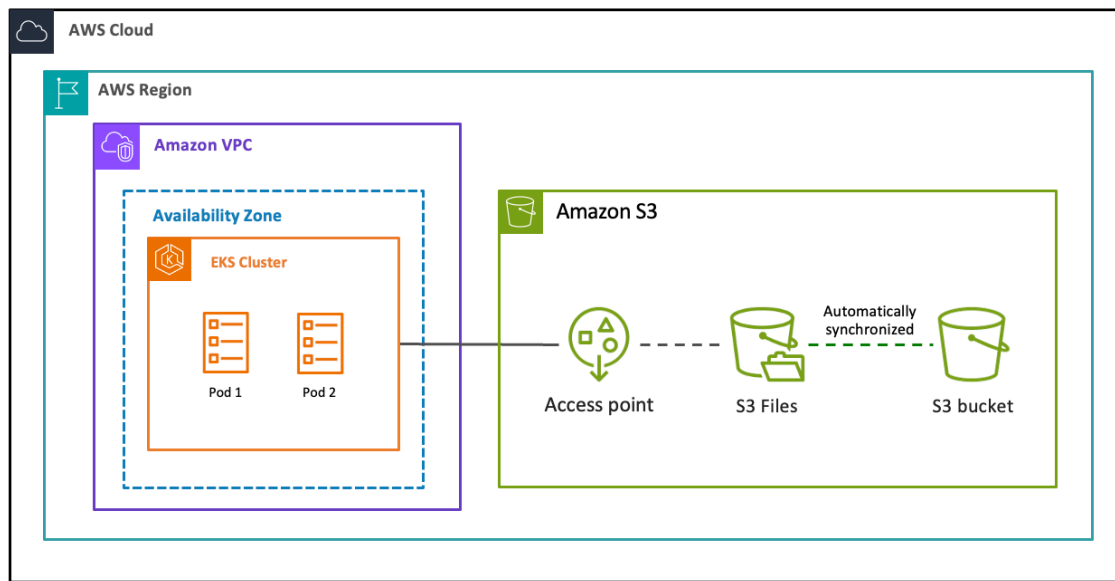
- Sulla console S3, scegli File system nel riquadro di navigazione a sinistra.
- Seleziona il file system che desideri montare sulla tua funzione Lambda.
- Nella scheda Panoramica, scegli Allega sotto Allega a una funzione Lambda.
- Seleziona una funzione Lambda disponibile dal menu a discesa. L'elenco disponibile mostra solo le funzioni all'interno dello stesso VPC e delle stesse sottoreti in cui è presente un target di montaggio.
- Specificate il percorso di montaggio locale.
- Se disponi di più punti di accesso, seleziona un punto di accesso.
- Scegli Collega. Il file system verrà ora collegato la prossima volta che richiamerai la funzione Lambda.

Per maggiori dettagli, consulta [Configurazione dell'accesso ai file Amazon S3](#) con AWS Lambda

Puoi monitorare lo storage del file system, le prestazioni, le connessioni client e gli errori di sincronizzazione utilizzando [Amazon CloudWatch](#).

Montaggio di file system S3 su Amazon EKS

Puoi collegare un file system S3 a un cluster Amazon EKS utilizzando il driver Amazon EFS Container Storage Interface (CSI). Il driver supporta il provisioning dinamico e statico. Per configurarlo, installa il driver efs-csi, che è il driver CSI per Amazon EFS e S3 Files.



Prerequisiti

Prima di montare un file system S3 su un cluster EKS, assicurati di avere quanto segue:

- Hai un file system S3 con almeno una destinazione di montaggio disponibile.
- È stato configurato il necessario. [Gruppi di sicurezza](#)
- Il cluster EKS deve trovarsi nello stesso VPC del target di montaggio.
- Il driver Amazon EFS CSI necessita delle autorizzazioni IAM (AWS Identity and Access Management) per connettersi e interagire con i file system S3. Per informazioni dettagliate, vedi [Ruolo IAM per collegare il tuo file system a AWS risorse di calcolo](#).
- AWS suggerisce di utilizzare EKS Pod Identities. Per ulteriori informazioni, vedere [Panoramica sulla configurazione di EKS Pod Identities](#).
- Per informazioni sui ruoli IAM per gli account di servizio e sulla configurazione di un provider IAM OpenID Connect (OIDC) per il cluster, consulta [Creare un provider IAM OIDC per il cluster](#).
- Lo strumento a riga di comando `kubectl` è installato sul dispositivo o AWS CloudShell. La versione deve essere inclusa in una versione secondaria della versione del Kubernetes cluster. Ad esempio, se la versione del cluster è 1.29, puoi utilizzare la `kubectl` versione 1.28, 1.29 o 1.30 con essa. Per installare o aggiornare `kubectl`, consulta [Configurare kubectl ed eksctl](#).

Come montare il file system S3 su un cluster EKS

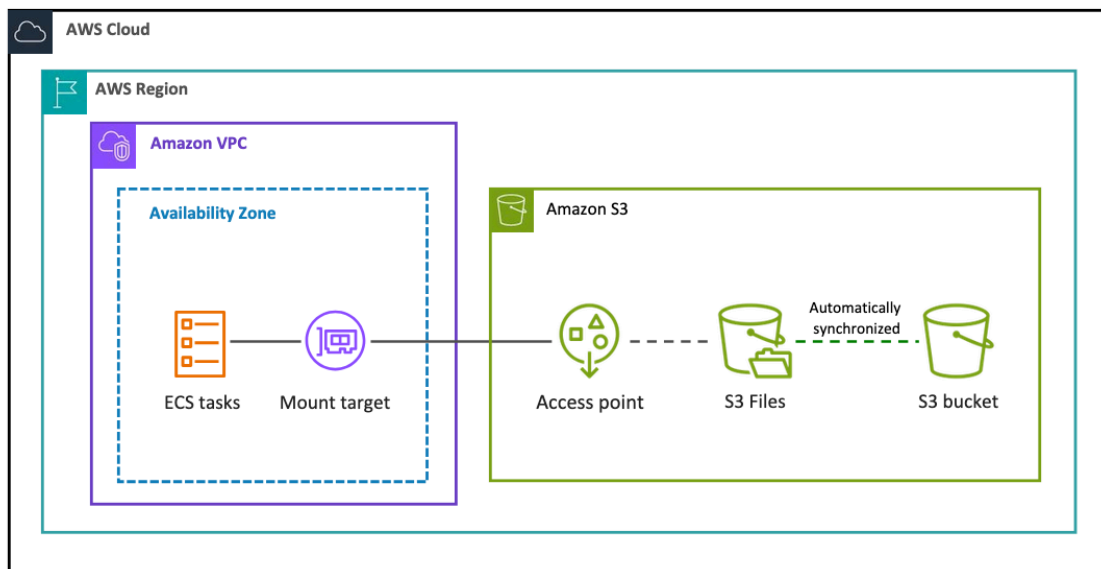
Il driver CSI per Amazon EFS richiede le autorizzazioni IAM per interagire con il file system. Crea un ruolo IAM e allega ad esso la policy `AmazonS3FilesCSIDriverPolicy` gestita. Quindi aggiungi il driver EFS CSI al tuo cluster EKS e specifica il ruolo IAM. È possibile utilizzare la console AWS di gestione o l' AWS API. Per informazioni dettagliate, consulta [Utilizzo dello storage di file system S3 con Amazon EKS](#).

Puoi anche utilizzare i file system S3 con AWS Batch su Amazon EKS. Per allegare un volume di file system S3 al tuo processo AWS Batch, utilizza i pod Amazon EKS con una dichiarazione di volume persistente. Per maggiori dettagli, consulta la VolumeClaim [sezione](#) persistente delle [pagine Register Job Definitions](#) ed EKS Persistent Volume Claim della AWS Batch API Reference Guide.

Puoi monitorare lo storage del file system, le prestazioni, le connessioni dei client e gli errori di sincronizzazione utilizzando [Amazon CloudWatch](#).

Montaggio di file system S3 su Amazon ECS

Puoi allegare un file system S3 a una definizione di attività Amazon ECS e quindi distribuire l'attività per accedere ai dati S3 dai tuoi contenitori.



In Amazon ECS, il supporto del volume S3 Files è disponibile per AWS Fargate ed ECS Managed Instances at General Availability. I volumi S3 Files non sono supportati nel tipo di avvio di Amazon EC2. Se configuri un volume S3 Files in una definizione di attività e tenti di eseguirlo sul tipo di avvio EC2, l'operazione avrà esito negativo.

Prerequisiti

Prima di collegare un file system S3 a un'attività ECS, assicurati di disporre di quanto segue:

- Hai un file system S3 con almeno una destinazione di montaggio nello stato disponibile.
- L'attività ECS deve trovarsi nello stesso VPC del target di montaggio.
- Aggiungi le autorizzazioni al ruolo IAM dell'attività ECS per accedere ai file system S3. Per informazioni dettagliate, vedi [Ruolo IAM per collegare il tuo file system a AWS risorse di calcolo](#).
- Hai configurato il necessario. [Gruppi di sicurezza](#)

Come montare il file system S3 su un'attività ECS

- Sulla console S3, scegli File system nel riquadro di navigazione a sinistra.
- Seleziona il file system che desideri montare.
- Nella scheda Panoramica, scegli Allega sotto Allega a un'attività ECS.
- Seleziona la definizione dell'attività ECS desiderata dal menu a discesa.
- Specificate il percorso di montaggio locale.
- Facoltativamente, è possibile specificare un punto di accesso, una directory principale e una porta di crittografia di transito.
- Una volta inserito il file system nella definizione dell'attività, è possibile avviare un'attività utilizzando questa definizione di attività nei seguenti modi:
 - È possibile distribuire l'attività come esecuzione autonoma, una tantum. Per i dettagli, consulta [Running an application as a Amazon ECS task](#) nella Amazon ECS Developer Guide.
 - Puoi anche distribuire la definizione dell'attività come servizio. Per i dettagli, consulta [Visualizza la cronologia dei servizi utilizzando le distribuzioni dei servizi Amazon ECS](#) nella Amazon ECS Developer Guide.

Per i dettagli, consulta [Utilizzo dello storage del file system S3 con Amazon ECS](#).

Puoi monitorare lo storage del file system, le prestazioni, le connessioni client e gli errori di sincronizzazione utilizzando [Amazon CloudWatch](#).

Tutorial: montare un file system S3 su più account

È possibile accedere a un file system S3 da risorse di calcolo in un AWS account diverso da quello del proprietario del file system. Questo è chiamato accesso tra account. Con l'accesso tra più account, i team con account diversi possono condividere lo stesso file system senza duplicare i dati.

Cross-account l'accesso richiede quanto segue:

- Accesso alla rete sulla porta 2049
- DNS che risolve la destinazione di montaggio del file system
- Autorizzazioni S3 Files che consentono l'accesso dall'account remoto

In questo tutorial, configuri l'accesso tra account da un'istanza Amazon EC2 utilizzando la Console di gestione. AWS L'account A possiede il file system S3 e l'account B possiede l'istanza EC2 che si connette ad esso.

Prerequisiti

Prima di iniziare, assicurati di disporre di:

- Un file system S3 con obiettivi di montaggio nell'account A. Per ulteriori informazioni, vedi [Guida introduttiva ai file S3](#).
- Un'istanza EC2 in esecuzione nell'account B con <https://github.com/aws/efs-utils> amazon-efs-utils v3.0.0 o successivo.
- Un ruolo [IAM per collegare il file system alle risorse di calcolo collegate all'istanza EC2. AWS](#)
- Una policy [del file system](#) che concede all'Account B le autorizzazioni per e. `s3files:ClientMount s3files:ClientWrite`
- Non-overlapping CIDR VPC nell'account A e nell'account B.
- Entrambi gli account soddisfano tutti i prerequisiti di S3 Files. Per ulteriori informazioni, consulta [Prerequisiti per S3 Files](#).

Valori di esempio utilizzati in questo tutorial

Questo tutorial utilizza i seguenti valori di esempio. Sostituisci questi valori con i tuoi valori.

Elemento	Valore
Account A (account S3 Files)	111111111111
Account B (account di istanza EC2)	222222222222
ID del file system S3	fs-0123456abcdef0189
Region	us-east-1
Nome DNS dei file S3	<code>{az_id}.fs-0123456abcdef0189.s3fil es.us-east-1.on.aws</code>
Ruolo dell'istanza EC2 (Account B)	ec2-instance-role

Fase 1: Registrazione dei dettagli di rete del file system

Nell'Account A, registra i seguenti dettagli di rete dal tuo file system.

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Scegli bucket generici, quindi scegli il bucket collegato al tuo file system S3.
3. Scegli la scheda File system, scegli il tuo file system, quindi scegli la scheda Mount targets.
4. Verifica che le destinazioni di montaggio esistano in ogni zona di disponibilità da cui intendi connetterti.
5. Registra i seguenti valori da utilizzare nelle fasi successive:
 - ID VPC del file system
 - ID AZ (ad esempio use1-az1, use1-az2)
 - Indirizzo IPv4 di ogni destinazione di montaggio (mappato su ciascun ID AZ)
 - ID del gruppo di sicurezza dei target di montaggio

Passaggio 2: creare una connessione peering VPC

Gli intervalli CIDR non devono sovrapporsi

Il peering VPC richiede che gli intervalli CIDR non si sovrappongano. Verificatelo prima di procedere.

1. In entrambi gli account, verifica che nel VPC siano abilitate le seguenti impostazioni DNS. Nella console VPC, scegli il tuo VPC, quindi scegli **Modifica impostazioni VPC**:
 - Risoluzione DNS (abilitata): abilitata DnsSupport
 - Nomi host DNS (abilitati): DnsHostnames abilitati
2. Nell'Account B, apri la console VPC, scegli **Peering Connections**, quindi scegli **Create peering connection**. Immetti uno dei seguenti valori:
 - ID VPC (Richiedente): VPC dell'istanza EC2 (Account B)
 - Account: un altro account, quindi inserisci 111111111111
 - Regione: us-east-1
 - ID VPC (Accettatore): VPC del file system S3 (Account A)
3. Nell'Account A, apri la console VPC, scegli **Peering Connections**, trova la richiesta in sospeso, quindi scegli **Azioni**, **Accetta richiesta**. Verifica che lo stato cambi in **Attivo**.

Fase 3: Aggiungere percorsi

Nell'account B (account di istanza EC2):

1. Apri la console VPC, scegli **Route Tables** e seleziona la tabella di route per la sottorete dell'istanza EC2.
2. Scegli **Modifica percorsi**, quindi scegli **Aggiungi percorso**:
 - Destinazione: CIDR del file S3 (VPC) nell'account A
 - Obiettivo: seleziona **Peering Connection**, quindi seleziona la connessione peering che hai creato nel passaggio 2

Nell'account A (account S3 Files):

1. Apri la console VPC, scegli **Route Tables** e seleziona la tabella di route per S3 Files VPC.

2. Scegli Modifica percorsi, quindi scegli Aggiungi percorso:

- Destinazione: CIDR del VPC dell'istanza EC2 nell'account B
- Obiettivo: seleziona Peering Connection, quindi seleziona la connessione peering creata nel passaggio 2

Fase 4: Configurare i gruppi di sicurezza

Il gruppo di sicurezza di mount target nell'Account A deve consentire il traffico NFS in entrata dall'istanza EC2 nell'Account B. Il gruppo di sicurezza dell'istanza EC2 nell'Account B deve consentire il traffico NFS in uscita verso il mount target.

1. Nella console VPC, scegli Security Groups, quindi seleziona il gruppo di sicurezza mount target che hai annotato nel passaggio 1.
2. Scegli Modifica regole in entrata e aggiungi la seguente regola:
 - Type (Tipo): NFS
 - Porta: 2049
 - Fonte: scegli Personalizzato, quindi inserisci l'ID del gruppo di sicurezza EC2 dall'account B
3. Verifica che il gruppo di sicurezza delle istanze EC2 nell'account B consenta il TCP in uscita sulla porta 2049.

Gruppo di sicurezza	Tipo di regola	Protocollo	Porta	Source/Destination
Istanza EC2 (Account B)	In uscita	TCP	2049	Gruppo di sicurezza Mount target (Account A)
Montare l'obiettivo (Account A)	In entrata	TCP	2049	Gruppo di sicurezza delle istanze EC2 (Account B)

Passaggio 5: aggiungere una politica del file system

Nell'Account A, aggiungi una policy del file system che conceda al ruolo dell'Account B l'autorizzazione al montaggio. S3 Files valuta questa politica ad ogni richiesta di montaggio. Il montaggio fallisce senza di esso, indipendentemente dalla configurazione della rete o del DNS.

1. Apri la console Amazon S3, scegli il tuo bucket, quindi seleziona la scheda **File system**.
2. Seleziona il tuo file system, quindi scegli **Modifica politica del file system**.
3. Aggiungi una policy che conceda al ruolo dell'Account B l'autorizzazione al montaggio. Il seguente esempio di policy `s3files:ClientWrite` assegna `s3files:ClientMount` e assegna il ruolo di istanza EC2 nell'Account B:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountMount",
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::222222222222:role/ec2-instance-
role" },
      "Action": [
        "s3files:ClientMount",
        "s3files:ClientWrite"
      ],
      "Resource": "arn:aws:s3files:us-east-1:111111111111:file-system/
fs-0123456abcdef0189"
    }
  ]
}
```

Fase 6: Creare le zone ospitate di Route 53

Nell'account B, crea zone private ospitate in modo che l'istanza EC2 possa risolvere i nomi DNS del file system. S3 Files utilizza i nomi DNS nel seguente formato per indirizzare le richieste di montaggio alla zona di disponibilità corretta:

```
{az_id}.{fs_id}.s3files.{region}.on.aws
```

Crea una zona ospitata privata per ogni ID AZ con una destinazione di montaggio. Per ogni ID AZ:

1. Apri la console Route 53, scegli **Zone ospitate**, quindi scegli **Crea zona ospitata**. Immetti uno dei seguenti valori:
 - Nome di dominio: `{az_id}.fs-0123456abcdef0189.s3files.us-east-1.on.aws`
 - Tipo: **zona ospitata privata**

- Regione: `us-east-1`
 - ID VPC: VPC dell'istanza EC2 nell'account B
2. Scegli Crea zona ospitata.
 3. Scegli Crea record e inserisci i seguenti valori:
 - Nome del record: (lasciare vuoto)
 - Tipo di record: A
 - Valore: indirizzo IPv4 del target di montaggio per quell>ID AZ (dal passaggio 1)
 4. Scegli Crea record.
 5. Ripeti l'operazione per tutti gli ID AZ da cui intendi connetterti.

Esempio:

Nome di dominio della zona ospitata	Un valore record
<code>use1-az1.fs-0123456abcdef0189.s3file s.us-east-1.on.aws</code>	Monta l'IP di destinazione per use1-az1
<code>use1-az2.fs-0123456abcdef0189.s3file s.us-east-1.on.aws</code>	Monta l'IP di destinazione per use1-az2
<code>use1-az4.fs-0123456abcdef0189.s3file s.us-east-1.on.aws</code>	Monta l'IP di destinazione per use1-az4

Fase 7: Configurare le autorizzazioni IAM

Associa un ruolo IAM all'istanza EC2 nell'account B. Il ruolo deve includere le seguenti autorizzazioni per montare e accedere al file system:

- La policy **AmazonS3FilesClientFullAccess** gestita (o equivalente): questa policy concede all'istanza EC2 il permesso di connettersi e interagire con i file system S3 Files.
- Una politica in linea che concede l'accesso agli oggetti S3 al bucket tra account: questa politica concede all'istanza EC2 l'autorizzazione a leggere gli oggetti direttamente dal bucket S3 nell'account A.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3ObjectReadAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::BUCKET_NAME_ACCOUNT_A/*"
    },
    {
      "Sid": "S3BucketListAccess",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::BUCKET_NAME_ACCOUNT_A"
    }
  ]
}
```

Sostituisci **BUCKET_NAME_ACCOUNT_A** con il nome del bucket S3 nell'account A.

Note

Per l'elenco completo delle politiche di base richieste per la tua risorsa di elaborazione, vedi il ruolo [IAM per collegare il tuo file system alle risorse di calcolo. AWS](#)

Fase 8: Montare il file system

[Connettiti alla tua istanza EC2](#) nell'account B ed esegui i seguenti comandi.

1. Crea un punto di montaggio:

```
sudo mkdir /mnt/s3files
```

2. Montare il file system:

```
sudo mount -t s3files fs-0123456abcdef0189 /mnt/s3files
```

3. Verifica il montaggio:

```
df -h /mnt/s3files  
ls /mnt/s3files
```

Risoluzione dei problemi

Utilizza le seguenti informazioni per risolvere i problemi più comuni durante il montaggio di un file system S3 su più account.

Il montaggio non riesce con un errore di risoluzione DNS

Verifica che entrambi i VPC siano abilitati `enableDnsSupport` e `enableDnsHostnames` abilitati. Verifica che le zone ospitate private di Route 53 siano associate al VPC corretto nell'account B e che i record A puntino agli indirizzi IP di destinazione di montaggio corretti.

Il montaggio si blocca o scade

Verifica che lo stato della connessione peering VPC sia Attivo. Verifica che le tabelle di routing in entrambi gli account contengano voci per il CIDR VPC peer che puntano alla connessione peering. Verifica che il gruppo di sicurezza mount target consenta il TCP in ingresso sulla porta 2049 dal gruppo di sicurezza dell'istanza EC2.

Autorizzazione negata per le operazioni sui file

Verifica che al ruolo IAM dell'istanza EC2 siano allegate sia la policy `AmazonS3FilesClientFullAccess` gestita che la policy di accesso agli oggetti S3 in linea. Verifica che la politica del file system nell'Account A conceda il ruolo `s3files:ClientMount` e `s3files:ClientWrite` nell'Account B.

Creazione e gestione delle risorse S3 Files

Questa pagina descrive come creare, configurare e gestire le risorse S3 Files. Per gestire le risorse utilizzando la AWS CLI, consulta il riferimento alle API di [S3 Files](#).

File system

Un file system condiviso collegato al bucket S3. Memorizza una parte dei dati S3 utilizzati attivamente come file e directory in modo che le applicazioni e gli utenti possano beneficiare di prestazioni a bassa latenza. È possibile accedere ai dati utilizzando le operazioni standard del file system, tra cui lettura, scrittura e blocco dei file.

- [Creazione dei file system](#)
- [Eliminazione dei file system](#)

Monta obiettivi

Un target di montaggio fornisce l'accesso di rete al file system all'interno di una singola zona di disponibilità del VPC. È necessario almeno un target di montaggio per accedere al file system dalle risorse di calcolo ed è possibile creare un massimo di un target di montaggio per zona di disponibilità. Ti consigliamo di creare un target di montaggio in ogni zona di disponibilità in cui operi in modo che le risorse di calcolo abbiano sempre un percorso di rete locale verso il file system, migliorando sia la disponibilità che la latenza. Quando si crea un file system utilizzando la Console di AWS gestione, S3 Files crea automaticamente una destinazione di montaggio in ogni zona di disponibilità del VPC predefinito.

- [Creazione di destinazioni di montaggio](#)
- [Gestione dei target di montaggio](#)
- [Eliminazione degli obiettivi di montaggio](#)

Policy dei file system

Una policy del file system è una policy opzionale sulle risorse IAM che puoi creare per il tuo file system S3 per controllare l'accesso dei client NFS al file system.

- [Creazione di policy del file system](#)
- [Eliminazione delle politiche del file system](#)

Punti di accesso

I punti di accesso sono punti di ingresso specifici dell'applicazione a un file system che semplificano la gestione dell'accesso ai dati su larga scala per i set di dati condivisi. È possibile utilizzare i punti di accesso per imporre le identità e le autorizzazioni degli utenti per tutte le richieste di file system effettuate tramite il punto di accesso. Inoltre, i punti di accesso possono limitare i client ad accedere solo ai dati all'interno di una directory principale specificata e delle relative sottodirectory. Quando si crea un file system utilizzando la AWS Management Console, S3 Files crea automaticamente un punto di accesso per il file system.

Un file system può avere un massimo di 25.000 punti di accesso. Per ulteriori informazioni, consulta [Funzionalità, limiti e quote non supportati](#).

- [Creazione di punti di accesso per un file system S3](#)
- [Eliminazione dei punti di accesso per un file system S3](#)

Tag

I tag sono coppie chiave-valore che definisci e associ alle tue risorse S3 Files per organizzarle, identificarle e gestirle.

- [Etichettare le risorse dei file S3](#)

CloudFormation modello

Puoi anche utilizzare CloudFormation i modelli per creare e gestire le risorse di S3 Files. Consulta [Amazon Simple Storage Service Files \(Amazon S3 Files\)](#) nella Guida per l'AWS CloudFormation utente per tutti i tipi di risorse S3 Files disponibili.

Argomenti

- [Creazione dei file system](#)
- [Eliminazione dei file system](#)
- [Creazione di destinazioni di montaggio](#)
- [Gestione dei target di montaggio](#)
- [Eliminazione degli obiettivi di montaggio](#)
- [Creazione di policy del file system](#)
- [Eliminazione delle politiche del file system](#)
- [Creazione di punti di accesso per un file system S3](#)
- [Eliminazione dei punti di accesso per un file system S3](#)
- [Etichettare le risorse dei file S3](#)

Creazione dei file system

Puoi creare file system utilizzando la AWS console, l'interfaccia a riga di AWS comando (AWS CLI) o l'API Amazon S3 per qualsiasi bucket S3 per uso generico esistente o nuovo. Per informazioni sulla creazione di un nuovo bucket, consulta. [Creazione di un bucket per uso generico](#)

Autorizzazioni IAM richieste per la creazione di file system

Quando crei un file system S3, devi specificare un ruolo IAM che S3 Files assume per leggere e scrivere nel tuo bucket S3. Questo ruolo consente a S3 Files di sincronizzare le modifiche tra il file system e il bucket S3. Quando crei un file system utilizzando la AWS console, S3 Files crea

automaticamente questo ruolo IAM con le autorizzazioni richieste. Se utilizzi la AWS CLI o l'API S3, consulta. [Ruolo IAM per accedere al bucket dal file system](#)

Per ulteriori informazioni sulla gestione delle autorizzazioni per le operazioni API, consulta [Come funziona S3 Files con IAM](#).

Stato di un file system

Un file system può avere uno dei valori di stato descritti nella tabella seguente che è possibile ottenere utilizzando il `get-file-system` comando.

Stato del file system	Description
DISPONIBILE	Il file system è integro, raggiungibile e disponibile per l'uso.
CREAZIONE IN CORSO	S3 Files sta creando il nuovo file system.
ELIMINAZIONE IN CORSO	S3 Files sta eliminando il file system in risposta a una richiesta di eliminazione avviata dall'utente.
ELIMINATO	S3 Files ha eliminato il file system in risposta a una richiesta di eliminazione avviata dall'utente.
ERRORE	Il file system si trova in uno stato di errore ed è irreversibile. Per accedere ai dati del file system, ripristina un backup del file system non riuscito su un nuovo file system. Controlla il StatusMessage campo per informazioni sull'errore.

Note

S3 Files restituisce un errore quando si tenta di creare un file system con un prefisso con un numero elevato di oggetti. Questo errore ti avvisa che operazioni ricorsive di ridenominazione o spostamento di grandi dimensioni possono influire sulle prestazioni del file system e aumentare i costi delle richieste S3, poiché ogni file richiede richieste di copia ed eliminazione separate nel bucket S3. Se desideri comunque creare un file system con ambito a quel prefisso, puoi aggiungere il parametro. `--AcceptBucketWarning`

Utilizzo della console S3

Questa sezione spiega come utilizzare la console Amazon S3 per creare un file system per S3 Files.

- Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
- Nella barra di navigazione, verifica di trovarti nella AWS regione desiderata.
- Nel pannello di navigazione a sinistra, scegli File system.
- Seleziona Crea file system.
- Nella pagina di creazione, scegli il bucket o il prefisso S3 da cui creare il file system. Puoi inserire direttamente l'URI S3 (ad esempio, `s3://bucket-name/prefix`) o scegliere Browse S3 per accedere e selezionare il bucket o il prefisso.
- Seleziona un VPC per il tuo file system. S3 Files seleziona automaticamente il tuo VPC predefinito. Questo è il VPC in cui le risorse di elaborazione si connettono al file system. Per utilizzare un VPC diverso, scegline uno dal menu a discesa.
- Seleziona Crea e attendi che diventi lo stato del tuo file system. `Available`

Impostazioni predefinite nella console AWS di gestione

S3 Files creerà il tuo file system con la seguente configurazione:

- Crittografia: S3 Files imposta la configurazione di crittografia dal bucket S3 di origine e la applica ai dati inattivi nel file system.
- Ruolo IAM: S3 Files crea un nuovo ruolo IAM che si assume per gestire la sincronizzazione dei dati tra il file system e il bucket.
- Monta destinazioni: S3 Files crea automaticamente una destinazione di montaggio in ogni zona di disponibilità nel VPC scelto.
- Punto di accesso: S3 Files crea un punto di accesso per il file system.

Utilizzo di AWS CLI

Quando utilizzi la AWS CLI, crei queste risorse in ordine. Prima di tutto si crea il file system. Quindi, è possibile creare destinazioni di montaggio ed eventuali tag opzionali aggiuntivi per il file system utilizzando i comandi AWS CLI corrispondenti.

Il comando di `create-file-system` esempio seguente mostra come utilizzare la AWS CLI per creare un file system per i file S3.

```
aws s3files create-file-system --region aws-region --bucket s3-bucket-arn --client-  
token idempotency-token --role-arn iam-role
```

Sostituisci quanto segue con i valori desiderati:

- *aws-region*: La AWS regione del tuo bucket. Ad esempio, `us-east-1`.
- *bucket-arn*: L'ARN del tuo bucket S3.
- *idempotency-token*: Un token di idempotenza. Questo è facoltativo.
- *iam-role*: ARN del ruolo IAM che S3 Files assume per leggere e scrivere nel bucket S3. Assicurati di aver aggiunto le autorizzazioni corrette a questo ruolo IAM. Per ulteriori informazioni, consulta [Ruolo IAM per accedere al bucket dal file system](#).

Dopo aver creato correttamente il file system, S3 Files restituisce la descrizione del file system come JSON.

Eliminazione dei file system

Quando si elimina un file system, il file system, i relativi dati e la relativa configurazione vengono rimossi in modo permanente. Assicurati che nessuna applicazione stia utilizzando attivamente il file system prima dell'eliminazione per evitare interruzioni del servizio. Prima dell'eliminazione, è necessario eliminare prima tutte le destinazioni di montaggio e i punti di accesso associati al file system. Per ulteriori informazioni, consultare [Eliminazione degli obiettivi di montaggio](#) e [Eliminazione dei punti di accesso per un file system S3](#).

Quando elimini un file system, S3 Files verifica se tutte le modifiche nel file system sono state sincronizzate con il bucket S3 collegato. Se ci sono modifiche che non sono ancora state sincronizzate, S3 Files restituisce un errore e l'eliminazione non procede. Ciò garantisce che tutti i dati vengano archiviati in modo sicuro nel bucket S3 prima dell'eliminazione del file system. Se desideri procedere con l'eliminazione e accettare che eventuali modifiche non sincronizzate vadano perse, puoi riprovare la richiesta di eliminazione con l'opzione «eliminazione forzata». Nella AWS CLI, aggiungi il `--ForceDelete` flag alla tua chiamata API di eliminazione. Sulla AWS console, scegli il pulsante Force nel messaggio di errore che appare quando elimini un file system mentre sono presenti modifiche non sincronizzate.

Utilizzo della console S3

Questa sezione spiega come utilizzare la console Amazon S3 per eliminare un file system per S3 Files.

- Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
- Nella barra di navigazione, verifica di trovarti nella AWS regione del file system che desideri eliminare.
- Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
- Scegliete un bucket generico a cui è collegato il file system.
- Seleziona la scheda File system e seleziona il file system che desideri eliminare.
- Scegli Elimina.
- Nella finestra di conferma, digitate `confirm`.

Utilizzo di AWS CLI

Il comando di `delete-file-system` esempio seguente mostra come utilizzare la AWS CLI per eliminare un file system per i file S3.

```
aws s3files delete-file-system --file-system-id file-system-id
```

Creazione di destinazioni di montaggio

È necessaria una destinazione di montaggio per accedere al file system dalle risorse di elaborazione ed è possibile creare al massimo una destinazione di montaggio per zona di disponibilità. Ti consigliamo di creare un target di montaggio per ogni zona di disponibilità in cui operi. Quando crei un file system utilizzando la console S3, S3 Files crea automaticamente una destinazione di montaggio in ogni zona di disponibilità nel tuo VPC predefinito.

È possibile creare destinazioni di montaggio per il file system in un VPC alla volta. Se desideri modificare il VPC per le tue destinazioni di montaggio, devi prima eliminare tutte le destinazioni di montaggio esistenti per il file system e quindi creare una destinazione di montaggio in un nuovo VPC. Se la VPC dispone di più sottoreti in una zona di disponibilità, è possibile creare un target di montaggio in una sola di tali sottoreti. Tutte le istanze EC2 nella zona di disponibilità possono condividere il singolo target di montaggio.

Utilizzo della console S3

Questa sezione spiega come utilizzare la console Amazon S3 per creare una destinazione di montaggio per i file S3.

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nella barra di navigazione, verifica di trovarti nella AWS regione del file system per cui desideri creare un target di montaggio.
3. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
4. Scegliete un bucket generico a cui è collegato il file system.
5. Seleziona la scheda File system e seleziona il file system desiderato.
6. Seleziona la scheda Mount targets e seleziona Crea target di montaggio.
7. Nella pagina Crea destinazione di montaggio, verrà selezionato automaticamente il tuo VPC predefinito. Scegli la zona di disponibilità e l'ID di sottorete. Il VPC, la zona di disponibilità e l'ID di sottorete non possono essere modificati dopo la creazione del target di montaggio.

Note

Il tipo di indirizzo IP deve corrispondere al tipo IP della sottorete. Inoltre, il tipo di indirizzo IP ha la precedenza sull'attributo di indirizzo IP della sottorete. Ad esempio, se il tipo di indirizzo IP è IPv4-only e l'attributo di indirizzamento IPv6 è abilitato per la sottorete, le interfacce di rete create nella sottorete ricevono un indirizzo IPv4 dall'intervallo della sottorete. Per ulteriori informazioni, consulta la sezione [Modifica dell'attributo di assegnazione degli indirizzi IP della sottorete](#).

8. Se conosci l'indirizzo IP in cui desideri posizionare la destinazione di montaggio, inseriscilo nella casella dell'indirizzo IP corrispondente al tipo di indirizzo IP. Se non specifichi un valore, S3 Files seleziona un indirizzo IP inutilizzato dalla sottorete specificata.
9. Scegliete i gruppi di sicurezza da associare alla destinazione di montaggio. [Gruppi di sicurezza](#) Consulta i prerequisiti per comprendere le configurazioni dei gruppi di sicurezza necessarie per iniziare a utilizzare il file system.
10. Scegli Crea destinazione di montaggio.

Utilizzo di AWS CLI

Il comando di `create-mount-target` esempio seguente mostra come utilizzare la AWS CLI per creare una destinazione di montaggio per i file S3.

```
aws s3files create-mount-target --region aws-region --file-system-id file-system-id --  
subnet-id subnet-id
```

La creazione dei target di montaggio può richiedere fino a ~5 minuti.

Gestione dei target di montaggio

È possibile aggiungere o rimuovere gruppi di sicurezza associati a un target di montaggio. I gruppi di sicurezza definiscono le possibilità di accesso in entrata e in uscita. Quando si modificano i gruppi di sicurezza associati a un target di montaggio, è necessario assicurarsi di autorizzare l'accesso in entrata e in uscita. In questo modo si consente alla risorsa di elaborazione di comunicare con il file system. [Gruppi di sicurezza](#) Consulta i prerequisiti per comprendere le configurazioni dei gruppi di sicurezza necessarie per iniziare a utilizzare il file system.

Utilizzo della console S3

Questa sezione spiega come utilizzare la console Amazon S3 per aggiungere o rimuovere gruppi di sicurezza per un target di montaggio in S3 Files.

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, verifica di trovarti nella AWS regione desiderata in cui esiste il tuo target di montaggio.
3. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
4. Scegliete un bucket generico a cui è collegato il file system.
5. Seleziona la scheda File system e seleziona il file system desiderato.
6. Seleziona la scheda Mount targets e seleziona il mount target che desideri modificare.
7. Scegli Modifica. Vedrai i dettagli del tuo target di montaggio.
8. Aggiungi o rimuovi gruppi di sicurezza dal menu a discesa dei gruppi di sicurezza.
9. Scegli Save (Salva).

Utilizzo di AWS CLI

Il seguente comando di `update-mount-target` esempio mostra come utilizzare la AWS CLI per aggiungere o rimuovere gruppi di sicurezza per una destinazione di montaggio in S3 Files.

```
aws s3files update-mount-target --region aws-region --mount-target-id mount-target-id
--security-groups security-group-ids-separated-by-space
```

Eliminazione degli obiettivi di montaggio

Quando si elimina un target di montaggio, vengono interrotti tutti i mount del file system. Ciò potrebbe interrompere le risorse di calcolo e le applicazioni che utilizzano tali montaggi. Per evitare interruzioni, arrestate le applicazioni e smontate il file system prima di eliminare la destinazione di montaggio.

È possibile eliminare le destinazioni di montaggio per un file system utilizzando la Console di AWS gestione, la AWS CLI o, a livello di programmazione, utilizzando gli SDK. AWS

Utilizzo della console S3

Usa la console Amazon S3 per eliminare un target di montaggio per i file S3.

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, verifica di trovarti nella AWS regione della destinazione di montaggio che desideri eliminare.
3. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
4. Scegli un bucket generico a cui è collegato il tuo file system.
5. Seleziona la scheda File system e seleziona il file system desiderato.
6. Seleziona la scheda Mount targets e seleziona il mount target che desideri eliminare.
7. Scegliere Elimina.
8. Nella finestra di conferma, digita **confirm** e scegli Elimina.

Utilizzo di AWS CLI

Il `delete-mount-target` comando seguente elimina una destinazione di montaggio per i file S3 utilizzando la AWS CLI.

```
aws s3files delete-mount-target --region aws-region --mount-target-id mount-target-id
```

Creazione di policy del file system

È possibile utilizzare le politiche del file system per concedere o negare le autorizzazioni ai client NFS per eseguire operazioni come il montaggio, la scrittura e l'accesso root sui file system. Un file

system ha una politica del file system vuota (predefinita) o esattamente una politica esplicita. È possibile aggiornare la politica del file system in qualsiasi momento dopo la creazione del file system utilizzando la console di AWS gestione, la AWS CLI o AWS I' SDK.

Puoi aggiornare una policy del file system utilizzando la console Amazon S3, la AWS CLI, a livello di codice con gli AWS SDK o direttamente l'API S3 Files. Queste modifiche alle policy possono richiedere diversi minuti prima che abbiano effetto. Le policy del file system S3 hanno un limite di 20.000 caratteri. Per ulteriori informazioni sull'utilizzo di una policy del file system S3, sulle azioni supportate, sulle chiavi di condizione supportate ed esempi, consulta. [Come funziona S3 Files con IAM](#)

Utilizzo della console S3

Questa sezione spiega come utilizzare la console Amazon S3 per creare una politica del file system per S3 Files.

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, verifica di trovarti nella AWS regione in cui esiste il tuo file system.
3. Nel pannello di navigazione a sinistra, scegli File system.
4. Scegli il file system desiderato.
5. Seleziona la scheda Autorizzazioni e seleziona Modifica.
6. È possibile utilizzare l'editor delle politiche per aggiungere la propria politica del file system.
7. Dopo aver completato la modifica della policy, scegli Salva.

Utilizzo di AWS CLI

Il comando di `put-file-system-policy` esempio seguente mostra come utilizzare la AWS CLI per creare una politica del file system per i file S3. La seguente policy del file system concede solo autorizzazioni `ClientMount` (di sola lettura) al ruolo IAM. `ReadOnly` Sostituisci l'ID dell' AWS account di esempio **111122223333** con l'ID del tuo account. AWS

```
aws s3files put-file-system-policy --file-system-id file-system-id --policy '{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::111122223333:role/ReadOnly"
    },
    "Action": [
        "s3files:ClientMount"
    ]
}
]
```

Eliminazione delle politiche del file system

Puoi eliminare una policy del file system utilizzando la console Amazon S3 e la CLI AWS .

Utilizzo della console S3

Questa sezione spiega come utilizzare la console Amazon S3 per eliminare una politica del file system per S3 Files.

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, verifica di trovarti nella AWS regione in cui esiste il tuo file system.
3. Nel pannello di navigazione a sinistra, scegli File system.
4. Scegli il tuo file system.
5. Seleziona la scheda Autorizzazioni e seleziona Elimina.
6. Nella finestra di conferma, digita **confirm** e scegli Elimina.

Utilizzo di AWS CLI

Il comando di `delete-file-system-policy` esempio seguente mostra come utilizzare la AWS CLI per eliminare una politica del file system per i file S3.

```
aws s3files delete-file-system-policy --file-system-id file-system-id
```

Creazione di punti di accesso per un file system S3

I punti di accesso sono punti di ingresso specifici dell'applicazione a un file system che semplificano la gestione dell'accesso ai dati su larga scala per i set di dati condivisi. È possibile utilizzare i punti

di accesso per imporre le identità e le autorizzazioni degli utenti per tutte le richieste di file system effettuate tramite il punto di accesso. Inoltre, i punti di accesso possono limitare i client ad accedere solo ai dati all'interno di una directory principale specificata e delle relative sottodirectory. Quando si crea un file system utilizzando la AWS Management Console, S3 Files crea automaticamente un punto di accesso per il file system.

Un file system può avere un massimo di 25.000 punti di accesso. Per ulteriori informazioni, consulta [Funzionalità, limiti e quote non supportati](#). Puoi creare punti di accesso utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando o l'SDK. AWS

I punti di accesso per un file system S3 non possono essere modificati dopo la creazione. Se si desidera effettuare aggiornamenti, è necessario eliminare il punto di accesso esistente e crearne uno nuovo.

Utilizzo della console S3

Questa sezione spiega come utilizzare la console Amazon S3 per creare un punto di accesso per un file system S3.

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, verifica di trovarti nella AWS regione del file system per il quale desideri creare un punto di accesso.
3. Nel pannello di navigazione a sinistra, scegli File system.
4. Scegli il file system desiderato.
5. Seleziona la scheda Punti di accesso e seleziona Crea punto di accesso.
6. Nella pagina Crea, inserisci un nome per il punto di accesso.
7. (Facoltativo) Specificate il percorso della directory principale per il punto di accesso. I client che utilizzano questo punto di accesso saranno limitati a questa directory e alle relative sottodirectory. Per impostazione predefinita, S3 Files presuppone che la directory principale del punto di accesso sia la directory principale del file system.
8. (Facoltativo) Nel pannello utente POSIX, è possibile specificare l'identità POSIX completa da utilizzare per applicare le informazioni su utenti e gruppi per tutte le operazioni sui file da parte dei client che utilizzano il punto di accesso.
 - ID utente - Immetti l'ID utente POSIX numerico dell'utente.
 - ID gruppo - Immetti l'ID numerico del gruppo POSIX dell'utente.

- ID gruppi secondari - Immetti un elenco di ID gruppi secondari facoltativi separati da virgole.
9. (Facoltativo) Per le autorizzazioni per la creazione della directory principale, è possibile specificare le autorizzazioni da utilizzare quando S3 Files crea il percorso della directory principale, se specificato e la directory principale non esiste già.

Note

Se non specifichiate la proprietà e le autorizzazioni della directory principale e la directory principale non esiste già, S3 Files non creerà la directory principale. Qualsiasi tentativo di montare il file system utilizzando il punto di accesso avrà esito negativo.

- ID utente proprietario: immetti l'ID utente POSIX numerico da utilizzare come proprietario della directory radice.
 - ID gruppo proprietario: immetti l'ID gruppo POSIX numerico da utilizzare come gruppo proprietario della directory radice.
 - Permessi: immetti la modalità Unix della directory. Una configurazione comune è 755. Assicurati che il bit di esecuzione sia impostato per l'utente del punto di accesso in modo che sia in grado di eseguire il montaggio.
- 10.(Facoltativo) In Tag, puoi scegliere di aggiungere tag al tuo punto di accesso.
- 11.Scegli Crea punto di accesso.

Utilizzo di AWS CLI

Il seguente comando di `create-access-point` esempio mostra come utilizzare la AWS CLI per creare un punto di accesso per un file system S3.

```
aws s3files create-access-point --file-system-id file-system-id --root-directory root-directory --posix-user posix-user
```

Ad esempio:

```
aws s3files create-access-point --file-system-id fs-abcdef0123456789a --client-token 010102020-3 \
  --root-directory "Path=/s3files/mobileapp/
east,CreationInfo={OwnerId=0,OwnerGid=11,Permissions=775}" \
  --posix-user "Uid=22,Gid=4" \
```

```
--tags Key=Name,Value=east-users
```

Note

Se più richieste di creazione di punti di accesso sullo stesso file system vengono inviate in rapida successione e il file system si avvicina al limite dei punti di accesso, è possibile che si verifichi una risposta limitata per queste richieste. Questo serve a garantire che il file system non superi la quota del punto di accesso.

Eliminazione dei punti di accesso per un file system S3

Quando si elimina un punto di accesso, assicurarsi che nessuna applicazione lo stia utilizzando attivamente prima dell'eliminazione per evitare interruzioni del servizio. Una volta eliminato, il punto di accesso e la relativa configurazione vengono rimossi definitivamente.

Utilizzo della console S3

Questa sezione spiega come utilizzare la console Amazon S3 per eliminare un punto di accesso per i file S3.

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, verifica di trovarti nella AWS regione del file system in cui è presente il punto di accesso che desideri eliminare.
3. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
4. Scegliete un bucket generico a cui è collegato il file system.
5. Seleziona la scheda File system e seleziona il file system che desideri utilizzare.
6. Seleziona la scheda Punti di accesso e seleziona il punto di accesso che desideri eliminare.
7. Scegli Elimina.
8. Nella finestra di conferma, digita **confirm** e scegli Elimina.

Utilizzo di AWS CLI

Il comando di `delete-access-point` esempio seguente mostra come utilizzare la AWS CLI per eliminare un punto di accesso per i file S3.

```
aws s3files delete-access-point --access-point-id access-point-id
```

Etichettare le risorse dei file S3

Per aiutarti a gestire le tue risorse S3 Files, puoi assegnare i tuoi metadati a ciascuna risorsa sotto forma di tag. Con i tag, puoi classificare AWS le tue risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa categorizzazione è utile quando si hanno molte risorse dello stesso tipo, in quanto è possibile identificare rapidamente una risorsa specifica in base ai tag che le sono stati assegnati. Puoi taggare le risorse del file system S3 e dei punti di accesso che già esistono nel tuo account. Questo argomento descrive i tag e mostra come crearli.

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50
- Per ogni risorsa, ogni chiave di tag deve essere unica e ogni chiave di tag può avere un solo valore.
- Lunghezza massima della chiave: 128 caratteri Unicode in UTF-8
- Lunghezza massima del valore: 256 caratteri Unicode in UTF-8
- I caratteri consentiti sono: lettere, numeri e spazi rappresentabili in UTF-8, e i seguenti caratteri: . + - = . _ : / @
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.
- Il `aws :` prefisso è riservato all'uso AWS . Se il tag ha una chiave di tag con questo prefisso, non puoi modificare o eliminare la chiave o il valore de tag. I tag con il prefisso `aws :` non vengono conteggiati per il limite del numero di tag per risorsa.

Non puoi aggiornare o eliminare una risorsa solo sulla base dei relativi tag. Devi specificare il relativo identificatore. Ad esempio, per eliminare i file system etichettati con una chiave di tag chiamata `DeleteMe`, è necessario utilizzare l'`DeleteFileSystem` azione con gli identificatori di risorsa del file system, ad esempio l'ID del file system.

Quando tagghi risorse pubbliche o condivise, i tag che assegni sono disponibili solo per il tuo AWS account. Nessun altro AWS account avrà accesso a quei tag. Per il controllo dell'accesso basato su tag alle risorse condivise, ogni AWS account deve assegnare il proprio set di tag per controllare l'accesso alla risorsa.

Utilizzo della console S3

Puoi utilizzare la console S3 Files per gestire i tag sulle tue risorse.

- Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
- Nella barra di navigazione, verifica di trovarti nella AWS regione desiderata.
- Nel pannello di navigazione a sinistra, scegli File system.
- È possibile specificare i tag per una risorsa al momento della creazione della risorsa, ad esempio un file system S3 o un punto di accesso. In alternativa, puoi aggiungere, modificare o eliminare i tag dopo la creazione accedendo alle proprietà della risorsa.

Utilizzo di AWS CLI

Se utilizzi l'API S3 Files, la AWS CLI o AWS un SDK, puoi utilizzare TagResource l'azione API S3 Files per applicare tag alle risorse esistenti. Inoltre, alcune azioni di creazione di risorse consentono di specificare i tag per una risorsa al momento della creazione della risorsa, ad esempio quando si crea un file system.

I comandi AWS CLI per la gestione dei tag e le azioni API S3 Files equivalenti sono elencati nella tabella seguente.

Comando CLI	Description	Operazione API equivalente
tag-resource	Aggiungere nuovi tag o aggiornare i tag esistenti	TagResource
list-tags-for-resource	Recuperare i tag esistenti	ListTagsForResource
untag-resource	Eliminare i tag esistenti	UntagResource

Comprendere come funziona la sincronizzazione

S3 Files mantiene il file system e il bucket S3 collegato sincronizzati automaticamente. I dati utilizzati attivamente vengono copiati nel file system, in modo da poter leggere e scrivere file utilizzando le

operazioni sui file standard di Linux a bassa latenza. S3 Files richiede che il versionamento S3 sia abilitato sul bucket S3 collegato. Quando modifichi i file sul file system, S3 Files copia le modifiche nel bucket S3 come nuove versioni degli oggetti corrispondenti, assicurandosi che le vecchie versioni vengano conservate. Quando altre applicazioni aggiungono, modificano o eliminano oggetti nel bucket S3, S3 Files riflette automaticamente tali modifiche nel file system. Quando si verifica un conflitto a causa di modifiche simultanee agli stessi dati sia nel file system che nel bucket S3, S3 Files considera il bucket S3 come fonte di verità [in caso di conflitti](#).

Per ottimizzare i costi di archiviazione, S3 Files rimuove dal file system i dati non utilizzati di recente. I dati rimangono archiviati in modo duraturo nel bucket S3 collegato e vengono recuperati nel file system al successivo accesso.

Il bucket S3 è accessibile tramite il file system

Dopo aver creato un file system S3, puoi [montare i bucket S3 su risorse di calcolo](#) e iniziare subito ad accedere ai dati del bucket S3. Per impostazione predefinita, quando accedi per la prima volta a una directory elencandone il contenuto o aprendo un file al suo interno, S3 Files importa i metadati di tutti i file in quella directory, insieme ai dati per i file inferiori alla soglia di dimensione di importazione (impostazione predefinita 128 KiB) dal bucket S3. Il primo accesso a una directory potrebbe avere una latenza più elevata, ma le letture e le scritture successive sono notevolmente più veloci. Importando i metadati in anticipo, S3 Files consente di sfogliare i contenuti delle directory, visualizzare le dimensioni dei file e controllare le autorizzazioni a bassa latenza.

Ad esempio, supponiamo che il bucket S3 contenga un prefisso con 1.000 oggetti. `data/images/`. La prima volta che si esegue `ls /mnt/s3files/data/images/`, S3 Files importa i metadati per tutti i 1.000 file e copia in modo asincrono i dati per i file al di sotto della soglia di dimensione di importazione nel file system. L'elenco iniziale può richiedere alcuni secondi, ma i comandi successivi, ad esempio, `cat` sui singoli file di quella `stat` directory `ls -la`, vengono restituiti a bassa latenza.

Per i file di dimensioni superiori alla soglia di importazione, S3 Files importa solo metadati, mentre i dati non vengono copiati nel file system e vengono invece letti direttamente dal bucket S3 quando vi si accede. Puoi modificare questa soglia per adattarla meglio al tuo carico di lavoro. Ad esempio, puoi aumentarla per importare più dati in anticipo per i carichi di lavoro che accedono ripetutamente agli stessi file e beneficiano di letture a bassa latenza. Per i carichi di lavoro che trasmettono dati in modo sequenziale, una soglia più bassa può essere più conveniente, poiché il vantaggio in termini di latenza derivante dall'importazione anticipata dei dati è meno significativo quando i dati vengono letti in sequenza in grandi blocchi anziché in piccole letture casuali. Per ulteriori informazioni, consulta [Personalizzazione della sincronizzazione per i file S3](#).

Le modifiche al file system si riflettono automaticamente nel bucket S3

Quando crei, modifichi o elimini file nel file system, S3 Files copia automaticamente tali modifiche nel bucket S3. I nuovi file diventano nuovi oggetti S3, le modifiche ai file esistenti diventano nuove versioni degli oggetti e i file eliminati diventano indicatori di eliminazione S3.

Le autorizzazioni POSIX impostate su file e directory tramite il file system, ad esempio owner (UID), group (GID) e bit di autorizzazione, vengono archiviate come metadati degli oggetti S3 definiti dall'utente negli oggetti S3 corrispondenti. Quando modifichi le autorizzazioni utilizzando `chmod`, `chown`, S3 Files esporta tali modifiche nel bucket S3 `chgrp` insieme a qualsiasi modifica ai dati. Quando S3 Files importa oggetti dal bucket S3, legge questi metadati e applica le autorizzazioni POSIX corrispondenti sul file system. Agli oggetti che non dispongono dei metadati delle autorizzazioni POSIX vengono assegnate le autorizzazioni predefinite.

Quando un file viene modificato sul file system, S3 Files attende un periodo di inattività di scrittura (60 secondi) prima di esportare nuovamente le modifiche nel bucket S3. Le scritture rapide e successive sullo stesso file vengono acquisite in una singola richiesta PUT S3 anziché generare più versioni dell'oggetto per ogni singola modifica. Ciò riduce sia i costi delle richieste S3 che i costi di archiviazione. È possibile utilizzare questa finestra di inattività di 60 secondi come trigger di esportazione. Ad esempio, se l'applicazione aggiunge dati a un file ogni 30 secondi per un totale di 5 minuti, S3 Files avvia il processo di esportazione al minuto 6. Se si apportano ulteriori modifiche, il processo si ripete dopo ogni periodo di 60 secondi di inattività di scrittura.

Le modifiche nel bucket S3 vengono visualizzate automaticamente nel file system

S3 Files monitora le modifiche nel bucket S3 utilizzando le notifiche di eventi S3. Quando un'altra applicazione che funziona con l'API S3 aggiunge, modifica o elimina oggetti nel bucket S3, S3 Files riflette automaticamente tali modifiche nel file system per i file i cui dati sono attualmente archiviati nella memoria ad alte prestazioni del file system. I file i cui dati sono scaduti dal file system non vengono aggiornati fino al successivo accesso, dopodiché S3 Files recupera la versione più recente dal bucket S3.

Comprendere l'impatto delle operazioni di ridenominazione e spostamento

Amazon S3 utilizza una struttura di storage piatta in cui gli oggetti sono identificati dai loro nomi chiave. Mentre S3 Files consente di organizzare i dati in directory, S3 non ha un concetto nativo di directory. Ciò che appare come una directory nel file system è un prefisso comune condiviso dalle

chiavi degli oggetti all'interno del bucket S3. Inoltre, gli oggetti S3 sono immutabili e non supportano le ridenominazioni atomiche. Di conseguenza, quando si rinomina o si sposta un file, S3 Files deve scrivere i dati su un nuovo oggetto con la chiave aggiornata ed eliminare l'originale. Quando si rinomina o si sposta una directory, S3 Files deve ripetere questo processo per ogni oggetto che condivide quel prefisso. Pertanto, quando si rinomina o si sposta una directory contenente decine di milioni di file, i costi delle richieste S3 e il tempo di sincronizzazione aumentano notevolmente.

S3 Files restituisce un errore quando si tenta di creare un file system con un prefisso con un numero elevato di oggetti, in modo tale che la ridenominazione possa richiedere fino a 4 ore (circa fino a 12 milioni di oggetti). Questo errore segnala che le operazioni di ridenominazione o spostamento ricorsive di grandi dimensioni possono influire sulle prestazioni del file system, poiché ogni file richiede richieste di scrittura ed eliminazione separate nel bucket S3. Se desideri comunque creare un file system con ambito di quel prefisso, puoi aggiungere il parametro. `--AcceptBucketWarning`

Poiché S3 Files rinomina gli oggetti singolarmente nel bucket S3, entrambe le directory saranno visibili nel bucket S3 fino al completamento della ridenominazione. Gli oggetti scritti dopo che la directory è stata rinominata ma prima che la ridenominazione sia completamente sincronizzata non verranno spostati. Per semplificare il lavoro di riorganizzazione dei dati, si consiglia di non creare nuovi oggetti tramite il bucket S3 durante la ridenominazione di una directory corrispondente.

Ad esempio, se esegui `mv /mnt/s3files/projects/alpha /mnt/s3files/projects/beta`, la ridenominazione viene completata immediatamente sul file system. Nel bucket S3, S3 Files inizia a copiare ed eliminare ogni oggetto nella nuova chiave all'interno del bucket S3 (sostituendo il prefisso con) e a eliminare l'originale. `projects/alpha/ projects/beta/` Durante questo processo, il bucket S3 contiene temporaneamente oggetti sia sotto che. `projects/alpha/ projects/beta/` Una volta che tutti gli oggetti sono stati spostati, ne rimane solo `projects/beta/` uno.

I dati non utilizzati vengono eliminati dal file system per ottimizzare l'archiviazione

S3 Files ottimizza i costi di archiviazione rimuovendo automaticamente dal file system i dati dei file che non sono stati letti di recente. I tuoi dati rimangono archiviati in modo sicuro nel tuo bucket S3. S3 Files rimuove solo la copia dal file system. I metadati dei file, come nomi, dimensioni e autorizzazioni, non vengono mai rimossi dal file system in modo da poter continuare a navigare nel file system a bassa latenza.

Se un file nel file system non viene letto da 30 giorni (configurabile) e le relative modifiche sono già state sincronizzate nel bucket S3, S3 Files rimuove i dati del file dal file system. Alla successiva

lettura del file, S3 Files recupera l'ultima versione dell'oggetto corrispondente dal bucket S3 e la copia nuovamente nel file system.

Ad esempio, supponiamo di elaborare un set di dati `/mnt/s3files/data/batch-jan.parquet` a gennaio e di non accedervi nuovamente. Dopo 30 giorni, S3 Files rimuove i dati del file dal file system. Il file viene ancora visualizzato negli elenchi delle directory con le dimensioni e le autorizzazioni corrette, ma i dati non sono più presenti nel file system. Quando rileggi il file ad aprile, S3 Files lo recupera dal bucket S3 e lo copia nuovamente nel file system. La prima lettura può avere una latenza maggiore, ma le letture successive sono veloci.

Il bucket S3 è la fonte della verità in caso di conflitti

Un conflitto si verifica quando lo stesso file è stato modificato tramite il file system e anche l'oggetto S3 corrispondente è cambiato prima che S3 Files abbia sincronizzato le modifiche al file system nel bucket S3. Ad esempio, è possibile modificare un file tramite il file system montato mentre un'altra applicazione carica una nuova versione dell'oggetto corrispondente, o la elimina, direttamente nel bucket S3 collegato.

S3 Files rileva i conflitti quando tenta di sincronizzare le modifiche apportate al file system nel bucket S3 o quando riceve una notifica di evento S3 che indica che l'oggetto è cambiato. Il bucket S3 funge da archivio a lungo termine per i tuoi dati, quindi S3 Files considera il bucket S3 come fonte di verità in caso di conflitto. Ciò garantisce una coerenza prevedibile, assicurando che la versione nel bucket S3 abbia sempre la precedenza. In caso di conflitto, S3 Files sposta il file in conflitto dalla posizione corrente nel file system in una directory smarrita e importa la versione più recente dal bucket S3 collegato nel file system.

Ad esempio, supponiamo di modificare `/mnt/s3files/report.csv` tramite il file system. Prima che S3 Files sincronizzi nuovamente le modifiche nel bucket S3, un'altra applicazione carica una nuova versione direttamente nel bucket S3. `report.csv` Quando S3 Files rileva il conflitto, sposta la tua versione nella directory degli oggetti smarriti e `report.csv` la sostituisce con la versione del bucket S3.

La directory degli oggetti smarriti si trova nella directory principale del file system con il nome `.s3files-lost+found-file-system-id`. Se si monta il file system tramite un punto di accesso che specifica una directory principale, la directory smarrita non è visibile da quel mount perché si trova sopra la directory principale del punto di accesso. Per accedere alla directory smarrita, montate il file system senza un punto di accesso o utilizzate un punto di accesso senza una restrizione alla directory principale in modo da poter accedere all'intero ambito del file system tramite il punto di accesso.

Quando S3 Files sposta un file nella directory degli oggetti smarriti, aggiunge al nome del file un identificatore per distinguere più versioni dello stesso file che possono essere spostate nel tempo. I file nella directory degli oggetti smarriti non vengono copiati nel bucket S3. È possibile eliminare file e copiare file da questa directory, ma non è possibile spostare o rinominare i file al suo interno o eliminare la directory stessa. Se desideri mantenere le modifiche al file system invece della versione più recente nel bucket S3, copia il file dalla directory oggetti smarriti nel percorso originale. Puoi recuperare il percorso originale del file dagli attributi estesi del file nella directory degli oggetti smarriti. S3 Files lo copierà quindi nel bucket S3 come nuova versione dell'oggetto. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi ai file S3](#).

Note

I file in conflitto che S3 Files sposta nella directory degli oggetti smarriti rimangono lì a tempo indeterminato e vengono conteggiati ai fini dei costi di archiviazione del file system. È necessario eliminare i file dalla directory oggetti smarriti per liberare spazio di archiviazione quando non sono più necessari.

Le impostazioni di sincronizzazione predefinite funzioneranno per la maggior parte dei carichi di lavoro per l'accesso ai dati S3 a bassa latenza e basato su file. Per maggiori dettagli su come configurare questi parametri, consulta [Personalizzazione della sincronizzazione per i file S3](#)

Argomenti

- [Personalizzazione della sincronizzazione per i file S3](#)

Personalizzazione della sincronizzazione per i file S3

S3 Files ti consente di controllare il flusso di dati tra il file system e il bucket S3 collegato tramite una configurazione di sincronizzazione. Le impostazioni predefinite bilanciano latenza e costi per la maggior parte dei carichi di lavoro, ma puoi ottimizzarle in base ai tuoi modelli di accesso. L'importazione anticipata di più dati riduce la latenza di lettura a scapito di costi di archiviazione e scrittura più elevati. L'importazione di meno dati mantiene bassi i costi di archiviazione, ma significa che vengono servite più letture da S3 con una latenza più elevata. Ogni configurazione ha due componenti: le regole di importazione dei dati, che controllano quali dati vengono copiati sul file system e quando, e le regole sui dati di scadenza, che controllano per quanto tempo i dati inutilizzati rimangono nel file system. È possibile aggiornare queste regole utilizzando la console di AWS gestione o l' `PutSynchronizationConfiguration` API.

Regole di importazione dei dati

Le regole di importazione dei dati controllano il modo in cui i dati vengono copiati dal bucket al file system. È possibile avere un massimo di 10 regole di importazione dei dati per file system. Ogni regola di importazione dei dati ha i seguenti parametri:

prefisso: il prefisso S3 a cui si applica la regola. Specificate una stringa vuota («») per l'intero bucket (ambito del file system) o un prefisso specifico (ad esempio, «data/ml/») all'interno del file system. Il prefisso deve terminare con una barra (/), a meno che non si specifichi l'intero bucket con «». È necessario includere esattamente una regola di importazione per la directory principale. Impostazione predefinita: «» (intero bucket o ambito del file system).

trigger — Quando importare i dati: `ON_DIRECTORY_FIRST_ACCESS` o `ON_FILE_ACCESS`.
Impostazione predefinita: `ON_DIRECTORY_FIRST_ACCESS`.

- `ON_DIRECTORY_FIRST_ACCESS`: i dati del file vengono importati quando si accede per la prima volta a una directory. Ad esempio, quando accedete per la prima volta a una directory elencandone il contenuto o aprendo un file al suo interno, vengono importati i dati per tutti i file figlio immediati presenti in quella directory di dimensioni inferiori alla soglia. `sizeLessThan` Questa opzione è utile per i carichi di lavoro che richiedono una bassa latenza al primo accesso ai file.
- `ON_FILE_ACCESS` — I dati del file vengono importati solo quando un file viene letto per la prima volta. Questa opzione riduce al minimo i dati importati a scapito di una maggiore latenza alla prima lettura.

sizeLessThan— Dimensione massima del file (in byte) da importare automaticamente. Sebbene S3 Files importi i metadati per tutti i file, importa solo i dati per i file più piccoli di questa soglia. Minimo: 0 byte (nessun dato importato, i metadati verranno comunque importati). Massimo: 52.673.613.135.872 byte (48 TiB). Impostazione predefinita: 131.072 byte (128 KiB).

Comportamento della corrispondenza dei prefissi

Quando più regole di importazione dei dati corrispondono a un file, S3 Files applica la regola con il prefisso più specifico. Ad esempio, supponiamo di avere tre regole:

- Regola 1: prefisso = «» (intero bucket), `sizeLessThan` = 64 KiB, trigger = `ON_FILE_ACCESS`
- Regola 2: prefisso = «hot/», = 1 MiB, trigger `sizeLessThan` = `ON_DIRECTORY_FIRST_ACCESS`
- Regola 3: prefix = «hot/LargeData/», = 256 KB, trigger = `sizeLessThan`
`ON_DIRECTORY_FIRST_ACCESS`

Per un file in `hot/largeData/data.txt`, S3 Files applies Rule 3. For a file at `hot/data.txt`, S3 Files applies Rule 2. For a file at `cold/data formato.txt`, S3 Files applica la regola 1 perché non esiste una regola specifica per il prefisso `cold/`.

Regole relative ai dati di scadenza

Le regole relative ai dati di scadenza controllano quando i dati non utilizzati vengono rimossi dal file system per ottimizzare i costi di archiviazione. S3 Files rimuove i dati dopo che non sono stati letti per una durata specificata e le modifiche sono già state sincronizzate con il bucket S3. Ogni volta che un file viene letto, il relativo timer di scadenza si reimposta, prolungando il tempo di permanenza dei dati nel file system. È possibile specificare il seguente parametro nelle regole relative ai dati di scadenza:

`daysAfterLastAccesso`: numero di giorni dopo l'ultima lettura quando i dati vengono rimossi dal file system. Minimo: 1 giorno. Massimo: 365 giorni. Impostazione predefinita: 30 giorni.

Se hai carichi di lavoro di lunga durata che accedono spesso agli stessi dati, prendi in considerazione periodi di scadenza più lunghi (30-90 giorni). Per i dati temporanei, prendi in considerazione periodi più brevi (1-7 giorni).

Configurazioni di esempio

Condivisione di file per scopi generici (configurazione predefinita): un team di sviluppatori e data scientist monta un file system S3 per condividere codice, file di configurazione e set di dati di piccole dimensioni. La maggior parte dei file ha una dimensione inferiore a 128 KiB e viene letta ripetutamente nel corso della giornata. La configurazione predefinita è ideale per questo carico di lavoro: `ON_DIRECTORY_FIRST_ACCESS` importa metadati e dati di file di piccole dimensioni quando si accede per la prima volta a qualsiasi file in una directory, il che funziona bene quando è probabile che si acceda contemporaneamente ai file nella stessa directory, come i file di origine in un progetto o i file di configurazione in una distribuzione. L'accesso successivo da parte di qualsiasi utente è rapido. Quando un utente apre un file di grandi dimensioni come un archivio di log, S3 Files lo trasmette automaticamente direttamente da S3 per un throughput elevato. La finestra di scadenza di 30 giorni mantiene i file utilizzati attivamente sul file system senza pulizia manuale.

Formazione ML con letture ripetute: un processo di formazione legge ripetutamente migliaia di file di piccole dimensioni (<10 MiB) in più epoche. Per ridurre al minimo la latenza, impostate una `sizeLessThan` soglia alta (ad esempio, 10 MiB) con `ON_DIRECTORY_FIRST_ACCESS` in modo che i dati del file vengano precaricati quando lo script di addestramento elenca per la prima volta ciascuna directory. Imposta una scadenza breve (ad esempio, 3 giorni) in modo che i dati vengano rimossi dal file system subito dopo il completamento del processo di formazione.

Carichi di lavoro agentici con ampio rilevamento dei file: un agente di intelligenza artificiale esplora un ampio archivio di documenti, codice o file di knowledge base per rispondere alle domande, leggendo molti file di piccole dimensioni una volta mentre cerca il contesto pertinente. Imposta su 0 `sizeLessThan` in modo che nessun dato venga importato nel file system. L'agente può sfogliare l'intero albero di directory a bassa latenza per scoprire i file, mentre ogni file letto viene fornito direttamente da S3. Ciò mantiene bassi i costi per i carichi di lavoro che toccano molti file in modo imprevedibile ma che raramente rivisitano lo stesso file, e si ridimensiona naturalmente man mano che si aggiungono più agenti che leggono in parallelo.

Prefissi caldi e freddi: un file system contiene sia i file di configurazione a cui si accede di frequente che i dati di archivio a cui si accede raramente. `config/` `archive/`
Crea due regole di importazione: una per `config/` con un valore alto `sizeLessThan` e `ON_DIRECTORY_FIRST_ACCESS` e una per con impostato su 0 e `ON_FILE_ACCESS`. `archive/sizeLessThan` Ciò mantiene i file di configurazione sul file system per un accesso rapido, evitando al contempo i costi di archiviazione per i dati di archiviazione che vengono letti raramente.

Monitoraggio e controllo dei file S3

S3 Files si integra con i seguenti AWS servizi per aiutarvi a monitorare i vostri file system:

Amazon CloudWatch

Per impostazione predefinita, i dati metrici di S3 Files vengono inviati automaticamente a intervalli di 1 minuto, CloudWatch a meno che non sia specificato diversamente per alcune metriche individuali. Puoi anche controllare una singola metrica in un periodo di tempo specificato ed eseguire una o più azioni in base al valore della metrica rispetto a una determinata soglia in un certo numero di periodi di tempo. L'operazione è una notifica inviata a un argomento Amazon Simple Notification Service (Amazon SNS) o alla policy di Amazon EC2 Auto Scaling.

Per ulteriori informazioni, consulta [Monitoraggio dei file S3 con Amazon CloudWatch](#).

CloudTrail

CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. S3 Files registra gli eventi di gestione, tra cui la creazione di file system, la creazione di destinazioni di montaggio e il montaggio dei file system sulle istanze di calcolo. S3 Files non registra gli eventi relativi ai dati, come le operazioni di lettura e scrittura dei file.

Per ulteriori informazioni, consulta [Registrazione con CloudTrail per i file S3](#).

Argomenti

- [Monitoraggio dei file S3 con Amazon CloudWatch](#)
- [Registrazione con CloudTrail per i file S3](#)

Monitoraggio dei file S3 con Amazon CloudWatch

Puoi monitorare i file system S3 Files utilizzando [Amazon CloudWatch](#), che raccoglie ed elabora i dati grezzi da Amazon S3 Files in metriche leggibili. Queste metriche vengono conservate per 15 mesi, in modo da poter accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni dei file system.

I dati metrici di S3 Files vengono inviati automaticamente a CloudWatch. La maggior parte delle metriche viene inviata a intervalli di 1 minuto, mentre le metriche di archiviazione vengono inviate ogni 15 minuti. Puoi creare [CloudWatch allarmi](#) che inviano notifiche quando una metrica supera una soglia specificata. Puoi anche utilizzare i CloudWatch dashboard, che sono home page personalizzabili nella CloudWatch Console che puoi utilizzare per monitorare le tue risorse in un'unica visualizzazione. Per ulteriori informazioni, consulta [Creazione di un CloudWatch pannello di controllo personalizzato](#).

Metriche dei file CloudWatch S3

Le metriche di S3 Files utilizzano lo spazio dei nomi. `AWS/S3/Files` Tutte le metriche vengono riportate per una singola dimensione. `FileSystemId` Lo spazio dei nomi `AWS/S3/Files` include i parametri descritti di seguito:

Metrica	Description	Unità e statistiche valide
<code>StorageBytes</code>	La dimensione totale del file system in byte, che include dati e metadati. Questa metrica viene emessa ogni 15 minuti. CloudWatch	Unità: byte. Minimo, massimo, medio
<code>Inodes</code>	Il numero totale di inode (come file, directory, collegamenti simbolici) in un file system S3 Files. Questa metrica viene emessa ogni 15 minuti. CloudWatch	Unità: conta. Somma

Metrica	Description	Unità e statistiche valide
PendingExports	Il numero totale di file e directory in attesa di esportazione nel bucket S3.	Unità: conta. Somma
ImportFailures	Il numero totale di oggetti che non sono stati importati nel file system dopo nuovi tentativi (ad esempio, autorizzazioni IAM errate).	Unità: conteggio. Somma
ExportFailures	Numero totale di file e directory che non sono stati esportati e che non verranno ritentati. Questa metrica consente di identificare gli errori di esportazione dei terminali in modo da poter risolvere i problemi e intervenire (ad esempio, aggiornare le autorizzazioni IAM).	Unità: conteggio. Somma
ImportAge	L'età delle modifiche in corso che il file system importa dal bucket S3 collegato. L'età viene misurata a partire dal momento in cui si è verificata ogni modifica nel bucket. Utilizza questa metrica per monitorare se le importazioni sono aggiornate. Un aumento sostenuto significa che le importazioni sono in ritardo rispetto alle variazioni del periodo.	Unità: secondi
ExportAge	L'età delle modifiche in corso che il file system esporta nel bucket S3 collegato. L'età viene misurata a partire dal momento in cui si è verificata ogni modifica nel file system. Utilizza questa metrica per monitorare se le esportazioni sono aggiornate. Un aumento sostenuto significa che le esportazioni sono in ritardo rispetto alle modifiche apportate al file system.	Unità: secondi

Metrica	Description	Unità e statistiche valide
DataReadBytes	Il numero di byte letti dal file system. <code>SampleCount</code> fornisce il numero di operazioni di lettura dei dati. È possibile calcolare la velocità effettiva di lettura dei dati visualizzando questa metrica per unità di tempo.	Unità: byte (minimo, massimo, media, somma), conteggio () <code>SampleCount</code>
DataWriteBytes	Il numero di byte scritti nel file system. <code>SampleCount</code> fornisce il numero di operazioni di scrittura dei dati. È possibile calcolare la velocità di scrittura dei dati visualizzando questa metrica per unità di tempo.	Unità: byte (minimo, massimo, media, somma), conteggio () <code>SampleCount</code>
MetadataReadBytes	Il numero di byte di metadati letti dal file system. <code>SampleCount</code> fornisce il numero di operazioni di lettura dei metadati.	Unità: byte (minimo, massimo, media, somma), conteggio () <code>SampleCount</code>
MetadataWriteBytes	Il numero di byte di metadati scritti nel file system. <code>SampleCount</code> fornisce il numero di operazioni di scrittura dei metadati.	Unità: byte (minimo, massimo, media, somma), conteggio () <code>SampleCount</code>
LostAndFoundFiles	Numero totale di file nella directory degli oggetti smarriti. La directory persa e trovata si trova nella directory principale del file system sotto il nome <code>.s3files-lost+found-<i>file-system-id</i></code> . I file nella directory degli oggetti smarriti non vengono copiati nel bucket S3. Quando si verifica un conflitto dovuto a modifiche simultanee e agli stessi dati sia nel file system che nel bucket S3, S3 Files considera il bucket S3 come fonte di informazioni e sposta il file in conflitto in una directory smarrita.	Unità: conta. Somma

Metrica	Description	Unità e statistiche valide
ClientConnections	Il numero di connessioni client attive a un file system.	Unità: conteggio. Somma

Metriche di connettività dei client

S3 Files può ottimizzare le prestazioni di lettura consentendo ai client di leggere i dati dei file direttamente dal bucket S3 collegato. A supporto di ciò, il client S3 Files emette metriche di connettività che controllano se il client è in grado di stabilire le connessioni necessarie.

Queste metriche vengono emesse dal client S3 Files (amazon-efs-utils) e pubblicate nel namespace. efs-utils/S3Files CloudWatch L'emissione delle metriche è abilitata per impostazione predefinita come parte dell'esperienza S3 Files.

Metrica	Description	Unità e statistiche valide
NFSConnectionAccessible	Indica se il client può connettersi al file system tramite il montaggio NFS. Il valore 1 indica che la connessione è accessibile. Il valore 0 indica che la connessione non è accessibile.	Unità: nessuna. Minimo, massimo, medio
S3BucketAccessible	Indica se il client dispone delle autorizzazioni necessarie per leggere i dati dal bucket S3 collegato. Il valore 1 indica che il client dispone delle autorizzazioni necessarie. Un valore pari a 0 indica che il client non dispone delle autorizzazioni necessarie.	Unità: nessuna. Minimo, massimo, medio
S3BucketReachable	Indica se il bucket e il prefisso S3 collegati esistono e sono raggiungibili dal client. Il valore 1 indica che il bucket e il prefisso sono raggiungibili. Un valore pari a 0 indica che il bucket o il prefisso non è raggiungibile.	Unità: nessuna. Minimo, massimo, medio

Accesso alle CloudWatch metriche

Puoi visualizzare le metriche di S3 Files utilizzando la CloudWatch console, la AWS CLI o l'API. CloudWatch

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel riquadro di navigazione, scegli Metriche, quindi scegli Tutte le metriche.
3. Scegli lo spazio dei nomi S3Files.
4. Scegli File System Metrics.
5. Seleziona le metriche che desideri visualizzare.
6. Scegli la scheda Metriche grafiche per configurare la visualizzazione del grafico.

Per visualizzare le metriche utilizzando il AWS CLI

Utilizza il comando `get-metric-statistics`. Ad esempio, per visualizzare: `DataReadBytes`

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/S3/Files \
  --metric-name DataReadBytes \
  --dimensions Name=FileSystemId,Value=file-system-id \
  --start-time 2025-01-20T00:00:00Z \
  --end-time 2025-01-20T23:59:59Z \
  --period 3600 \
  --statistics Sum
```

Registrazione con CloudTrail per i file S3

Amazon S3 Files è integrato con CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in S3 Files. CloudTrail acquisisce tutte le chiamate API per S3 Files come eventi, incluse le chiamate dalla console S3 Files e le chiamate di codice alle operazioni dell'API S3 Files.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per i file S3. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte

da CloudTrail, puoi determinare la richiesta che è stata fatta a S3 Files, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Informazioni sui file S3 in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Amazon S3 Files, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#) nella Guida CloudTrail per l'utente.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per i file S3, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utenteCloudTrail :

- [Creare un percorso per il tuo account AWS](#)
- [AWS integrazioni di servizi con log CloudTrail](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Tutti i [file S3 APIs](#) vengono registrati da. CloudTrail Ad esempio, le chiamate a CreateMountTarget e CreateFileSystem le TagResource operazioni generano voci nei file di CloudTrail registro. S3 Files genera CloudTrail registri anche quando si monta il file system su una risorsa di calcolo.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS .

Per ulteriori informazioni, vedete l'[elemento CloudTrail UserIdentity nella Guida](#) per l'CloudTrail utente.

S3 Files non registra gli eventi relativi ai dati. Gli eventi relativi ai dati includono le operazioni di lettura e scrittura dei file eseguite sul file system.

Informazioni sulle voci dei file di registro di S3 Files

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Esempio: CreateFileSystem

L'esempio seguente mostra una voce di CloudTrail registro che illustra l>CreateFileSystemazione:

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "111122223333",
    "arn": "arn:aws:sts::111122223333:assumed-role/myRole/i-0123456789abcdef0",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:role/myRole",
        "accountId": "111122223333",
        "userName": "myRole"
      },
      "attributes": {
        "creationDate": "2026-03-20T12:58:28Z",
        "mfaAuthenticated": "false"
      },
      "ec2RoleDelivery": "2.0"
    }
  },
  "eventTime": "2026-03-20T17:43:19Z",
```

```

    "eventSource": "s3files.amazonaws.com",
    "eventName": "CreateFileSystem",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0",
    "requestParameters": {
        "bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
        "prefix": "images/",
        "clientToken": "myClientToken",
        "roleArn": "arn:aws:iam::111122223333:role/myS3FilesRole"
    },
    "responseElements": {
        "creationTime": "Mar 20, 2026, 5:43:19 PM",
        "fileSystemArn": "arn:aws:s3files:us-west-2:111122223333:file-system/fs-
abcd123456789ef0",
        "fileSystemId": "fs-abcd123456789ef0",
        "bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
        "prefix": "images/",
        "clientToken": "myClientToken",
        "status": "creating",
        "roleArn": "arn:aws:iam::111122223333:role/myS3FilesRole",
        "ownerId": "111122223333",
        "tags": []
    },
    "requestID": "dEXAMPLE-feb4-11e6-85f0-736EXAMPLE75",
    "eventID": "eEXAMPLE-2d32-4619-bd00-657EXAMPLEe4",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::S3Files::FileSystem",
            "ARN": "arn:aws:s3files:us-west-2:111122223333:file-system/fs-
abcd123456789ef0"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "s3files.us-west-2.api.aws"
    }
}

```

```
}
```

Esempio: CreateMountTarget

L'esempio seguente mostra una voce di CloudTrail registro per l'CreateMountTargetazione:

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "111122223333",
    "arn": "arn:aws:sts::111122223333:assumed-role/myRole/i-0123456789abcdef0",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:role/myRole",
        "accountId": "111122223333",
        "userName": "myRole"
      },
      "attributes": {
        "creationDate": "2026-03-20T13:09:56Z",
        "mfaAuthenticated": "false"
      },
      "ec2RoleDelivery": "2.0"
    }
  },
  "eventTime": "2026-03-20T18:05:14Z",
  "eventSource": "s3files.amazonaws.com",
  "eventName": "CreateMountTarget",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.0",
  "requestParameters": {
    "fileSystemId": "fs-abcd123456789ef0",
    "subnetId": "subnet-01234567890abcdef",
    "securityGroups": [
      "sg-c16d65b6"
    ]
  },
  "responseElements": {
    "availabilityZoneId": "usw2-az2",
```



```

    "ownerId": "111122223333",
    "mountTargetId": "fsmt-1234567",
    "fileSystemId": "fs-abcd123456789ef0",
    "subnetId": "subnet-01234567890abcdef",
    "ipv4Address": "192.0.2.0",
    "ipv6Address": "2001:db8::1",
    "networkInterfaceId": "eni-0123456789abcdef0",
    "vpcId": "vpc-01234567",
    "securityGroups": [
        "sg-c16d65b6"
    ],
    "status": "creating"
},
"requestID": "dEXAMPLE-feb4-11e6-85f0-736EXAMPLE75",
"eventID": "eEXAMPLE-2d32-4619-bd00-657EXAMPLEe4",
"readOnly": false,
"resources": [
    {
        "accountId": "111122223333",
        "type": "AWS::S3Files::FileSystem",
        "ARN": "arn:aws:s3files:us-west-2:111122223333:file-system/fs-
abcd123456789ef0"
    },
    {
        "accountId": "111122223333",
        "type": "AWS::S3Files::MountTarget",
        "ARN": "arn:aws:s3files:us-west-2:111122223333:mount-target/fsmt-1234567"
    },
    {
        "accountId": "111122223333",
        "type": "AWS::EC2::Subnet",
        "ARN": "arn:aws:ec2:us-west-2:111122223333:subnet/subnet-01234567890abcdef"
    },
    {
        "accountId": "111122223333",
        "type": "AWS::EC2::NetworkInterface",
        "ARN": "arn:aws:ec2:us-west-2:111122223333:network-interface/
eni-0123456789abcdef0"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management",

```

```
"tlsDetails": {  
  "tlsVersion": "TLSv1.3",  
  "cipherSuite": "TLS_AES_128_GCM_SHA256",  
  "clientProvidedHostHeader": "s3files.us-west-2.api.aws"  
}
```

Specifiche prestazionali

S3 Files ridimensiona automaticamente la velocità effettiva e gli IOPS in base al carico di lavoro senza richiedere il provisioning o la gestione della capacità. Questa pagina descrive le caratteristiche prestazionali di S3 Files.

Riepilogo delle prestazioni

Specifiche	Valore
Velocità di lettura aggregata per file system	Fino a terabyte al secondo
Throughput di scrittura aggregato per file system	1—5 GiB/s
Numero massimo di IOPS di lettura per bucket S3 con file S3	Nessun limite (collega più file system allo stesso bucket)
IOPS di scrittura massimi per bucket S3 con file S3	Nessun limite (collega più file system allo stesso bucket)
Numero massimo di IOPS di lettura per file system	250.000
IOPS di scrittura massimo per file system	50.000
Velocità massima di lettura per client	3 GiB/s

In che modo S3 Files offre prestazioni

S3 Files gestisce i dati provenienti da due livelli di storage e indirizza automaticamente ogni operazione al livello più adatto.

High-performance archiviazione: il livello di archiviazione a bassa latenza all'interno del file system in cui risiedono i dati e i metadati dei file utilizzati attivamente. S3 Files gestisce automaticamente questo spazio di archiviazione, copiando i dati su di esso quando si accede ai file e rimuovendo i dati che non sono stati letti entro una finestra di scadenza configurabile. Paghi una tariffa di archiviazione per i dati che risiedono nello storage ad alte prestazioni.

Direttamente da S3: S3 Files trasmette le letture dei file direttamente dal bucket S3 in due casi: quando i dati del file non sono archiviati nella memoria ad alte prestazioni del file system e per letture di grandi dimensioni ≥ 1 MiB, anche quando i dati risiedono anche nello storage ad alte prestazioni del file system. Il bucket S3 è ottimizzato per un throughput elevato mentre il livello di storage ad alte prestazioni del file system è ottimizzato per l'accesso a bassa latenza. Questo approccio a più livelli per lo streaming di dati direttamente dal bucket S3 offre un throughput elevato per le letture sequenziali, rendendolo ideale per analisi, elaborazione multimediale e altri carichi di lavoro di streaming. S3 Files importa in modo asincrono i dati per file di piccole dimensioni (< 128 KiB per impostazione predefinita) nello storage ad alte prestazioni del file system per l'accesso a bassa latenza nelle letture successive.

Poiché S3 Files applica automaticamente questo modello a due livelli, non è necessario scegliere tra latenza e velocità effettiva. Small-file i carichi di lavoro ottengono le prestazioni del file system. Large-file i carichi di lavoro ottengono un throughput S3. I carichi di lavoro misti ottengono entrambi.

Prestazioni di lettura

Il throughput di lettura si ridimensiona in base al numero di istanze di calcolo connesse e al grado di parallelismo all'interno di ciascuna istanza. La velocità massima di lettura per client è 3. GiB/s S3 Files supporta fino a terabyte al secondo di velocità di lettura aggregata e fino a 250.000 IOPS di lettura per file system.

Prestazioni di scrittura

Le scritture vengono trasferite nella memoria ad alte prestazioni e durano immediatamente. A seconda della regione, S3 Files supporta 1-5 GiB/s del throughput di scrittura aggregato e fino a 50.000 IOPS di scrittura per file system. Le prestazioni di scrittura si scalano in modo elastico in base all'attività del carico di lavoro.

Quando modifichi un file nel file system, S3 Files attende circa 60 secondi, aggregando tutte le modifiche successive apportate al file in quel lasso di tempo, prima di copiarlo nel bucket S3. Ciò significa che le scritture rapide e successive sullo stesso file vengono acquisite in una singola

richiesta PUT S3 anziché generare una nuova versione dell'oggetto per ogni singola modifica, riducendo i costi delle richieste S3 e i costi di archiviazione. Se continui a modificare il file dopo che S3 Files ha copiato le modifiche nel bucket S3, le modifiche successive verranno copiate secondo necessità.

Latenza del primo accesso

La prima volta che si accede a una directory, S3 Files importa i metadati per tutti i file in quella directory e, a seconda della configurazione di importazione, i dati per i file di piccole dimensioni. Quindi l'accesso iniziale richiede più tempo rispetto alle operazioni successive. Una volta importati, tutti i successivi elenchi di directory e gli accessi ai file vengono restituiti a bassa latenza.

Prestazioni di sincronizzazione

S3 Files sincronizza le modifiche tra il file system e il bucket S3 in background.

Importazione di modifiche da S3: quando un'altra applicazione aggiunge o modifica un oggetto nel bucket S3, S3 Files riflette la modifica nel file system in genere in pochi secondi. S3 Files elabora fino a 2.400 modifiche agli oggetti al secondo per file system, con una velocità di importazione dei dati fino a 700 megabyte al secondo.

Esportazione delle modifiche in S3: quando si scrive un file tramite il file system, S3 Files raggruppa le modifiche in batch per circa 60 secondi per consolidare le scritture successive rapide in un'unica versione dell'oggetto S3, riducendo i costi delle richieste S3 e della versione di archiviazione. Dopo la finestra di batch, S3 Files copia il file nel bucket S3. S3 Files esporta fino a 800 file al secondo per file system, con una velocità di esportazione dei dati fino a 2.700 megabyte al secondo.

Metrica operativa	Valore	Unità
Importazione da bucket S3 IOPS	2.400	oggetti al secondo per file system
Importazione dal throughput del bucket S3	700	megabyte al secondo
Esportazione in bucket IOPS S3	800	file al secondo per file system
Esportazione verso il throughput del bucket S3	2.700	megabyte al secondo

Amazon S3 utilizza una struttura di storage piatta in cui gli oggetti sono identificati dai loro nomi chiave. Mentre S3 Files consente di organizzare i dati in directory, S3 non ha un concetto nativo di directory. Ciò che appare come una directory nel file system è un prefisso comune condiviso dalle chiavi degli oggetti all'interno del bucket S3. Inoltre, gli oggetti S3 sono immutabili e non supportano le ridenominazioni atomiche. Di conseguenza, quando si rinomina o si sposta un file, S3 Files deve scrivere i dati su un nuovo oggetto con la chiave aggiornata ed eliminare l'originale. Quando si rinomina o si sposta una directory, S3 Files deve ripetere questo processo per ogni oggetto che condivide quel prefisso. Pertanto, quando si rinomina o si sposta una directory contenente decine di milioni di file, i costi delle richieste S3 e il tempo di sincronizzazione aumentano notevolmente. Una ridenominazione di una directory di 100.000 file richiede alcuni minuti per essere inserita completamente nel bucket S3, sebbene la ridenominazione sia istantanea sul file system. Per ulteriori informazioni, consulta [Comprendere l'impatto delle operazioni di ridenominazione e spostamento](#).

Se il carico di lavoro genera modifiche più velocemente della velocità di sincronizzazione, S3 Files mette in coda le modifiche e le elabora in ordine. Puoi monitorare il conteggio delle esportazioni in sospeso utilizzando la metrica `PendingExports` CloudWatch. Per ulteriori informazioni, consulta [Monitoraggio dei file S3 con Amazon CloudWatch](#).

Monitoraggio delle prestazioni

Puoi monitorare le prestazioni del tuo file system utilizzando Amazon CloudWatch. S3 Files pubblica metriche tra cui `DataReadBytes`, `DataWriteBytes`, `MetadataReadBytes` e `MetadataWriteBytes`, che puoi utilizzare per monitorare la velocità effettiva e gli IOPS nel tempo. Per ulteriori informazioni, consulta [Monitoraggio dei file S3 con Amazon CloudWatch](#).

Sicurezza per i file S3

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e te. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

Sicurezza del cloud

AWS è responsabile della protezione dell'infrastruttura che gestisce AWS e i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. Third-party e revisori testano

e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei Programmi di [AWS conformità](#). Per informazioni sui programmi di conformità che si applicano ai file Amazon S3, consulta [AWS Services in Scope by Compliance Program](#).

Sicurezza nel cloud

La tua responsabilità è determinata dal AWS servizio che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon S3 Files.

Protezione dei dati

Il [modello di responsabilità AWS condivisa](#) si applica alla protezione dei dati in S3 Files. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per AWS i servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post [AWS Modello di responsabilità condivisa](#) e GDPRAWS nel blog sulla sicurezza di .

Ai fini della protezione dei dati, ti consigliamo di proteggere le credenziali AWS dell'account e configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.

- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con S3 Files o altri AWS servizi utilizzando la console, l'API, la AWS CLI o gli SDK. AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Argomenti

- [Encryption \(Crittografia\)](#)
- [Come funziona S3 Files con IAM](#)
- [Controlla l'accesso del client a un file system S3 Files](#)
- [Autorizzazioni POSIX nei file S3](#)

Encryption (Crittografia)

S3 Files offre funzionalità di crittografia complete per proteggere i dati sia a riposo sia in transito.

Crittografia dei dati a riposo

Il tuo bucket S3 è crittografato utilizzando i meccanismi di crittografia di Amazon S3. Per informazioni sulla crittografia dei dati in S3, consulta [Protezione](#) dei dati con la crittografia.

S3 Files crittografa i dati inattivi nel file system S3 utilizzando la crittografia lato server. Server-side la crittografia è la crittografia dei dati a destinazione da parte dell'applicazione o del servizio che li riceve. Nei file system S3, i dati e i metadati vengono crittografati per impostazione predefinita prima di essere scritti sullo storage e vengono decrittografati automaticamente durante la lettura. Questi processi sono gestiti in modo trasparente da S3 Files, quindi non è necessario modificare le applicazioni. Tutti i dati archiviati nel file system vengono crittografati utilizzando uno dei seguenti metodi:

- (Impostazione predefinita) Server-side crittografia con chiavi di S3-managed crittografia Amazon (SSE-S3)

- Server-side crittografia con AWS Key Management Service (SSE-KMS)

Sono previsti costi aggiuntivi per l'utilizzo delle chiavi AWS KMS. Per ulteriori informazioni, consulta i [concetti chiave di AWS KMS](#) nella AWS Key Management Service Developer Guide e i prezzi di [AWS KMS](#).

Server-side crittografia con chiavi di S3-managed crittografia Amazon (SSE-S3)

Questo è il metodo predefinito per crittografare i dati inattivi nel file system S3. Le chiavi di S3-managed crittografia Amazon sono una raccolta di chiavi di proprietà e gestione di Amazon S3. S3 Files possiede e gestisce la crittografia dei dati e dei metadati archiviati nel file system S3 quando utilizzi una chiave di crittografia Amazon S3-managed . Per ulteriori informazioni sulle chiavi di S3-managed crittografia Amazon, consulta [Protezione dei dati con le chiavi gestite di Amazon S3](#).

Server-side crittografia con AWS Servizio di gestione delle chiavi (SSE-KMS)

Durante la creazione del file system, è possibile scegliere di configurare una AWS chiave del servizio di gestione delle chiavi (AWS KMS) da gestire. Quando utilizzi SSE-KMS la crittografia con un file system S3, le chiavi AWS KMS devono trovarsi nella stessa regione del file system.

Le politiche chiave di S3 Files per AWS KMS

Le policy delle chiavi sono il modo principale per controllare l'accesso alle chiavi gestite dai clienti. Per ulteriori informazioni sulle politiche chiave, consulta le [politiche chiave in AWS KMS nella AWS Key Management Service Developer Guide](#). L'elenco seguente descrive tutte le autorizzazioni AWS relative a KMS supportate da S3 Files per la crittografia dei file system inattivi:

kms:Encrypt

(Facoltativo) Crittografa il testo semplice in testo cifrato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

kms:Decrypt

(Obbligatorio) Decifra il testo cifrato. Il testo cifrato è un testo normale che è stato precedentemente crittografato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

kms:ReEncrypt

(Facoltativo) Crittografa i dati sul lato server con una nuova chiave gestita dal cliente, senza esporre il testo in chiaro dei dati sul lato client. I dati sono prima decifrati e quindi nuovamente crittografati. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

kms:GenerateDataKeyWithoutPlaintext

(Obbligatorio) Restituisce una chiave di crittografia dei dati crittografata con una chiave gestita dal cliente. Questa autorizzazione è inclusa nella politica delle chiavi predefinita in kms:GenerateDataKey *.

kms:CreateGrant

(Obbligatorio) Aggiunge una concessione a una chiave per specificare chi può utilizzare la chiave e in quali condizioni. I grant sono meccanismi di autorizzazioni alternative alle policy sulle chiavi. Per ulteriori informazioni sulle sovvenzioni, consulta [Grants in AWS KMS nella AWS Key Management Service Developer Guide](#). Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

kms:DescribeKey

(Obbligatorio) Fornisce informazioni dettagliate sulla chiave gestita dal cliente specificata. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

kms:ListAliases

(Facoltativo) Elenca tutti gli alias chiave dell'account. Quando si utilizza la console per creare un file system crittografato, questa autorizzazione popola l'elenco Seleziona chiave KMS. Consigliamo di usare questa autorizzazione per garantire la migliore esperienza utente. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

Stati chiave e relativi effetti

Lo stato della chiave KMS influisce direttamente sull'accesso al file system crittografato:

Abilitato

Funzionamento normale: accesso completo in lettura e scrittura al file system.

Disabilitato

Il file system diventa inaccessibile dopo qualche tempo. Può essere riattivato.

In attesa di eliminazione

Il file system diventa inaccessibile. L'eliminazione può essere annullata durante il periodo di attesa. Nota che dopo aver annullato l'eliminazione della chiave, la chiave deve essere spostata nello stato abilitato.

Eliminato

File system permanentemente inaccessibile. Questa azione non può essere annullata.

Warning

Se disabiliti o elimini la chiave KMS utilizzata per il tuo file system o revochi l'accesso di S3 Files alla chiave, il file system diventerà inaccessibile. Ciò può causare la perdita di dati se non si dispone di backup. Assicurati sempre di disporre di procedure di backup adeguate prima di apportare modifiche alle chiavi di crittografia.

Crittografia dei dati in transito

S3 Files richiede la crittografia dei dati in transito utilizzando Transport Layer Security (TLS). Quando monti il file system utilizzando il mount helper, tutti i dati che viaggiano tra il client e il file system vengono crittografati tramite TLS. Il mount helper inizializza il processo efs-proxy per stabilire una connessione TLS sicura con il file system. Il mount helper crea anche un processo chiamato amazon-efs-mount-watchdog che monitora lo stato dei mount e viene avviato automaticamente la prima volta che viene montato un file system S3. Garantisce che il processo efs-proxy di ogni mount sia in esecuzione e arresta il processo quando il file system viene smontato. Se per qualche motivo il processo viene interrotto in modo imprevisto, il processo watchdog lo riavvia.

Di seguito viene descritto come funziona la crittografia TLS in transito:

1. Viene stabilita una connessione TLS sicura tra il client e il file system
2. Tutto il traffico NFS viene instradato attraverso questa connessione crittografata
3. I dati vengono crittografati prima della trasmissione e decrittografati al momento della ricezione

La crittografia dei dati in transito modifica la configurazione del client NFS. Quando si ispezionano i tuoi file system montati, se ne vede uno montato all'indirizzo 127.0.0.1 o localhost, come nell'esempio seguente.

```
$ mount | column -t
127.0.0.1:/ on /home/ec2-user/s3files          type nfs4
(rw,relatime,vers=4.1,rsize=1048576,wsiz=1048576,namlen=255,hard,proto=tcp,port=20127,timeo=6
```

Il file system viene montato utilizzando il mount helper, che crittografa sempre i dati in transito utilizzando TLS. Pertanto, durante il montaggio, il client NFS viene riconfigurato per il montaggio su una porta locale.

Come funziona S3 Files con IAM

Questa pagina descrive come funziona AWS Identity and Access Management (IAM) con S3 Files e come è possibile utilizzare le policy IAM per controllare l'accesso ai file system.

S3 Files utilizza IAM per due tipi distinti di controllo degli accessi:

- **Accesso API:** controlla chi può creare, gestire ed eliminare risorse di S3 Files come file system, destinazioni di montaggio e punti di accesso. Puoi controllare questo accesso utilizzando politiche basate sull'identità associate a utenti, gruppi o ruoli IAM.
- **Accesso client:** controlla ciò che i client (le risorse di calcolo montate) possono fare con il file system una volta connessi, ad esempio leggere, scrivere o accedere ai file come utente root. Puoi controllare questo accesso utilizzando una combinazione di politiche basate sulle risorse, politiche basate sull'identità, punti di accesso e autorizzazioni POSIX.

Utilizzando IAM, è possibile consentire ai client di eseguire operazioni specifiche su un file system, incluso l'accesso di sola lettura, scrittura e root. Un'autorizzazione «consenti» per un'azione o in una policy di identità IAM o in una policy di risorse del file system consente l'accesso a tale azione. L'autorizzazione non deve essere concessa sia in una policy di identità sia in una policy delle risorse.

Le politiche del bucket S3 sul bucket S3 collegato regolano anche l'accesso dalla risorsa di elaborazione e dal file system al bucket S3. È inoltre necessario assicurarsi che le politiche del bucket di origine non neghino l'accesso alla risorsa di elaborazione o al file system. Per maggiori dettagli, consulta le politiche dei [bucket per Amazon S3](#).

Identity-based politiche

Identity-based le policy sono policy JSON da allegare a utenti, gruppi o ruoli IAM. Puoi fornire queste autorizzazioni scrivendo policy personalizzate o allegando una AWS policy gestita. Per ulteriori informazioni sulle politiche gestite disponibili sia per l'accesso alle API che per l'accesso dei client, consulta le politiche [AWS gestite per Amazon S3 Files](#).

S3 Files ottimizza anche le prestazioni di lettura consentendo ai client di leggere i dati dei file direttamente dal bucket S3 di origine. Quando si monta un file system S3 sulla risorsa di calcolo, è necessario aggiungere una policy in linea al ruolo IAM della risorsa di calcolo che conceda le autorizzazioni per leggere gli oggetti dal bucket S3 specificato. L'helper di montaggio utilizza queste autorizzazioni per leggere i dati S3. Per maggiori dettagli su questa politica, consulta. [Ruolo IAM per collegare il tuo file system a AWS risorse di calcolo](#)

Resource-based politiche

Una policy del file system è una policy basata sulle risorse IAM che si allega direttamente a un file system per controllare l'accesso dei client. È possibile utilizzare le politiche del file system per concedere o negare ai client le autorizzazioni per eseguire operazioni come il montaggio, la scrittura e l'accesso root.

Un file system ha una politica del file system vuota (predefinita) o esattamente una politica esplicita. Le policy del file system S3 hanno un limite di 20.000 caratteri. Per informazioni sulla creazione e la gestione delle politiche del file system, vedere. [Creazione di policy del file system](#)

Azioni relative ai file S3 per i client

È possibile specificare le seguenti azioni in una politica del file system per controllare l'accesso dei client:

Azione	Description
s3files:ClientMount	Fornisce un accesso in sola lettura a un file system.
s3files:ClientWrite	Fornisce le autorizzazioni di scrittura su un file system.
s3files:ClientRoot Access	Fornisce la possibilità di utilizzare l'utente root quando si accede a un file system.

Chiavi di condizione dei file S3 per i client

È possibile utilizzare le seguenti chiavi di condizione nell'Conditionelemento di una politica del file system per perfezionare ulteriormente il controllo degli accessi:

Chiave di condizione	Description	Operatore
s3files:AccessPointArn	ARN del punto di accesso S3 Files a cui il client si sta connettendo.	Stringa

Esempi di policy del file system

Esempio: concedere accesso in sola lettura

La seguente politica del file system concede solo autorizzazioni ClientMount (di sola lettura) al ruolo IAM. ReadOnly Sostituisci **111122223333** con l'ID del tuo account. AWS

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ReadOnly"
      },
      "Action": [
        "s3files:ClientMount"
      ]
    }
  ]
}
```

Esempio: concedere l'accesso a un punto di accesso S3 Files

La seguente politica del file system utilizza un elemento condizionale per concedere a un punto di accesso specifico l'accesso completo al file system durante il montaggio tramite il punto di accesso specificato. Sostituisci l'ARN del punto di accesso e l'ID dell'account con i tuoi valori. Per ulteriori informazioni, consulta [Creazione di punti di accesso per un file system S3](#).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::555555555555:role/S3FilesAccessPointFullAccess"
      },

```

```
    "Action": [
      "s3files:Client*"
    ],
    "Condition": {
      "StringEquals": {
        "s3files:AccessPointArn": "arn:partition:s3files:region:account-id:file-system/fs-1234567890/access-point/fsap-0987654321"
      }
    }
  }
]
```

Autorizzazioni POSIX

Dopo il successo dell'autorizzazione IAM, S3 Files applica le autorizzazioni POSIX (Unix-style) standard a livello di file e directory. Le autorizzazioni POSIX controllano l'accesso in base all'ID utente (UID), all'ID di gruppo (GID) e ai bit di autorizzazione (lettura, scrittura, esecuzione) associati a ciascun file e directory. I punti di accesso possono imporre un'identità utente POSIX specifica per tutte le richieste, semplificando la gestione degli accessi per i set di dati condivisi. Per ulteriori informazioni, consulta [Creazione di punti di accesso per un file system S3](#).

Gruppi di sicurezza

I gruppi di sicurezza agiscono come un firewall a livello di rete che controlla il traffico tra le risorse di calcolo e le destinazioni di montaggio del file system. Per dettagli sulla configurazione dei gruppi di sicurezza per iniziare a usare S3 Files, consulta [Gruppi di sicurezza](#).

AWS policy gestite per i file Amazon S3

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. Le policy gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché sono disponibili per tutti i clienti. AWS si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS. Se AWS aggiorna le autorizzazioni definite in una policy AWS gestita, l'aggiornamento ha effetto su tutte le identità

principali (utenti, gruppi e ruoli) a cui la policy è associata. AWS è più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AmazonS3FilesFullAccess

È possibile allegare la policy AmazonS3FilesFullAccess alle identità IAM. Questa policy garantisce l'accesso completo ai file Amazon S3, comprese le autorizzazioni per creare e gestire file system, obiettivi di montaggio e punti di accesso. Per ulteriori informazioni su questa policy, consulta il AWS Managed Policy [AmazonS3FilesFullAccess](#) Reference.

AWS politica gestita: AmazonS3FilesReadOnlyAccess

È possibile allegare la policy AmazonS3FilesReadOnlyAccess alle identità IAM. Questa policy garantisce l'accesso in sola lettura ai file Amazon S3, incluse le autorizzazioni per visualizzare i file system, le destinazioni di montaggio, i punti di accesso e le relative configurazioni. Per ulteriori informazioni su questa policy, consulta il Managed Policy Reference [AmazonS3FilesReadOnlyAccess](#). AWS

AWS politica gestita: AmazonS3FilesClientFullAccess

È possibile allegare la policy AmazonS3FilesClientFullAccess alle identità IAM. Questa policy garantisce l'accesso completo del client ai file system S3 Files, inclusa la possibilità di montare, leggere, scrivere e accedere ai file come utente root. Per ulteriori informazioni su questa policy, consulta [AmazonS3FilesClientFullAccess](#) il AWS Managed Policy Reference.

AWS politica gestita: AmazonS3FilesClientReadWriteAccess

È possibile allegare la policy AmazonS3FilesClientReadWriteAccess alle identità IAM. Questa policy garantisce ai client l'accesso in lettura e scrittura ai file system S3 Files, inclusa la possibilità di montare, leggere e scrivere. Questa policy non garantisce l'accesso root. Per ulteriori informazioni su questa politica, consulta [AmazonS3FilesClientReadWriteAccess](#) il AWS Managed Policy Reference.

AWS politica gestita: AmazonS3FilesClientReadOnlyAccess

È possibile allegare la policy AmazonS3FilesClientReadOnlyAccess alle identità IAM. Questa policy garantisce al client l'accesso in sola lettura ai file system S3 Files, inclusa la possibilità di montare e leggere dal file system. Per ulteriori informazioni su questa policy, consulta il Managed Policy [AmazonS3FilesClientReadOnlyAccess](#) Reference. AWS

AWS politica gestita: AmazonS3FilesCSIDriverPolicy

È possibile allegare la policy AmazonS3FilesCSIDriverPolicy alle identità IAM. Questa policy concede le autorizzazioni al driver Amazon EFS Container Storage Interface (CSI) per gestire i punti di accesso S3 Files per conto dei cluster Amazon EKS. Per ulteriori informazioni su questa policy, consulta [AmazonS3FilesCSIDriverPolicy](#) il Managed Policy Reference. AWS

AWS politica gestita: AmazonElasticFileSystemsUtils

È possibile allegare la policy AmazonElasticFileSystemsUtils alle identità IAM. Questa policy concede le autorizzazioni alle utilità client S3 Files (amazon-efs-utils) per eseguire operazioni come la descrizione delle destinazioni di montaggio, la pubblicazione CloudWatch di metriche e log e la comunicazione con Systems Manager. AWS Per ulteriori informazioni su questa politica, consulta il Managed Policy Reference. [AmazonElasticFileSystemsUtils](#) AWS

Aggiornamenti di Amazon S3 Files a AWS policy gestite

Visualizza i dettagli sugli aggiornamenti delle policy AWS gestite per Amazon S3 Files da quando S3 Files ha iniziato a tracciare queste modifiche.

Modifica	Descrizione	Data
AmazonElasticFileSystemsUtils — Aggiornato	Sono state aggiunte CloudWatch PutMetricData le autorizzazioni Amazon per supportare la pubblicazione delle metriche di connettività dei client.	7 aprile 2026
AmazonS3FilesCSIDriverPolicy — Aggiunto	Nuova policy gestita che concede le autorizzazioni al driver CSI di Amazon EFS per gestire i punti di accesso S3 Files per conto dei cluster Amazon EKS.	7 aprile 2026
AmazonS3FilesClientReadOnlyAccess — Aggiunto	Nuova policy gestita che garantisce ai client l'accesso	7 aprile 2026

Modifica	Descrizione	Data
	in sola lettura ai file system S3 Files.	
AmazonS3FilesClientReadWriteAccess — Aggiunto	Nuova politica gestita che concede ai client l'accesso in lettura e scrittura ai file system S3 Files.	7 aprile 2026
AmazonS3FilesClientFullAccess — Aggiunto	Nuova politica gestita che garantisce l'accesso completo del cliente ai file system S3 Files, incluso l'accesso root.	7 aprile 2026
AmazonS3FilesReadOnlyAccess — Aggiunto	Nuova politica gestita che garantisce l'accesso in sola lettura alle risorse di S3 Files.	7 aprile 2026
AmazonS3FilesFullAccess — Aggiunto	Nuova politica gestita che garantisce l'accesso completo alle risorse di S3 Files.	7 aprile 2026
S3 Files ha iniziato a tenere traccia delle modifiche	Amazon S3 Files ha iniziato a tracciare le modifiche relative alle politiche AWS gestite.	7 aprile 2026

Controlla l'accesso del client a un file system S3 Files

Questo argomento descrive come utilizzare le policy del file system, le policy di identità IAM e i controlli di rete per controllare quali client possono accedere al file system S3 Files e attraverso quali punti di accesso.

Punti di accesso ai file S3

I punti di accesso S3 Files sono punti di accesso specifici dell'applicazione a un file system che semplificano la gestione dell'accesso ai dati su larga scala. È possibile utilizzare i punti di accesso per applicare le identità e le autorizzazioni degli utenti per tutte le richieste di file system effettuate

tramite il punto di accesso e limitare i client all'accesso solo ai dati all'interno di una directory principale specificata e delle relative sottodirectory.

I punti di accesso definiscono ciò che un client può fare sul file system. Non stabiliscono quali client possono utilizzarli. Qualsiasi ruolo dell'account con `s3files:ClientMount` autorizzazione può essere installato tramite qualsiasi punto di accesso sul file system, a meno che una politica del file system non lo limiti. Per controllare quali client possono utilizzare un determinato punto di accesso, combina tre livelli: controlli di rete (impedimento della connessione), una politica delle risorse del file system (negazione esplicita che sopravvive alle modifiche della politica di identità) e una politica di identità IAM (privilegio minimo sul ruolo).

S3 Files valuta e `s3files:ClientRootAccess` confronta la `s3files:ClientMount` politica `s3files:ClientWrite` del file system su ogni installazione. La chiave di `s3files:AccessPointArn` condizione viene inoltre valutata ad ogni installazione, quindi puoi scrivere un'unica dichiarazione di negazione che blocchi l'accesso tramite qualsiasi punto di accesso tranne quello specificato. Se un'azione richiesta viene negata o non concessa, il montaggio fallisce prima che si verifichino le operazioni sui file. Le due sezioni seguenti trattano i due requisiti più comuni: limitare un carico di lavoro a un punto di accesso specifico e negare del tutto l'accesso di un carico di lavoro al file system.

Limita l'accesso a un punto di accesso specifico

Questo modello si applica quando un ruolo (ad esempio, un ruolo di istanza EC2 o un ruolo di attività ECS) deve montare il file system tramite un solo punto di accesso. La chiave della condizione è `s3files:AccessPointArn`. La policy richiede sia un punto di accesso `Allow` per il punto di accesso previsto che uno esplicito `Deny` per ogni altro punto di accesso. Le concessioni di autorizzazione IAM si sommano a tutte le policy relative alle identità e alle risorse; senza una negazione esplicita, una policy separata può concedere l'accesso a un punto di accesso diverso.

Esempio di politica del file system:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowComputeAOnlyViaSpecificAP",
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::ACCOUNT:role/compute-a-role" },
      "Action": [
        "s3files:ClientMount",
```

```

        "s3files:ClientWrite"
    ],
    "Condition": {
        "StringEquals": {
            "s3files:AccessPointArn": "arn:aws:s3files:REGION:ACCOUNT:file-system/fs-ID/
access-point/fsap-ID"
        }
    }
},
{
    "Sid": "DenyComputeAIfWrongAP",
    "Effect": "Deny",
    "Principal": { "AWS": "arn:aws:iam::ACCOUNT:role/compute-a-role" },
    "Action": "s3files:Client*",
    "Condition": {
        "StringNotEquals": {
            "s3files:AccessPointArn": "arn:aws:s3files:REGION:ACCOUNT:file-system/fs-ID/
access-point/fsap-ID"
        }
    }
}
]
}

```

Il ruolo può essere montato e scritto solo quando la richiesta `compute-a-role` è `fsap-ID` indirizzata ed è esplicitamente negato su ogni altro punto di accesso su questo file system. Una negazione esplicita in una policy relativa alle risorse non può essere sostituita dalle policy di identità, quindi questa restrizione vale anche se in un secondo momento al ruolo viene associata una policy IAM più ampia.

Comando di montaggio:

```
sudo mount -t s3files -o accesspoint=fsap-ID fs-ID:/ /mnt/s3files
```

Negare l'accesso a un carico di lavoro tramite qualsiasi punto di accesso

Questo modello si applica quando un ruolo condivide un account con un file system S3 Files ma non deve montarlo tramite alcun punto di accesso o direttamente. Per bloccare l'utilizzo di tutti i punti di accesso, applica tre livelli, ordinati dalla garanzia di isolamento più forte a quella più debole.

1. Controlli di rete. Rimuovi la regola del gruppo di sicurezza che concede `compute-b-role` alle istanze l'accesso alla destinazione di montaggio sulla porta TCP 2049. I controlli di rete sono il

livello più resiliente perché impediscono il tentativo di montaggio prima che avvenga lo scambio di credenziali. Anche se una policy configurata in modo errato concede i permessi di montaggio, la connessione NFS non può raggiungere l'obiettivo di montaggio.

2. Negazione esplicita nella politica del file system. Un'istruzione di negazione nella policy del file system rifiuta il montaggio anche se al ruolo vengono concesse in un secondo momento autorizzazioni IAM più ampie. Una policy relativa alle risorse del file system prevede una negazione che persiste anche se qualcuno `iam:PutRolePolicy` modifica le politiche di identità del ruolo. Solo i responsabili con `s3files:PutFileSystemPolicy` possono modificare questo livello.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyComputeBOnFileSystem",
      "Effect": "Deny",
      "Principal": { "AWS": "arn:aws:iam::ACCOUNT:role/compute-b-role" },
      "Action": "s3files:Client*",
      "Resource": "*"
    }
  ]
}
```

3. Politica di identità IAM. Non concedere `s3files:Client*` autorizzazioni al ruolo. Questo è l'ultimo livello e il più facile da configurare erroneamente, poiché qualsiasi amministratore `iam:PutRolePolicy` può concedere le autorizzazioni di montaggio a un ruolo.

Senza una politica del file system, qualsiasi ruolo può essere installato tramite qualsiasi punto di accesso

Una politica delle risorse del file system prevede una negazione che non può essere rimossa da qualcuno che ha solo l'autorizzazione a modificare le politiche di identità. Senza una politica del file system, qualsiasi ruolo incluso `s3files:ClientMount` nella politica di identità può essere installato tramite qualsiasi punto di accesso sul file system. Si consiglia di allegare una politica del file system a ogni file system con una linea di base di negazione, quindi aggiungere le istruzioni di autorizzazione per carico di lavoro.

Le migliori pratiche per l'isolamento dei punti di accesso

La tabella seguente riassume gli approcci consigliati per gli obiettivi comuni di isolamento dei punti di accesso.

Obiettivo	Approccio consigliato
Limita un carico di lavoro a un singolo punto di accesso	Consenti il ruolo sull'ARN del punto di accesso specifico, oltre a una negazione esplicita su ogni altro punto di accesso. Vedi «Limita l'accesso a un punto di accesso specifico».
Impedisci a un ruolo nello stesso account di montare il file system	Rimuovi l'accesso di rete alla porta 2049, nega la politica del file system e non concedetelo in IAM.
Carichi di lavoro multipli sullo stesso file system, ciascuno associato al proprio punto di accesso	Mantieni una coppia allow+deny per ruolo nella policy del file system, ciascuna con ambito ARN di un punto di accesso diverso.
Cross-account accesso tramite un punto di accesso	Utilizza la policy del file system per concedere il ruolo tra account diversi sull'ARN del punto di accesso specifico. Non fate affidamento solo sulle politiche di identità.

Autorizzazioni POSIX nei file S3

I file system POSIX richiedono proprietà e autorizzazioni su ogni file. Amazon S3 archivia i dati come oggetti con accesso controllato da policy IAM e bucket policy e non archivia nativamente la proprietà o gli attributi di autorizzazione dei file. S3 Files colma questa differenza archiviando i metadati POSIX, inclusi i permessi del proprietario, del gruppo e dei file, come metadati definiti dall'utente su ogni oggetto S3. Quando crei o modifichi un file tramite S3 Files, il servizio scrive automaticamente tutti i metadati delle autorizzazioni. Quando un oggetto viene scritto nel bucket S3 all'esterno del file system, ad esempio tramite la console Amazon S3, la AWS CLI AWS o l'SDK, non esistono metadati POSIX su quell'oggetto. S3 Files assegna a tali oggetti un valore predefinito di `root:root` proprietà e 644 autorizzazioni, che consente agli utenti non root di leggere il file ma non di scrivervi. Se queste impostazioni predefinite soddisfano i requisiti di accesso, non è richiesta alcuna azione. Se l'applicazione lo richiede, è possibile sovrascrivere le autorizzazioni predefinite su tali oggetti. Questo tutorial illustra come applicare le autorizzazioni personalizzate.

In che modo S3 Files archivia i metadati POSIX

S3 Files memorizza le informazioni POSIX come metadati definiti dall'utente su ciascun oggetto. Le seguenti chiavi di metadati controllano la proprietà e le autorizzazioni:

Chiave per i metadati	Description	Valore di esempio
x-amz-meta-file-owner	ID utente POSIX (UID)	1000
x-amz-meta-file-group	ID di gruppo POSIX (GID)	1000
x-amz-meta-file-permissions	Tipo di file e bit di autorizzazione (ottali)	0100644

Quando un oggetto non ha metadati POSIX, S3 Files applica le seguenti impostazioni predefinite:

- File: **root:root** proprietà con autorizzazioni () 0644 -rw-r--r--
- Elenchi: **root:root** proprietà con 0755 autorizzazioni () drwxr-xr-x

In base a queste impostazioni predefinite, tutti gli utenti possono leggere i file e navigare tra le directory, ma solo il proprietario (root) può scrivere. Per impostazione predefinita, i file non sono eseguibili.

Impostazione dei metadati POSIX su oggetti esistenti

Utilizzate la seguente procedura per applicare la proprietà e le autorizzazioni POSIX agli oggetti già esistenti nel bucket.

Passaggio 1: Identifica l'UID e il GID dell'utente di destinazione

Per questo esempio, l'utente di destinazione è `ec2-user` con UID 1000:

```
$ id ec2-user
uid=1000(ec2-user) gid=1000(ec2-user) groups=1000(ec2-user)
```

Fase 2: Aggiornare i metadati degli oggetti utilizzando copy-object

Il `aws s3api copy-object` comando copia l'oggetto al suo posto con i metadati aggiornati. Sostituisci **BUCKET_NAME** e **OBJECT_KEY** con i tuoi valori.

L'`--metadata-directive REPLACE` opzione sostituisce tutti i metadati definiti dall'utente sull'oggetto. Include `--content-type` per preservare il tipo di contenuto dell'oggetto, perché lo `REPLACE` reimposta al valore predefinito (`binary/octet-stream`). Se utilizzate altri campi di metadati, includeteli nel `--metadata` parametro.

```
aws s3api copy-object \
  --bucket BUCKET_NAME \
  --key OBJECT_KEY \
  --copy-source BUCKET_NAME/OBJECT_KEY \
  --metadata-directive REPLACE \
  --content-type CONTENT_TYPE \
  --metadata '{"file-owner":"1000", "file-group":"1000", "file-
permissions":"0100644"}
```

Fase 3: Verifica che i metadati siano stati applicati

Esegui il comando seguente per confermare i metadati:

```
aws s3api head-object --bucket BUCKET_NAME --key OBJECT_KEY
```

La risposta include i metadati POSIX:

```
{
  "AcceptRanges": "bytes",
  "LastModified": "Mon, 18 May 2026 14:43:00 GMT",
  "ContentLength": 7214,
  "ETag": "\"abc123...\"",
  "ContentType": "image/png",
  "Metadata": {
    "file-owner": "1000",
    "file-group": "1000",
    "file-permissions": "0100644"
  }
}
```

Passaggio 4: verifica le autorizzazioni sul file system S3

```
$ ls -ltr /mnt/s3files/  
-rw-r--r--. 1 ec2-user ec2-user 7214 May 18 14:43 s3.png
```

Il file è ora di proprietà di `ec2-user` e non richiede più l'accesso come `root`.

Impostazione dei metadati POSIX sui nuovi caricamenti

Puoi includere i metadati POSIX quando carichi oggetti nel tuo bucket.

Usare `aws s3 cp`

```
aws s3 cp localfile.txt s3://BUCKET_NAME/localfile.txt \  
  --metadata '{"file-owner":"1000", "file-group":"1000", "file-  
permissions":"0100644"}'
```

Usare `aws s3api put-object`

```
aws s3api put-object \  
  --bucket BUCKET_NAME \  
  --key localfile.txt \  
  --body localfile.txt \  
  --metadata '{"file-owner":"1000", "file-group":"1000", "file-  
permissions":"0100644"}'
```

Verifica i metadati sull'oggetto caricato

```
aws s3api head-object --bucket BUCKET_NAME --key localfile.txt
```

Riferimento ai valori di autorizzazione

La tabella seguente elenca i valori di autorizzazione POSIX comuni e i relativi casi d'uso.

Valore ottale	Modalità file	Caso d'uso
0100644	-rw-r--r--	File standard: proprietario read/write, altri di sola lettura
0100664	-rw-rw-r--	File condiviso: proprietario e gruppo read/write, altri di sola lettura

Valore ottale	Modalità file	Caso d'uso
0100755	-rwxr-xr-x	Eseguibile: accesso completo del proprietario, altri leggono ed eseguono
0100666	-rw-rw-rw-	World-writable file: tutti gli utenti possono leggere e scrivere
0040755	drwxr-xr-x	Cartella standard: accesso completo del proprietario, altri leggono e navigano

Best practice

Carica i file tramite il file system S3 ogni volta che è possibile. S3 Files archivia automaticamente la proprietà e le autorizzazioni del file come metadati degli oggetti, quindi non sono necessari passaggi aggiuntivi. Quando carichi direttamente nel bucket S3, includi i metadati POSIX nel comando upload per garantire che la proprietà e le autorizzazioni corrette siano impostate fin dall'inizio.

Come vengono misurati i file S3

S3 Files è un file system condiviso collegato al bucket S3, progettato per fornire un accesso ai file a bassa latenza mantenendo i costi proporzionali al set di lavoro attivo. Il file system mantiene una visualizzazione degli oggetti nel bucket e traduce in modo intelligente le operazioni del file system in richieste S3 efficienti per conto dell'utente. Quando lavorate con file e directory specifici attraverso il file system, i metadati e i contenuti dei file associati vengono inseriti nello storage ad alte prestazioni del file system, in particolare nelle porzioni che beneficiano dell'accesso a bassa latenza. Molte operazioni di lettura ignorano completamente il file system, con dati forniti direttamente dal bucket S3 alle frequenze di richiesta S3 GET senza costi per i dati dei file S3. I tuoi dati autorevoli rimangono sempre nel tuo bucket S3. Quando scrivi i dati, questi vengono archiviati nello storage ad alte prestazioni e duraturo del file system e quindi sincronizzati nuovamente con il bucket S3, mantenendo il file system e il bucket S3 coerenti in entrambe le direzioni.

Con S3 Files, paghi un costo di archiviazione per la frazione di dati attivi sullo storage ad alte prestazioni del file system e paghi i costi di accesso ai dati per la lettura e la scrittura sullo storage ad alte prestazioni del file system. Questa pagina spiega come viene misurata ogni dimensione in modo da poter comprendere e ottimizzare i costi. Per i prezzi per AWS regione, consulta i prezzi di [Amazon S3](#).

Come viene misurato lo storage del file system

Quando si accede ai dati, il file system carica porzioni di metadati e contenuti dei file su richiesta sullo storage ad alte prestazioni del file system, garantendo letture rapide senza duplicare l'intero set di dati. Si configura una soglia di dimensione del file (impostazione predefinita 128 KB) che determina quali file vengono archiviati su uno storage ad alte prestazioni. I file con o al di sotto di questa soglia traggono i maggiori vantaggi dall'accesso a bassa latenza. I file che superano la soglia vengono trasmessi in streaming direttamente dal bucket S3 e non comportano costi di archiviazione S3 Files. I dati a cui non si accede entro una finestra configurabile (da 1 a 365 giorni, impostazione predefinita 30 giorni) scadono automaticamente dallo storage ad alte prestazioni. Paghi una tariffa di archiviazione per la frazione di dati attivi che risiede nello storage ad alte prestazioni. In genere, la frazione è piccola, poiché i file di grandi dimensioni vengono trasmessi direttamente dal bucket S3, i dati obsoleti scadono automaticamente e solo i file di piccole dimensioni e sensibili alla latenza vengono archiviati su uno storage ad alte prestazioni. La dimensione minima fatturabile del file nello storage ad alte prestazioni è di 10 KiB.

Come viene misurato l'accesso ai dati

Paghi i costi di accesso ai dati per le operazioni sui metadati e per le operazioni di lettura e scrittura sullo storage ad alte prestazioni del file system. Le letture di file di grandi dimensioni (IO di file pari o superiori a 1 MiB) vengono sempre trasmesse in streaming direttamente dal bucket S3, anche se i dati risiedono nello storage ad alte prestazioni del file system. S3 è ottimizzato per letture ad alto throughput, mentre lo storage ad alte prestazioni è ottimizzato per l'accesso a file di piccole dimensioni a bassa latenza. Le letture dirette prevedono richieste S3 GET e una lettura dei metadati di S3 Files (4 KiB) senza costi di lettura dei file. Le operazioni di sincronizzazione in background comportano anche costi di accesso ai dati e costi di richiesta S3. L'importazione di dati su uno storage ad alte prestazioni comporta costi di scrittura, mentre l'esportazione delle modifiche nel bucket S3 comporta costi di lettura.

Come viene misurato l'accesso ai dati dal file system

S3 Files misura ogni operazione del file system come lettura o scrittura e si applica a un file o ai metadati. Ogni operazione ha una dimensione minima misurata e viene quindi arrotondata al successivo incremento di 1 KiB. Ciò significa che ogni operazione rientra in una o due delle quattro categorie: lettura di dati, lettura di metadati, scrittura di dati o scrittura di metadati. Ad esempio, la lettura di un file viene misurata sia come lettura dei dati che come lettura dei metadati, mentre la ridenominazione di un file viene misurata come lettura dei metadati e come scrittura dei metadati. Nessuna singola operazione viene mai misurata come più di due categorie.

Le letture dei file dallo storage ad alte prestazioni vengono misurate in base alla dimensione dei dati letti, con un minimo di 32 KB per operazione di lettura.

Le scritture di file su storage ad alte prestazioni vengono misurate in base alla dimensione dei dati scritti, con un minimo di 32 KB per operazione di scrittura.

Le letture dei metadati vengono misurate con una dimensione minima di 4 KB e si applicano alle letture di S3 Files. Gli esempi di operazioni di lettura dei metadati includono l'elenco di una directory e la visualizzazione degli attributi dei file.

Le scritture dei metadati vengono misurate con una dimensione minima di 4 KB e si applicano alla scrittura di S3 Files. Gli esempi di operazioni di scrittura dei metadati includono la creazione o l'eliminazione di file e directory, la ridenominazione, la modifica delle autorizzazioni e le chiamate. `fsync`

Come viene misurato lo streaming diretto dal tuo bucket S3

S3 Files trasmette le letture direttamente dal tuo bucket S3 in due casi: i dati del file non vengono archiviati su uno storage ad alte prestazioni oppure la lettura è pari o superiore a 1 MiB, anche se i dati risiedono anche su uno storage ad alte prestazioni. Questo design riflette i punti di forza di ogni livello di storage. Il bucket S3 è ottimizzato per un throughput elevato, mentre il file system è ottimizzato per l'accesso a bassa latenza.

Per i file di piccole dimensioni (meno di 128 KB per impostazione predefinita), S3 Files importa i dati in modo asincrono su uno storage ad alte prestazioni in modo che le letture successive vengano eseguite a bassa latenza. Per i bucket stream diretti, paghi per le richieste S3 GET e per la lettura dei metadati di S3 Files (4 KiB), senza costi di lettura dei file.

Come viene misurata la sincronizzazione dei bucket

S3 Files mantiene automaticamente sincronizzati il file system e il bucket S3 collegato. La sincronizzazione viene misurata in base ai costi di lettura e scrittura dei file e alle richieste S3. Per ulteriori informazioni, consulta [Comprendere come funziona la sincronizzazione](#).

Importazione di dati sul file system: quando S3 copia i dati dal bucket S3 su uno storage ad alte prestazioni in base alle impostazioni, l'operazione viene misurata come scrittura del file system. Le scritture di importazione avvengono quando accedi a una directory per la prima volta, quando leggi un file non archiviato su uno storage ad alte prestazioni e quando S3 Files riflette le modifiche apportate direttamente al tuo bucket S3. La dimensione misurata è la quantità di dati scritti su uno storage ad alte prestazioni e in una scrittura di metadati.

Esportazione delle modifiche nel bucket S3: quando S3 Files copia le modifiche del file system nel bucket S3, l'operazione viene misurata come metadati del file system e lettura del file. Ai fini di questo addebito vengono conteggiati solo i dati letti dallo storage ad alte prestazioni. Ad esempio, se aggiungi dati a un file, S3 Files lo utilizza per evitare di `UploadPartCopy` importare l'intero oggetto su uno storage ad alte prestazioni prima dell'aggiunta. Questo ottimizza i costi di storage ad alte prestazioni.

Operazioni di ridenominazione e spostamento: i bucket S3 non supportano in modo nativo le directory o le ridenominazioni. Ciò che appare come una directory nel file system S3 è un prefisso comune condiviso dalle chiavi degli oggetti nel bucket e gli oggetti S3 sono immutabili. Di conseguenza, quando rinomini o sposti un file, S3 Files copia i dati su un nuovo oggetto con la chiave aggiornata (misurata come richiesta PUT S3) ed elimina l'originale. La sincronizzazione viene misurata come lettura di metadati e lettura di file in base alla posizione dei dati. Se i dati del file non sono archiviati su uno storage ad alte prestazioni, viene applicata solo una lettura di metadati di 4 KB. Per la ridenominazione dei file o lo spostamento di directory, S3 Files ripete questa operazione di copia ed eliminazione per ogni oggetto con quel prefisso. Per ulteriori informazioni, consulta [Comprendere l'impatto delle operazioni di ridenominazione e spostamento](#).

Scadenza dei dati dei file: i dati dei file a cui non si accede entro una finestra configurabile da 1 a 365 giorni (impostazione predefinita: 30 giorni) scadono automaticamente dallo storage ad alte prestazioni. La scadenza non comporta costi di accesso ai dati o ai metadati.

Aggiornamenti dei metadati: i metadati del file system (inode) riflettono il contenuto del bucket S3 collegato. Man mano che il bucket cambia, i metadati vengono aggiornati per rimanere coerenti con lo stato attuale del bucket. I metadati per le directory a cui si accede non scadono mai. Puoi utilizzare la CloudWatch metrica Inode per monitorare l'utilizzo dei metadati. La scadenza dei metadati non comporta alcun addebito. Le modifiche ai metadati POSIX come `chown` e `chmod` aggiornano l'oggetto nel bucket S3. Gli oggetti S3 sono immutabili, quindi S3 Files scrive una nuova versione dell'oggetto con i metadati aggiornati, misurati come richiesta PUT S3 ed esportazione di file S3. Ogni modifica dei metadati crea una versione aggiuntiva dell'oggetto.

Esempi di misurazione

Elencare una directory di grandi dimensioni per la prima volta

Quando elenchi una directory per la prima volta, S3 Files importa i metadati per tutti i file in quella directory. L'importazione di metadati di ogni file viene misurata come scrittura da 4 KB. A seconda della configurazione di importazione (impostazione predefinita 128 KB), S3 Files precarica e copia anche i dati per i file di piccole dimensioni in quella directory sullo storage ad alte prestazioni

del file system per ottimizzarli per la latenza più bassa. L'importazione di dati di ogni file viene misurata come scrittura alla dimensione del file (minimo 32 KB). Puoi controllare quali file hanno i relativi dati importati configurando le tue regole di importazione. Per ulteriori informazioni, consulta [Personalizzazione della sincronizzazione per i file S3](#).

Leggere un file di piccole dimensioni non archiviato su uno storage ad alte prestazioni

S3 Files trasmette i dati letti direttamente dal tuo bucket S3 al tuo client e importa in modo asincrono i dati nello storage ad alte prestazioni del file system, in modo che le letture future siano più veloci. Viene misurato come file system letto alla dimensione dei dati trasferiti (minimo 32 KB). L'importazione asincrona di dati nello storage ad alte prestazioni del file system viene misurata come scrittura in base alla dimensione dei dati trasferiti. Un processo simile viene seguito quando si legge un file i cui dati sono scaduti dal file system. La scadenza dei file dallo storage ad alte prestazioni non comporta alcun costo operativo del file system.

Scrittura sul file system

Tutte le scritture di file vengono archiviate su uno storage ad alte prestazioni e misurate in base alla dimensione dei dati scritti con un minimo di 32 KB. S3 Files attende un periodo di attività di scrittura inattiva (60 secondi) per aggregare le modifiche successive allo stesso file prima di copiarlo nel bucket S3. Le scritture rapide vengono acquisite in un singolo PUT S3 anziché generare una nuova versione dell'oggetto per ogni singola modifica. Ciò riduce sia i costi delle richieste S3 sia i costi di archiviazione dei file ad alte prestazioni. Questa sincronizzazione dei bucket viene misurata come un file system letto per i dati letti da uno storage ad alte prestazioni e come richiesta PUT S3.

Le migliori pratiche per i file S3

Questa pagina descrive le best practice consigliate per lavorare con i file system S3.

Ottimizzazione delle prestazioni e dei costi

- **Parallelizza i tuoi carichi di lavoro:** S3 Files è progettato per supportare carichi di lavoro altamente paralleli. La distribuzione delle letture su più file e più istanze di calcolo aiuta a massimizzare il throughput aggregato. Puoi anche creare più file system con ambito di diversi prefissi specifici all'interno dello stesso bucket (invece di creare un file system sull'intero bucket) per scalare orizzontalmente e migliorare il throughput aggregato.
- **Assegna il file system al prefisso minimo necessario al carico di lavoro per ridurre al minimo l'impatto delle ridenominazioni:** S3 non ha un concetto nativo di directory. Quando si rinomina o

si sposta una directory, S3 Files deve scrivere i dati su un nuovo oggetto con la chiave aggiornata ed eliminare l'originale per ogni file in quella directory. La ridenominazione delle directory con decine di milioni di file può aumentare significativamente i costi delle richieste S3 e i tempi di sincronizzazione. Ambina il tuo file system in base al set di dati attivo o struttura i dati in modo che le directory che prevedi di rinominare contengano meno file. Per ulteriori informazioni, consulta [Comprendere l'impatto delle operazioni di ridenominazione e spostamento](#).

- Utilizzate I/O di grandi dimensioni: S3 Files misura ogni operazione di lettura e scrittura a un minimo di 32 KB. L'utilizzo di I/O di dimensioni maggiori (1 MB o più) ammortizza il sovraccarico operativo ed è più conveniente rispetto a molte letture o scritture di piccole dimensioni. Quando si utilizza il mount helper, le dimensioni predefinite del buffer di lettura e scrittura NFS sono impostate su 1 MB per prestazioni ottimali.
- Regola il LessThan valore delle dimensioni nella configurazione di importazione in modo che corrisponda alle dimensioni dei file: per impostazione predefinita, S3 Files memorizza nella cache i dati per i file di dimensioni inferiori a 128 KB quando accedi per la prima volta a una directory. I file più grandi di questa soglia vengono letti direttamente da S3. Se il carico di lavoro esegue letture ridotte e sensibili alla latenza su file di grandi dimensioni, aumenta la LessThan soglia di dimensione in modo che corrisponda alle dimensioni dei file necessarie sullo storage ad alte prestazioni del file system per un accesso a bassa latenza. Per ulteriori informazioni, consulta [Personalizzazione della sincronizzazione per i file S3](#).
- Imposta le finestre di scadenza in base al ciclo di vita del carico di lavoro: i dati che non sono stati letti entro la finestra di scadenza vengono rimossi automaticamente dal file system. Per carichi di lavoro di breve durata, ad esempio processi in batch o cicli di formazione, utilizza una scadenza più breve (1—7 giorni) per ridurre al minimo i costi di archiviazione. Per i carichi di lavoro che rivisitano gli stessi dati per settimane, utilizza una scadenza più lunga (30-90 giorni) per continuare a beneficiare della bassa latenza. Per ulteriori informazioni, consulta [Personalizzazione della sincronizzazione per i file S3](#).
- Usa regole con ambito di prefisso per carichi di lavoro misti: se il bucket contiene dati a cui si accede di frequente e a cui si accede raramente, crea regole di importazione separate per ogni prefisso. Ciò ti consente di importare i dati in modo aggressivo per i prefissi caldi mantenendo i soli metadati dei prefissi freddi. Per ulteriori informazioni, consulta [Personalizzazione della sincronizzazione per i file S3](#).
- Crea un target di montaggio in ogni zona di disponibilità: ti consigliamo di creare un target di montaggio in ogni zona di disponibilità in cui operi in modo da ridurre i costi di trasferimento dei dati tra le diverse AZ e migliorare le prestazioni. Ciò garantisce che le risorse di elaborazione dispongano sempre di un percorso di rete locale verso il file system, migliorando sia la disponibilità

che la latenza. Quando si crea un file system utilizzando la Console di AWS gestione, S3 Files crea automaticamente una destinazione di montaggio in ogni zona di disponibilità del VPC selezionato.

Sincronizzazione

- Comprendi il modello di coerenza di S3 Files: quando un file nel file system viene modificato contemporaneamente all'oggetto corrispondente nel bucket S3, S3 Files considera il bucket S3 come fonte di verità e sposta il file nella directory degli oggetti smarriti. Per evitare conflitti, designate un percorso (file system o S3) come autore principale.
- Monitora lo stato della sincronizzazione: utilizza CloudWatch le metriche per monitorare lo stato della sincronizzazione tra il tuo file system e il bucket S3. Un aumento `PendingExports` indica che il carico di lavoro sta generando modifiche più velocemente della velocità di sincronizzazione, il che significa che il completamento della sincronizzazione richiederà più tempo. Una `ExportFailures` CloudWatch metrica diversa da zero indica i file che non possono essere esportati e richiedono un'azione. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi ai file S3](#).

Controllo accessi

- Segui il principio del privilegio minimo: concedi solo le autorizzazioni minime richieste per ogni ruolo IAM e policy del file system. Ad esempio, se una risorsa di calcolo deve solo leggere i dati dal file system, allega la policy `AmazonS3FilesClientReadOnlyAccess` gestita anziché `AmazonS3FilesClientFullAccess`. Inoltre, valuta la possibilità di creare il tuo file system con un prefisso specifico anziché l'intero bucket, in modo che i client possano accedere ai dati solo all'interno di quel prefisso.
- Non modificare il ruolo IAM di S3 Files: non modificate o eliminate il ruolo IAM che S3 Files assume per sincronizzare con il bucket S3. La modifica o la rimozione di questo ruolo può interrompere la sincronizzazione tra il file system e il bucket S3.
- Non modificare la regola S3 Files: S3 Files crea una EventBridge EventBridge regola (preceduta da `DO-NOT-DELETE-S3-Files`) per rilevare le modifiche nel bucket S3. Non disattivare, modificare o eliminare questa regola. La sua rimozione impedisce a S3 Files di rilevare oggetti nuovi o modificati nel bucket, causando l'obsolescenza del file system.
- Valuta la possibilità di limitare l'accesso ai log scritti da **efs-utils**: `efs-utils` scrive i nomi delle chiavi degli oggetti S3 direttamente nei log che memorizza nella directory `/var/log/amazon/efs`. Se i nomi delle chiavi S3 contengono informazioni sensibili, è necessario limitare l'accesso a

questa directory tramite le autorizzazioni POSIX. Ad esempio, è possibile limitare l'accesso tramite il comando. `sudo chmod 700 /var/log/amazon/efs`

Monitoraggio

- Imposta allarmi in caso di errori di sincronizzazione: crea CloudWatch allarmi attivi `ImportFailures` e ricevi una notifica quando i file non riescono `ExportFailures` a sincronizzarsi. Le esportazioni non riuscite possono indicare problemi di autorizzazione, problemi con le chiavi di crittografia o limiti di lunghezza del percorso. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi ai file S3](#).

Migrazione

Per migrare i dati dallo storage locale al bucket S3 per la prima volta, ti consigliamo di utilizzare. AWS DataSync DataSync automatizza e accelera il trasferimento di set di dati di grandi dimensioni e preserva i metadati e le autorizzazioni dei file durante la migrazione. Per ulteriori informazioni, vedi Che cos'è? [AWS DataSync](#).

Funzionalità, limiti e quote non supportati

Questa pagina descrive le limitazioni e le quote quando si utilizzano i file S3.

Funzionalità S3 non supportate

- Classi di archiviazione: non è possibile accedere agli oggetti nelle classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive tramite il file system. Analogamente, non è possibile accedere agli oggetti nei livelli S3 Intelligent-Tiering Archive Access o Deep Archive Access tramite il file system. È necessario innanzitutto ripristinare questi oggetti utilizzando l'API S3.
- Liste di controllo degli accessi (ACL) S3: gli ACL S3 non vengono conservati dopo le modifiche apportate tramite il file system. Ti consigliamo di mantenere gli ACL disattivati e di utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, indipendentemente da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Gestire l'accesso con gli ACL](#).

Limitazioni del file system

- Collegamenti fisici: S3 Files non supporta i collegamenti fisici. Ogni file nel file system corrisponde a una singola chiave oggetto S3.
- Dimensione del componente del percorso: S3 Files non supporta oggetti in cui una singola directory o nome di file nel percorso supera i 255 byte. Un componente di percorso è una directory o un nome di file derivato da una chiave oggetto S3. Ad esempio, la chiave `dir1/dir2/file.txt` ha tre componenti di percorso: `dir1`, `dir2`, e `file.txt`.
- Nomi chiave di oggetti S3 incompatibili: S3 Files non supporta l'accesso ai nomi di chiave S3 che non corrispondono a percorsi di file POSIX validi, inclusi i componenti del percorso vuoto (`()`), i componenti del percorso relativo (`(,foo//bar)`) e i nomi di chiave `foo/./bar` contenenti `foo/./bar` byte nulli.
- Limite di dimensione della chiave S3: i file o le directory il cui nome di percorso completo supera il limite di dimensione della chiave dell'oggetto S3 di 1.024 byte non possono essere esportati in S3.
- Destinazioni dei collegamenti simbolici: se un oggetto S3 è un collegamento simbolico, la sua destinazione deve essere un percorso valido che non sia vuoto e non superi i 4.080 byte.
- Dimensione dei metadati delle autorizzazioni POSIX: i file o le directory in cui i metadati delle autorizzazioni POSIX superano i 2 KB non possono essere esportati in S3.

Quote

Le seguenti quote possono essere aumentate contattando l'assistenza. AWS

Risorsa	Quota predefinita
File system per account AWS	1.000

Per richiedere un aumento, apri il Centro [AWS assistenza](#), scegli **Crea caso**, quindi scegli **Aumento del limite di servizio**.

Le seguenti quote non possono essere modificate.

Risorsa	Quota
Punti di accesso per file system	25.000

Risorsa	Quota
Connessioni per file system	25.000
Monta le destinazioni per file system per zona di disponibilità	1
Gruppi di sicurezza per destinazione di montaggio	5
Tag per file system	50
VPC per file system	1

Esistono anche quote specifiche per i singoli file system.

Risorsa	Quota
Dimensione massima dei file	52.673.613.135.872 byte (48 TiB)
Profondità massima della directory	1.000 livelli
Lunghezza massima dei nomi di file	255 byte
Lunghezza massima della destinazione del collegamento simbolico	4.080 byte
Lunghezza massima della chiave dell'oggetto S3	1.024 byte
Numero massimo di file aperti per client	65.536
Numero massimo di account utente attivi per cliente	65.536
Numero massimo di blocchi per file	512 in tutte le istanze connesse
Numero massimo di blocchi per montaggio	8.192 su un massimo di 256 coppie di processi di file
Limite delle dimensioni delle policy del file system	20.000 caratteri

Funzionalità NFS non supportate

S3 Files supporta NFSv4.1 e NFSv4.2, con le seguenti eccezioni:

- pNFS
- Delega o callback del cliente
- Chiusura obbligatoria (tutte le serrature sono indicative)
- Deny share
- Liste di controllo degli accessi (ACL)
- Kerberos-based sicurezza
- NFSv4.1 conservazione dei dati
- SetUID su cartelle
- Dispositivi a blocchi, dispositivi a caratteri, directory di attributi e attributi denominati
- Funzionalità opzionali introdotte in NFSv4.2 (come copia lato server, operazioni su file sparsi, prenotazione dello spazio, I/O consigli sulle applicazioni, blocchi di dati delle applicazioni, NFS etichettati e attributi estesi personalizzati definiti dall'utente)
- Cache di risposta persistente
- nconnectL'opzione mount

Risoluzione dei problemi relativi ai file S3

Questa pagina consente di diagnosticare e risolvere i problemi più comuni relativi ai file S3.

- [Il comando Mount non riesce](#)
- [Autorizzazione negata per le operazioni sui file](#)
- [Il routing di lettura intelligente non funziona](#)
- [Il file system restituisce costantemente un errore del server NFS](#)
- [Oggetto mancante nel bucket S3 dopo la scrittura del file system](#)
- [Oggetto S3 non visibile nel file system](#)
- [File che appaiono nella directory oggetti smarriti](#)
- [La sincronizzazione è in ritardo](#)
- [Attivazione dei log di debug dei client](#)

Il comando Mount non riesce

Il mount `-t s3files` comando ha esito negativo e genera un errore.

Cause e azioni comuni:

- «mount.s3files: command not found» — Il client S3 Files (amazon-efs-utils) non è installato o è inferiore alla versione 3.0.0. Installa o aggiorna il client. Per ulteriori informazioni, consulta [Prerequisiti per i file S3](#).
- «Risoluzione del nome DNS del file system non riuscita»: non esiste un target di montaggio nella zona di disponibilità in cui è in esecuzione l'istanza EC2. Crea un target di montaggio in quella zona di disponibilità o avvia l'istanza in una zona di disponibilità con un target di montaggio. Per ulteriori informazioni, consulta [Creazione di destinazioni di montaggio](#).
- Connessione scaduta: la configurazione del gruppo di sicurezza non consente il traffico NFS. Verifica che il gruppo di sicurezza del target di montaggio consenta il TCP in ingresso sulla porta 2049 dal gruppo di sicurezza della tua istanza e che il gruppo di sicurezza della tua istanza consenta il TCP in uscita sulla porta 2049 al gruppo di sicurezza del target di montaggio. Per ulteriori informazioni, consulta [Prerequisiti per i file S3](#).
- «Accesso negato» durante il montaggio: il ruolo IAM associato alla risorsa di calcolo non dispone delle autorizzazioni S3 Files richieste. Verifica che al ruolo sia associata la policy AmazonS3FilesClientFullAccess o AmazonS3FilesClientReadOnlyAccess gestita, o almeno l'autorizzazione. `s3files:ClientMount` Per ulteriori informazioni, consulta [Prerequisiti per i file S3](#).
- botocore non installato: il mount helper richiede botocore per interagire con i servizi. AWS Installa botocore seguendo le istruzioni nel README di amazon-efs-utils on. GitHub

Autorizzazione negata per le operazioni sui file

È possibile montare il file system ma ricevere gli errori «Autorizzazione negata» o «Operazione non consentita» durante la lettura, la scrittura o l'accesso ai file.

Cause e azioni comuni:

- Autorizzazione di scrittura mancante: se sai leggere ma non scrivere, verifica che il ruolo IAM associato alla tua risorsa di calcolo includa l'`s3files:ClientWrite` autorizzazione oppure allega la policy AmazonS3FilesClientReadWriteAccess o AmazonS3FilesClientFullAccess gestita. Per ulteriori informazioni, consulta le politiche [AWS gestite per i file Amazon S3](#).

- **Accesso root mancante:** se ricevi errori di autorizzazione durante l'accesso ai file di proprietà di root (UID 0), il tuo ruolo IAM potrebbe non disporre dell'`s3files:ClientRootAccess` autorizzazione. Senza questa autorizzazione, tutte le operazioni vengono eseguite come utente anonimo NFS (in genere `nfsnobody`), che potrebbe non avere accesso ai file. Allega la policy `AmazonS3FilesClientFullAccess` gestita o aggiungila `s3files:ClientRootAccess` alla tua policy.
- **Politica del file system che nega l'accesso:** se hai allegato una politica del file system, verifica che non neghi le azioni necessarie ai tuoi clienti. Un «consenti» nella policy basata sull'identità o nella policy del file system è sufficiente per l'accesso. Per ulteriori informazioni, consulta [Come funziona S3 Files con IAM](#).
- **Mancata corrispondenza delle autorizzazioni POSIX:** S3 Files applica le autorizzazioni POSIX standard (proprietario, gruppo, altri) su file e directory. Se l'applicazione viene eseguita come utente che non corrisponde al proprietario o al gruppo del file, l'accesso potrebbe essere negato anche se le autorizzazioni IAM sono corrette. Utilizza un punto di accesso per imporre uno specifico UID/GID per tutte le richieste. Per ulteriori informazioni, consulta [Creazione di punti di accesso per un file system S3](#).

Il routing di lettura intelligente non funziona

S3 Files esegue un routing di lettura intelligente poiché indirizza automaticamente le richieste di lettura al livello di archiviazione più adatto a loro, mantenendo al contempo la semantica completa del file system, tra cui coerenza, blocco e autorizzazioni POSIX. Le piccole letture casuali dei file utilizzati attivamente vengono eseguite dallo storage ad alte prestazioni per una bassa latenza. Le letture sequenziali di grandi dimensioni e le letture di dati non presenti nel file system vengono eseguite direttamente dal bucket S3 per un throughput elevato, senza alcun costo per i dati del file system.

Il routing di lettura intelligente potrebbe non funzionare se una delle metriche di connettività del client (`NFSConnectionAccessible`, `S3BucketAccessible`, `eS3BucketReachable`) mostra 0 o se non viene visualizzata la velocità di lettura prevista.

Cause e azioni comuni:

- **Politica in linea S3 mancante sul ruolo di elaborazione:** il ruolo IAM associato alla risorsa di elaborazione deve includere una concessione di policy in linea `s3:GetObject` e `s3:GetObjectVersion` sul bucket S3 collegato. Senza questa policy, il mount helper non può leggere direttamente da S3 e tutte le letture passano attraverso il file system. Per ulteriori informazioni, consulta [Prerequisiti per i file S3](#).

- **Secchio S3 non raggiungibile:** controlla la metrica. `S3BucketReachable`. Se mostra 0, verifica che la tua risorsa di calcolo abbia accesso alla rete a S3 (ad esempio, tramite un endpoint VPC o un gateway NAT).
- **Il file è stato modificato:** le letture vengono effettuate direttamente da S3 solo quando il file non è stato modificato tramite il file system. Se avete scritto sul file e le modifiche non sono ancora state sincronizzate con S3, le letture vengono eseguite nel file system fino al completamento della sincronizzazione.

Il file system restituisce costantemente un errore del server NFS

Un file system crittografato restituisce regolarmente errori del server NFS. Questi errori possono verificarsi quando S3 Files non è in grado di recuperare la chiave KMS da AWS KMS per uno dei seguenti motivi:

- La chiave è stata disabilitata.
- La chiave è stata eliminata.
- L'autorizzazione per S3 Files di utilizzare la chiave è stata revocata.
- AWS KMS è temporaneamente non disponibile.

Operazione da eseguire

Innanzitutto, conferma che la chiave AWS KMS sia abilitata. Puoi visualizzare le tue chiavi nella console AWS KMS. Per ulteriori informazioni, consulta [Visualizzazione di chiavi](#) nella Guida per gli sviluppatori del Servizio AWS di gestione delle chiavi.

Se la chiave non è abilitata, abilitarla. Per ulteriori informazioni, consulta [Abilitazione e disabilitazione delle chiavi](#) nella Guida per gli sviluppatori del Servizio AWS di gestione delle chiavi.

Se la chiave è in attesa di cancellazione, annulla l'eliminazione e riattiva la chiave. Per ulteriori informazioni, vedere [Pianificazione e annullamento dell'eliminazione](#) delle chiavi nella Key Management Service Developer Guide. AWS

Se la chiave è abilitata e i problemi persistono, contatta l'assistenza. AWS

Oggetto mancante nel bucket S3 dopo la scrittura del file system

Hai scritto un file tramite il file system e ti aspettavi che apparisse come oggetto nel bucket S3, ma l'oggetto non è presente. S3 Files attende un periodo di inattività di scrittura (60 secondi) prima di

esportare nuovamente le modifiche nel bucket S3. Se l'oggetto continua a non apparire dopo questo periodo, l'esportazione potrebbe non essere riuscita. In tal caso, viene visualizzato l'aumento della FailedExports CloudWatch metrica.

Operazione da eseguire

Controlla lo stato di esportazione del file utilizzando gli attributi estesi:

```
getfattr -n "user.s3files.status;$(date -u +%s)" missing-file.txt --only-values
```

Il timestamp nel nome dell'attributo ti assicura di ottenere lo stato più recente. Output di esempio:

```
S3Key: s3://bucket/prefix/missing-file.txt
ExportError: PathTooLong
```

ExportError non viene visualizzato se non si verifica un errore di esportazione. S3Key è vuoto se un oggetto S3 non è mai stato collegato al file.

La tabella seguente elenca tutti i ExportError valori possibili:

Errore	Causa
S3AccessDenied	Il ruolo IAM che S3 Files assume non dispone di autorizzazioni sufficienti per scrivere nel bucket S3. Per ulteriori informazioni, consulta Prerequisiti per i file S3 .
InternalError	Si è verificato un errore interno del sistema.
S3UserMetadataTooLarge	È stato superato il limite di dimensione dei metadati utente S3. Funzionalità, limiti e quote non supportati Per informazioni su questi limiti, consulta.
EncryptionKeyInaccessible	La chiave di crittografia utilizzata dal bucket S3 non è accessibile ai file S3. Concedi a S3 Files l'accesso alla tua chiave di crittografia. Per ulteriori informazioni, consulta Encryption (Crittografia) .
RoleAssumptionFailed	Non ho potuto assumere il ruolo. Controlla le tue politiche di fiducia. Per ulteriori informazioni, consulta Prerequisiti per i file S3 .

Errore	Causa
KeyTooLongToBreakCycle	S3 Files non è riuscito a risolvere una dipendenza circolare (ad esempio, a causa della ridenominazione di due file con i rispettivi nomi) perché il percorso del file supera il limite di lunghezza della chiave S3. Abbreviate il percorso della directory per risolvere questo errore.
PathTooLong	Il percorso del file supera il limite di lunghezza della chiave S3. Funzionalità, limiti e quote non supportati Per informazioni su questi limiti, consulta.
DependencyExportFailed	Un elemento principale o una dipendenza presenta un errore di esportazione non ripetibile. Controlla lo stato del genitore o di eventuali dipendenze utilizzando <code>getfattr</code> .
S3ObjectArchived	L'oggetto S3 è archiviato (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive) e non può essere letto. Ripristina prima l'oggetto utilizzando le API S3.

S3 Files riprova automaticamente le esportazioni non riuscite. `ExportError` viene visualizzato solo per gli errori non ripetibili.

Oggetto S3 non visibile nel file system

Un oggetto esiste nel bucket S3 ma non appare nel file system. Il nome della chiave dell'oggetto potrebbe non corrispondere a un percorso di file POSIX valido. S3 Files non supporta l'accesso ai nomi di chiave S3 con componenti di percorso vuoti (`foo//bar`), componenti di percorso relativo (`foo/./bar`, `foo/..bar`), nomi di chiave contenenti byte nulli o nomi di chiave in cui qualsiasi componente di percorso supera i 255 byte. Gli oggetti con nomi di chiave incompatibili non vengono importati nel file system.

File che appaiono nella directory oggetti smarriti

I file sono stati visualizzati nella `.s3files-lost+found-file-system-id` directory principale del file system. In questo caso, si vede l'aumento della `LostAndFoundFiles` CloudWatch metrica. Ciò si verifica quando si verifica un conflitto di sincronizzazione. Si verifica un conflitto quando lo stesso file viene modificato tramite il file system e l'oggetto S3 corrispondente cambia prima che S3

Files sincronizza le modifiche del file system con S3. S3 Files considera il bucket S3 come fonte di verità, sposta il file in conflitto nella directory degli oggetti smarriti e importa la versione più recente dal bucket S3 nel file system.

Identificazione dei file nella directory degli oggetti smarriti

Quando S3 Files sposta un file nella directory degli oggetti smarriti, aggiunge al nome del file un identificatore esadecimale per distinguere più versioni dello stesso file che possono essere spostate nel tempo. I nomi di file più lunghi di 100 caratteri vengono troncati per fare spazio a questo identificatore. Il percorso della directory originale del file non viene conservato nella directory degli oggetti smarriti.

Operazione da eseguire

Ottieni il percorso originale del file e la chiave oggetto S3 corrispondente:

```
getfattr -n "user.s3files.status;$(date -u +%s)" .s3files-lost  
+found-fs-12345678/abcdef1234_report.csv --only-values
```

Output di esempio:

```
S3Key: s3://bucket/prefix/report.csv  
FilePath: /data/report.csv
```

Campo	Description
S3Key	Percorso S3 completo dell'oggetto che ha causato il conflitto o vuoto se l'oggetto è stato eliminato nel bucket S3.
FilePath	Percorso relativo del file prima del conflitto.

È quindi possibile conservare la versione più recente dal bucket S3 ed eliminare il file dalla directory oggetti smarriti oppure copiare il file dalla directory oggetti smarriti nel percorso originale per sovrascrivere la versione S3.

 Note

I file nella directory degli oggetti smarriti rimangono lì a tempo indeterminato e vengono conteggiati ai fini dei costi di archiviazione del file system. Elimina i file dalla directory oggetti smarriti quando non sono più necessari.

La sincronizzazione è in ritardo

La PendingExports CloudWatch metrica è in aumento, a indicare che il carico di lavoro sta generando modifiche più velocemente di quanto S3 Files sia in grado di sincronizzarle con S3.

Ciò significa che il carico di lavoro potrebbe superare la velocità di sincronizzazione. S3 Files esporta fino a 800 file al secondo per file system. Valuta la possibilità di ridurre il tasso di modifiche ai file o di distribuire il lavoro su più file system. Monitora la PendingExports metrica nel tempo. Se si stabilizza o diminuisce, S3 Files sta recuperando terreno. Se continua a crescere, contatta l'assistenza. AWS

Attivazione dei log di debug dei client

Se stai risolvendo problemi di montaggio, connettività o bypass di lettura, puoi abilitare la registrazione a livello di debug sul client S3 Files per acquisire maggiori dettagli.

Mount helper e watchdog logs

Modifica `/etc/amazon/efs/s3files-utils.conf` e cambia il livello di registrazione da INFO a DEBUG:

```
[DEFAULT]
logging_level = DEBUG
```

Smonta e rimonta il file system affinché la modifica abbia effetto:

```
sudo umount /mnt/s3files
sudo mount -t s3files file-system-id:/ /mnt/s3files
```

I log vengono scritti su. `/var/log/amazon/efs/` Il log di mount helper è `mount.log`.

Log del proxy (efs-proxy)

Il proxy gestisce il traffico NFS e il bypass di lettura S3. Per abilitare la registrazione di debug per il proxy, modifica: `/etc/amazon/efs/s3files-utils.conf`

```
[proxy]
proxy_logging_level = DEBUG
```

Smonta e rimonta per rendere effettiva la modifica. I log dei proxy vengono scritti su. `/var/log/amazon/efs/`

Log del tunnel TLS (stunnel)

I log del tunnel TLS sono disabilitati per impostazione predefinita. Per abilitarli, modifica `/etc/amazon/efs/s3files-utils.conf` e imposta quanto segue:

```
[mount]
stunnel_debug_enabled = true
```

Per salvare tutti i log degli stunnel di un file system in un unico file, decommentate anche la `stunnel_logs_file` riga:

```
stunnel_logs_file = /var/log/amazon/efs/{fs_id}.stunnel.log
```

Limiti alle dimensioni dei log

I file di registro vengono ruotati automaticamente. È possibile configurare la dimensione e il numero massimi di file ruotati in: `s3files-utils.conf`

```
[DEFAULT]
logging_max_bytes = 1048576
logging_file_count = 10
```

L'impostazione predefinita è 1 MB per file di registro con 10 file ruotati, per un massimo di 10 MB per tipo di registro.

Condivisione dei log con l'assistenza AWS

Quando contatti l' AWS assistenza, raccogli i log e la configurazione del cliente in un unico archivio:

```
sudo tar -czf /tmp/s3files-support-logs.tar.gz \
/var/log/amazon/efs/ \
```

```
/etc/amazon/efs/s3files-utils.conf
```

/tmp/s3files-support-logs.tar.gzIncludilo nella tua richiesta di assistenza.

Controllo degli accessi in Amazon S3

In AWS, una risorsa è un'entità con cui puoi lavorare. In Amazon Simple Storage Service (S3), i bucket e gli oggetti sono le risorse originali di Amazon S3. Ogni cliente S3 ha probabilmente dei bucket con degli oggetti al loro interno. Con l'aggiunta di nuove funzionalità a S3, sono state aggiunte anche risorse supplementari, ma non tutti i clienti utilizzano queste risorse specifiche. Per ulteriori informazioni sulle risorse Amazon S3, consulta [Risorse S3](#).

Per impostazione predefinita, tutte le risorse Amazon S3 sono private. Inoltre, per impostazione predefinita, l'utente root di Account AWS che ha creato la risorsa (proprietario della risorsa) e gli utenti IAM all'interno di quell'account con le autorizzazioni necessarie possono accedere a una risorsa che hanno creato. Il proprietario della risorsa decide chi può accedere alla risorsa e le azioni che gli altri possono eseguire sulla risorsa. S3 dispone di vari strumenti di gestione degli accessi che possono essere utilizzati per concedere ad altri l'accesso alle risorse S3.

Le sezioni seguenti forniscono una panoramica delle risorse S3, degli strumenti di gestione degli accessi S3 disponibili e dei migliori casi d'uso per ciascuno strumento di gestione degli accessi. Gli elenchi di queste sezioni vogliono essere completi e includere tutte le risorse S3, gli strumenti di gestione degli accessi e i casi d'uso più comuni di gestione degli accessi. Allo stesso tempo, queste sezioni sono concepite come directory che conducono l'utente ai dettagli tecnici desiderati. Se hai già una buona conoscenza di alcuni dei seguenti argomenti, puoi passare alla sezione che fa al caso tuo.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Argomenti

- [Risorse S3](#)
- [Identità](#)
- [Strumenti di gestione degli accessi](#)
- [Azioni](#)
- [Casi d'uso della gestione degli accessi](#)
- [Risoluzione dei problemi di gestione degli accessi](#)

Risorse S3

Le risorse originali di Amazon S3 sono i bucket e gli oggetti che contengono. Con l'aggiunta di nuove funzionalità a S3, vengono aggiunte anche nuove risorse. Di seguito è riportato un elenco completo delle risorse S3 e delle rispettive caratteristiche.

Tipo di risorsa	Funzione Amazon S3	Description
bucket	Caratteristiche principali	Un bucket è un container per oggetti o file. Per memorizzare un oggetto in S3, creare un bucket e quindi caricare uno o più oggetti nel bucket. Per ulteriori informazioni, consulta Creazione, configurazione e utilizzo di bucket per uso generico Amazon S3 .
object		Un oggetto può essere un file e tutti i metadati che lo descrivono. Quando un oggetto è nel bucket, è possibile aprirlo, scaricarlo e spostarlo. Per ulteriori informazioni, consulta Utilizzo degli oggetti in Amazon S3 .
accesspoint	Punti di accesso	I punti di accesso sono endpoint di rete denominati, collegati a bucket che possono essere utilizzati per eseguire operazioni su oggetti Amazon S3, come <code>GetObject</code> e <code>PutObject</code> . Ogni punto di accesso ha autorizzazioni distinte, controlli di rete e una policy personalizzata che funziona insieme alla policy di bucket collegata al bucket sottostante. È possibile configurare qualsiasi punto di accesso in modo che accetti richieste solo da un cloud privato virtuale (VPC) o configurare impostazioni di blocco dell'accesso pubblico personalizzate per ciascun punto di accesso. Per ulteriori informazioni, consulta Gestione dell'accesso a set di dati condivisi con punti di accesso .
objectlambdaccesspoint		Un punto di accesso Lambda per oggetti è un punto di accesso per un bucket che è anche associato a una funzione Lambda. Con un punto di accesso Lambda per oggetti, è possibile aggiungere il proprio codice alle

Tipo di risorsa	Funzione Amazon S3	Description
		richieste di Amazon S3 GET, LIST e HEAD per modificare ed elaborare i dati quando vengono restituiti a un'applicazione. Per ulteriori informazioni, consulta Creazione di punti di accesso Object Lambda .
multiregionaccesspoint		Multi-Region Gli access point forniscono un endpoint globale che le applicazioni possono utilizzare per soddisfare le richieste provenienti da bucket Amazon S3 che si trovano in più regioni. AWS Puoi utilizzare gli Multi-Region Access Points per creare applicazioni multiregionali con la stessa architettura utilizzata in una singola regione e quindi eseguire tali applicazioni in qualsiasi parte del mondo. Invece di inviare richieste tramite la rete Internet pubblica e congestionata, le richieste di applicazione effettuate a un endpoint globale di Multi-Region Access Point vengono indirizzate automaticamente attraverso la rete AWS globale al bucket Amazon S3 di prossimità più vicino. Per ulteriori informazioni, consulta Gestione del traffico multiregionale con punti di Multi-Region accesso .
job	Operazioni in batch S3	Un processo è una risorsa della funzionalità Operazioni in batch S3. È possibile utilizzare Operazioni in batch S3 per eseguire operazioni in batch su larga scala su elenchi di oggetti Amazon S3 specificati dall'utente. Amazon S3 tiene traccia dell'avanzamento del processo dell'operazione batch, invia notifiche e memorizza un report dettagliato sul completamento di tutte le azioni, offrendo un'esperienza completamente gestita, verificabile e serverless. Per ulteriori informazioni, consulta Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch .

Tipo di risorsa	Funzione Amazon S3	Description
storagele nsconfigu ration	S3 Storage Lens	Una configurazione di S3 Storage Lens raccoglie le metriche di storage dell'intera organizzazione e i dati degli utenti tra gli account. S3 Storage Lens offre agli amministratori un'unica visione dell'utilizzo e dell'attività di object storage su centinaia o addirittura migliaia di account di un'organizzazione, con dettagli per generare approfondimenti a più livelli di aggregazione. Per ulteriori informazioni, consulta Monitoraggio dell'attività e dell'utilizzo dello storage con Amazon S3 Storage Lens .
storagele nsgroup		Un gruppo S3 Storage Lens aggrega le metriche utilizzando filtri personalizzati basati sui metadati degli oggetti. I gruppi S3 Storage Lens consentono di analizzare le caratteristiche dei dati, come la distribuzione degli oggetti in base all'età, i tipi di file più comuni e altro ancora. Per ulteriori informazioni, consulta Operazioni con i gruppi S3 Storage Lens per filtrare e aggregare le metriche .
accessgra ntsinstan ce	S3 Access Grants	Un'istanza di S3 Access Grants è un container per i grant S3 creati dall'utente. Con S3 Access Grants, è possibile creare grant ai dati Amazon S3 per le identità IAM all'interno del proprio account, per le identità IAM di altri account (multi-account) e per le identità di directory aggiunte a Centro identità AWS IAM dalla directory aziendale. Per ulteriori informazioni su S3 Access Grants, consulta Gestione dell'accesso con S3 Access Grants .

Tipo di risorsa	Funzione Amazon S3	Description
accessgrantslocation		Una posizione Access Grants è un bucket, un prefisso all'interno di un bucket o un oggetto registrato nell'istanza S3 Access Grants. È necessario registrare le posizioni all'interno dell'istanza S3 Access Grants prima di poter creare una concessione per quella posizione. Quindi, con S3 Access Grants, puoi concedere l'accesso al bucket, al prefisso o all'oggetto per le identità IAM all'interno del tuo account, le identità IAM in altri account (tra account) e le identità di directory aggiunte dalla tua directory aziendale . Centro identità AWS IAM Per ulteriori informazioni su S3 Access Grants, consulta Gestione dell'accesso con S3 Access Grants
accessgrant		Una concessione di accesso è una concessione individuale ai dati di Amazon S3. Con S3 Access Grants, puoi creare sovvenzioni ai tuoi dati Amazon S3 per le identità IAM all'interno del tuo account, le identità IAM in altri account (tra account) e le identità di directory aggiunte Centro identità AWS IAM dalla tua directory aziendale. Per ulteriori informazioni su S3 Access Grants, consulta Gestione dell'accesso con S3 Access Grants

Bucket

Esistono due tipi di bucket Amazon S3: bucket per uso generico e bucket di directory.

- I bucket per uso generico sono il tipo di bucket S3 originale e sono consigliati per la maggior parte dei casi d'uso e dei modelli di accesso. I bucket per uso generico consentono inoltre di archiviare oggetti in tutte le classi di storage, ad eccezione di S3 Express One Zone. Per ulteriori informazioni sulle classi di storage S3, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).
- I bucket di directory utilizzano la classe di storage S3 Express One Zone, consigliata se l'applicazione è sensibile alle prestazioni e beneficia di latenze a una cifra al millisecondo PUT e GET. Per ulteriori informazioni, consultare [Operazioni con i bucket di directory](#), [S3 Express One Zone](#) e [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).

Categorizzazione delle risorse S3

Amazon S3 offre funzioni per categorizzare e organizzare le risorse S3. La categorizzazione delle risorse non è utile solo per organizzarle, ma è anche possibile impostare regole di gestione degli accessi basate sulle categorie delle risorse. In particolare, i prefissi e i tag sono due funzioni di organizzazione dello storage che possono essere utilizzate quando si impostano le autorizzazioni per la gestione degli accessi.

Note

Le seguenti informazioni si riferiscono ai bucket per uso generico. I bucket di directory non supportano i tag e hanno limitazioni sui prefissi. Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).

- **Prefissi** - Un prefisso in Amazon S3 è una stringa di caratteri all'inizio del nome della chiave di un oggetto, utilizzata per organizzare gli oggetti memorizzati nei bucket S3. Si può usare un carattere delimitatore, come una barra in avanti (/), per indicare la fine del prefisso all'interno del nome della chiave dell'oggetto. Ad esempio, si possono avere nomi di chiavi di oggetti che iniziano con il prefisso `engineering/` oppure nomi di chiavi di oggetti che iniziano con il prefisso `marketing/campaigns/`. L'uso di un delimitatore alla fine del prefisso, come ad esempio un carattere di barra in avanti / emula le convenzioni di denominazione delle cartelle e dei file. Tuttavia, in S3, il prefisso fa parte del nome della chiave dell'oggetto. Nei bucket S3 per uso generico, non esiste una vera e propria gerarchia di cartelle.

Amazon S3 supporta l'organizzazione e il raggruppamento degli oggetti utilizzando i loro prefissi. È anche possibile gestire l'accesso agli oggetti in base ai loro prefissi. Ad esempio, è possibile limitare l'accesso solo agli oggetti con nomi che iniziano con un prefisso specifico.

Per ulteriori informazioni, consulta [Organizzazione degli oggetti utilizzando i prefissi](#). La console S3 utilizza il concetto di cartelle che, nei bucket per uso generico, sono essenzialmente prefissi che vengono anteposti al nome della chiave dell'oggetto. Per ulteriori informazioni, consulta [Organizzazione degli oggetti nella console di Amazon S3 utilizzando le cartelle](#).

- **Tag** - Ogni tag è una coppia chiave-valore che si assegna alle risorse. Ad esempio, è possibile etichettare alcune risorse con il tag `topicCategory=engineering`. L'etichettatura può essere utilizzata per contribuire all'allocazione dei costi, alla categorizzazione e all'organizzazione e al controllo degli accessi. L'etichettatura dei bucket viene utilizzata solo per l'allocazione dei costi. È possibile etichettare gli oggetti dei tag, S3 Storage Lens, i processi e S3 Access Grants ai fini

dell'organizzazione o del controllo degli accessi. In S3 Access Grants, è possibile utilizzare i tag per l'allocazione dei costi. Come esempio di controllo dell'accesso alle risorse tramite i loro tag, è possibile condividere solo gli oggetti che hanno un tag specifico o una combinazione di tag.

Per ulteriori informazioni, consultare [Controllo dell'accesso alle risorse AWS mediante i tag](#) nella Guida per l'utente di IAM.

Identità

In Amazon S3, il proprietario della risorsa è l'identità che ha creato la risorsa, come un bucket o un oggetto. Per impostazione predefinita, solo l'utente root dell'account che ha creato la risorsa e le identità IAM all'interno dell'account che dispongono delle autorizzazioni richieste possono accedere alla risorsa S3. I proprietari delle risorse possono concedere ad altre identità l'accesso alle loro risorse S3.

Le identità che non possiedono una risorsa possono richiedere l'accesso a tale risorsa. Le richieste a una risorsa sono autenticate o non autenticate. Le richieste autenticate devono includere un valore di firma che autentichi il mittente della richiesta, mentre le richieste non autenticate non richiedono una firma. Si consiglia di concedere l'accesso solo agli utenti autenticati. Per ulteriori informazioni sull'autenticazione delle richieste, consulta [Esecuzione di richieste](#) nella documentazione di riferimento delle API di Amazon S3.

Important

Ti consigliamo di non utilizzare le credenziali dell'utente root per effettuare richieste autenticate Account AWS. Crea invece un ruolo IAM, concedendo a esso l'accesso completo. Gli utenti con questo ruolo vengono definiti utenti amministratori. È possibile utilizzare le credenziali assegnate al ruolo di amministratore, anziché le credenziali di utente Account AWS root, per interagire AWS ed eseguire attività, ad esempio creare un bucket, creare utenti e concedere autorizzazioni. Per ulteriori informazioni, consulta [Credenziali dell'utente root e credenziali dell'utente IAM Account AWS](#) nella Guida all'utente IAM. Riferimenti generali di AWS e consulta le [Best practice di sicurezza in IAM](#) nella Guida dell'utente IAM.

Le identità che accedono ai dati in Amazon S3 possono essere una delle seguenti:

Account AWS owner

Chi ha creato la Account AWS risorsa. Ad esempio, l'account che ha creato il bucket. Questo account è il proprietario della risorsa. Per ulteriori informazioni, consulta [Account utente root AWS](#).

Identità IAM nello stesso account di Account AWS owner

Quando configura gli account per i nuovi membri del team che richiedono l'accesso a S3, il Account AWS proprietario può utilizzare AWS Identity and Access Management (IAM) per creare [utenti](#), gruppi e [ruoli](#). Il Account AWS proprietario può quindi condividere le risorse con queste identità IAM. Il proprietario dell'account può anche specificare le autorizzazioni da assegnare alle identità IAM, che consentono o negano le azioni che possono essere eseguite sulle risorse condivise.

Le identità IAM offrono maggiori funzionalità, tra cui la possibilità di richiedere agli utenti di inserire le credenziali di accesso prima di accedere alle risorse condivise. Utilizzando le identità IAM, è possibile implementare una forma di autenticazione a più fattori (MFA) per supportare una solida base di identità. Una best practice IAM consiste nel creare ruoli per la gestione degli accessi, invece di concedere autorizzazioni a ogni singolo utente. Si assegnano i singoli utenti al ruolo appropriato. Per ulteriori informazioni, consulta [Best practice per la sicurezza in IAM](#).

Altro AWS proprietari degli account e relative identità IAM (accesso tra account)

Il Account AWS proprietario può anche consentire ad altri titolari di AWS account, o identità IAM che appartengono a un altro AWS account, l'accesso alle risorse.

Note

Delega dei permessi - Se un Account AWS possiede una risorsa, può concedere tali permessi a un altro Account AWS. Tale account può quindi delegare tali autorizzazioni, o un sottoinsieme di esse, agli utenti dello stesso account. Si parla di delega del permesso. Ma un account che riceve permessi da un altro account non può delegare tali permessi "multi-account" a un altro Account AWS.

Utenti anonimi (accesso pubblico)

Il Account AWS proprietario può rendere pubbliche le risorse. Rendendo pubblica una risorsa, la si condivide tecnicamente con utente anonimo. I bucket creati da aprile 2023 bloccano tutti gli accessi pubblici per impostazione predefinita, a meno che non si modifichi questa impostazione. Si consiglia di impostare i bucket per bloccare l'accesso pubblico e di concedere l'accesso solo agli utenti autenticati. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Servizi AWS

Il proprietario della risorsa può concedere a un altro AWS servizio l'accesso a una risorsa Amazon S3. Ad esempio, puoi concedere al AWS CloudTrail servizio l'`s3:PutObject` autorizzazione a scrivere file di registro nel tuo bucket. Per ulteriori informazioni, vedi [Fornire l'accesso a un AWS servizio](#).

Identità di directory aziendali

Il proprietario della risorsa può concedere agli utenti o ai ruoli della directory aziendale l'accesso a una risorsa S3 utilizzando [S3 Access Grants](#). Per ulteriori informazioni sull'aggiunta della directory aziendale a Centro identità AWS IAM, consulta [Cos'è IAM Identity Center?](#).

Proprietari di bucket o risorse

Le Account AWS risorse utilizzate per creare bucket e caricare oggetti sono le proprietarie di tali risorse. Un proprietario del bucket può concedere a un altro Account AWS (o agli utenti di un altro account) autorizzazioni multiaccount per caricare gli oggetti.

Quando il proprietario di un bucket consente a un altro account di caricare oggetti in un bucket, il proprietario del bucket, per impostazione predefinita, è proprietario di tutti gli oggetti caricati nel suo bucket. Tuttavia, se entrambe le impostazioni del bucket applicate dal proprietario del bucket e quelle preferite dal proprietario del bucket sono disattivate, chi carica Account AWS gli oggetti possiede tali oggetti e il proprietario del bucket non dispone delle autorizzazioni sugli oggetti di proprietà di un altro account, con le seguenti eccezioni:

- È il proprietario del bucket a pagare la fattura. Il proprietario del bucket può rifiutare l'accesso agli oggetti nel bucket o eliminarli, indipendentemente dall'utente a cui appartengono.
- Il proprietario del bucket può archiviare qualsiasi oggetto o ripristinare gli oggetti archiviati, indipendentemente da chi ne sia il proprietario. Archiviazione si riferisce alla classe di storage utilizzata per memorizzare gli oggetti. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#).

Strumenti di gestione degli accessi

Amazon S3 offre una varietà di funzionalità e strumenti di sicurezza. Di seguito è riportato un elenco completo di queste funzioni e strumenti. Non è necessario disporre di tutti questi strumenti di gestione degli accessi, ma è necessario utilizzarne uno o più per concedere l'accesso alle risorse Amazon S3.

L'applicazione corretta di questi strumenti può aiutare a garantire che le risorse siano accessibili solo agli utenti previsti.

Lo strumento di gestione degli accessi più comunemente utilizzato è una policy di accesso. Una policy di accesso può essere una policy basata sulle risorse associata a una risorsa, ad esempio una policy bucket per un AWS bucket. Una policy di accesso può anche essere una policy basata sull'identità, collegata a un'identità AWS Identity and Access Management (IAM), come un utente, un gruppo o un ruolo IAM. Scrivi una policy di accesso per concedere a utenti, gruppi Account AWS e ruoli IAM il permesso di eseguire operazioni su una risorsa. Ad esempio, puoi concedere PUT Object l'autorizzazione a un altro account Account AWS in modo che l'altro account possa caricare oggetti nel tuo bucket.

Una policy di accesso descrive chi ha accesso a quali cose. Quando Amazon S3 riceve una richiesta, deve valutare tutte le policy di accesso per determinare se autorizzare o negare la richiesta. Per ulteriori informazioni su come Amazon S3 valuta le policy, consulta [In che modo Amazon S3 autorizza una richiesta](#).

Di seguito sono elencati gli strumenti di gestione degli accessi disponibili in Amazon S3.

Policy del bucket

Una policy sui bucket di Amazon S3 è una policy [basata sulle risorse JSON-formatted](#) AWS Identity and Access Management (IAM) collegata a un determinato bucket. Utilizza le politiche dei bucket per concedere altre autorizzazioni Account AWS o identità IAM per il bucket e gli oggetti in esso contenuti. Molti casi d'uso della gestione degli accessi S3 possono essere soddisfatti utilizzando una policy di bucket. Con le policy di bucket, è possibile personalizzare l'accesso ai bucket per assicurarsi che solo le identità approvate possano accedere alle risorse ed eseguire azioni al loro interno. Per ulteriori informazioni, consulta [Policy dei bucket per Amazon S3](#).

Di seguito è riportato un esempio di policy di bucket. La policy dei bucket è espressa da un file JSON. Questo esempio di policy concede a un ruolo IAM l'autorizzazione di lettura per tutti gli oggetti del bucket. Contiene un'istruzione denominata `BucketLevelReadPermissions`, che consente l'azione `s3:GetObject` (permesso di lettura) sugli oggetti di un bucket denominato `amzn-s3-demo-bucket1`. Specificando un ruolo IAM come `Principal`, questa policy consente l'accesso a qualsiasi utente IAM con questo ruolo. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BucketLevelReadPermissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-role"
      },
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    }
  ]
}
```

Note

Durante la creazione delle policy, è opportuno evitare l'uso di caratteri jolly (*) nell'elemento `Principal` perché questo consente a chiunque di accedere alle risorse Amazon S3. Invece, elencare esplicitamente gli utenti o i gruppi che possono accedere al bucket o elencare le condizioni che devono essere soddisfatte utilizzando una clausola di condizione nella policy. Inoltre, piuttosto che includere un carattere jolly per le azioni dei tuoi utenti o gruppi, concedete loro autorizzazioni specifiche, quando è il caso.

Identity-based policy

Una policy utente basata sull'identità o IAM è un tipo di [policy AWS Identity and Access Management \(IAM\)](#). Una policy basata sull'identità è una JSON-formatted policy allegata agli utenti, ai gruppi o ai ruoli IAM nel tuo account. AWS È possibile utilizzare le policy basate sull'identità per concedere a un'identità IAM l'accesso ai bucket o agli oggetti. È possibile creare utenti, gruppi e ruoli IAM nel proprio account e associare ad essi le policy di accesso. È quindi possibile concedere l'accesso alle risorse di AWS , comprese quelle di Amazon S3. Per ulteriori informazioni, consulta [Identity-based politiche per Amazon S3](#).

Di seguito è riportato un esempio di policy basata sull'identità. La policy di esempio consente al ruolo IAM associato di eseguire sei diverse azioni (autorizzazioni) di Amazon S3 su un bucket e

sugli oggetti in esso contenuti. Se si collega questa policy a un ruolo IAM dell'account e si assegna il ruolo ad alcuni utenti IAM, gli utenti con questo ruolo potranno eseguire queste azioni sulle risorse (bucket) specificate nella policy. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AssignARoleActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "AssignARoleActions2",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    }
  ]
}
```

Sovvenzioni di accesso S3

Utilizza S3 Access Grants per creare i permessi di accesso ai dati di Amazon S3 sia per le identità nelle directory di identità aziendali, come Active Directory, sia per le identità AWS Identity and Access Management (IAM). S3 Access Grants aiuta a gestire le autorizzazioni dei dati su scala. Inoltre, S3 Access Grants registra l'identità dell'utente finale e l'applicazione utilizzata per accedere ai dati S3 in

AWS CloudTrail. Questo fornisce una cronologia di audit dettagliata fino all'identità dell'utente finale per tutti gli accessi ai dati nei bucket S3. Per ulteriori informazioni, consulta [Gestione dell'accesso con S3 Access Grants](#).

Punti di accesso

Punti di accesso Amazon S3 semplifica la gestione dell'accesso ai dati su scala per le applicazioni che utilizzano set di dati condivisi su S3. I punti di accesso sono endpoint di rete denominati e collegati a un bucket. È possibile utilizzare i punti di accesso per eseguire operazioni sugli oggetti S3 in scala, come il caricamento e il recupero di oggetti. A un bucket possono essere collegati fino a 10.000 punti di accesso e per ogni punto di accesso è possibile applicare autorizzazioni e controlli di rete distinti per avere un controllo dettagliato sull'accesso agli oggetti S3. I punti di accesso S3 possono essere associati a bucket dello stesso account o di un altro account attendibile. Le policy dei punti di accesso sono policy basate sulle risorse che vengono valutate insieme alla policy di bucket sottostante. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

Lista di controllo degli accessi (ACL)

Una ACL è un elenco di concessioni che identifica il beneficiario e l'autorizzazione concessa. Le ACL concedono permessi di base di lettura o scrittura ad altri Account AWS. Le liste ACL utilizzano uno schema XML specifico di Amazon S3. Una ACL è un tipo di [policy AWS Identity and Access Management \(IAM\)](#). Una ACL per oggetti viene utilizzata per gestire l'accesso a un oggetto e una ACL per bucket viene utilizzata per gestire l'accesso a un bucket. Con le policy di bucket, esiste una singola policy per l'intero bucket, ma le ACL degli oggetti sono specificate per ciascun oggetto. È consigliabile mantenere le ACL disattivate, tranne in circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Per ulteriori informazioni sulle ACL, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Warning

La maggior parte dei casi d'uso moderni di Amazon S3 non richiede l'uso di ACL.

Di seguito è riportato un esempio di ACL del bucket. La concessione nell'ACL mostra il proprietario di un bucket che ha il permesso di controllo completo.

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
```

```
<Owner>
  <ID>Owner-Canonical-User-ID</ID>
</Owner>
<AccessControlList>
  <Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Canonical
User">
      <ID>Owner-Canonical-User-ID</ID>
    </Grantee>
    <Permission>FULL_CONTROL</Permission>
  </Grant>
</AccessControlList>
</AccessControlPolicy>
```

Proprietà dell'oggetto

Per gestire l'accesso ai propri oggetti, è necessario essere il proprietario dell'oggetto. È possibile utilizzare l'impostazione Proprietà oggetto a livello di bucket per controllare la proprietà degli oggetti caricati nel bucket. Inoltre, utilizzare la proprietà dell'oggetto per attivare le ACL. Per impostazione predefinita, la proprietà dell'oggetto è impostata sul proprietario del bucket e tutte le ACL sono disattivate. Quando le ACL sono disattivate, il proprietario del bucket possiede tutti gli oggetti del bucket e gestisce esclusivamente l'accesso ai dati. Per gestire l'accesso, il proprietario del bucket utilizza le policy o un altro strumento di gestione degli accessi, escluse le ACL. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Object Ownership ha tre impostazioni che possono essere utilizzate sia per controllare la proprietà degli oggetti caricati nel bucket, sia per attivare le ACL:

ACL disattivate

- Proprietario del bucket applicato (default) - Le ACL sono disattivate e il proprietario del bucket possiede automaticamente e ha il pieno controllo su ogni oggetto del bucket. Le ACL non influenzano le autorizzazioni ai dati nel bucket S3. Il bucket utilizza esclusivamente le policy per definire il controllo degli accessi.

ACL attivate

- Proprietario del bucket preferito - Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono sul bucket con l'ACL bucket-owner-full-control predefinita.

- Object writer – L' Account AWS che carica un oggetto lo possiede, ne ha il pieno controllo e può concedere ad altri utenti l'accesso tramite ACL.

Best practice aggiuntive

Considera l'utilizzo delle seguenti impostazioni e strumenti per i bucket per proteggere i dati in transito e a riposo, entrambi fondamentali per mantenere l'integrità e l'accessibilità dei tuoi dati:

- Blocca accesso pubblico - Non disattivare l'impostazione predefinita a livello di bucket Blocca accesso pubblico. Questa impostazione blocca per impostazione predefinita l'accesso pubblico ai tuoi dati. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).
- Controllo delle versioni S3 - Per garantire l'integrità dei dati, è possibile implementare l'impostazione di controllo delle versioni S3 per il bucket, che esegue il controllo della versione degli oggetti quando si effettuano gli aggiornamenti, invece di sovrascriverli. È possibile utilizzare il controllo delle versioni S3 per conservare, recuperare e ripristinare una versione precedente, se necessario. Per informazioni sulla funzione Controllo delle versioni S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).
- S3 Object Lock - S3 Object Lock è un'altra impostazione che si può implementare per ottenere l'integrità dei dati. Questa funzione può implementare un modello write-once-read-many (WORM) per memorizzare gli oggetti in modo immutabile. Per ulteriori informazioni sul blocco oggetti, consulta [Blocco di oggetti con Object Lock](#).
- Crittografia degli oggetti: Amazon S3 offre diverse opzioni di crittografia degli oggetti che proteggono i dati in transito e a riposo. Server-side la crittografia crittografa l'oggetto prima di salvarlo sui dischi dei suoi data center e quindi lo decrittografa quando scarichi gli oggetti. Se si autentica la richiesta e si dispone delle autorizzazioni di accesso, non c'è alcuna differenza nel modo in cui si accede agli oggetti crittografati o non crittografati. Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia lato server](#). S3 cripta gli oggetti appena caricati per impostazione predefinita. Per ulteriori informazioni, vedere. [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#) Client-side la crittografia è l'atto di crittografare i dati prima di inviarli ad Amazon S3. Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia lato client](#).
- Metodi di firma: la versione 4 di Signature è il processo di aggiunta di informazioni di autenticazione alle AWS richieste inviate tramite HTTP. Per motivi di sicurezza, la maggior parte delle richieste AWS deve essere firmata con una chiave di accesso, costituita da un ID della chiave di accesso e una chiave di accesso segreta. Queste due chiavi in genere vengono definite come le tue

credenziali di sicurezza. Per ulteriori informazioni, consulta [Autenticazione delle richieste \(AWS Signature versione 4\)](#) e Processo di [firma di Signature versione 4](#).

Azioni

Per un elenco completo delle autorizzazioni S3 e delle chiavi di condizione, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Azioni

Le azioni AWS Identity and Access Management (IAM) per Amazon S3 sono le possibili azioni che possono essere eseguite su un bucket o un oggetto S3. Si concedono queste azioni alle identità in modo che possano agire sulle risorse S3. Esempi di azioni S3 sono `s3:GetObject` per leggere oggetti in un bucket e `s3:PutObject` per scrivere oggetti in un bucket.

Chiavi di condizione

Oltre alle azioni, le chiavi di condizione IAM si limitano a concedere l'accesso solo quando è soddisfatta una condizione. Le chiavi di condizione sono opzionali.

Note

In una policy di accesso basata sulle risorse, come una policy di bucket, o in una policy basata sull'identità, è possibile specificare quanto segue:

- Un'azione o una serie di azioni nell'elemento `Action` dell'istruzione della policy.
- Nell'elemento `Effect` della istruzione di policy, è possibile specificare `Allow` per concedere le azioni elencate oppure `Deny` per bloccare le azioni elencate. Per mantenere ulteriormente la pratica dei privilegi minimi, le istruzioni `Deny` nell'elemento `Effect` della policy di accesso devono essere le più ampie possibile e le istruzioni `Allow` devono essere le più limitate possibile. Gli effetti `Deny` abbinati all'azione `s3:*` sono un altro buon modo per implementare le best practice di opt-in per le identità incluse nelle istruzioni sulla condizione delle policy.
- Una chiave di condizione nell'elemento `Condition` di un'istruzione di policy.

Casi d'uso della gestione degli accessi

Amazon S3 mette a disposizione dei proprietari delle risorse una serie di strumenti per concedere l'accesso. Lo strumento di gestione degli accessi S3 che si utilizza dipende dalle risorse S3 che si desidera condividere, dalle identità a cui si concede l'accesso e dalle azioni che si desidera consentire o negare. È possibile utilizzare uno o una combinazione di strumenti di gestione degli accessi S3 per gestire l'accesso alle risorse S3.

Nella maggior parte dei casi, è possibile utilizzare una policy di accesso per gestire le autorizzazioni. Una policy di accesso può essere una policy basata sulle risorse, collegata a una risorsa, come un bucket o un'altra risorsa Amazon S3 ([Risorse S3](#)). Una policy di accesso può anche essere una policy basata sull'identità, associata a un utente, gruppo o ruolo AWS Identity and Access Management (IAM) nel tuo account. È possibile che una policy di bucket sia più adatta al tuo caso d'uso. Per ulteriori informazioni, consulta [Policy dei bucket per Amazon S3](#). In alternativa, con AWS Identity and Access Management (IAM), puoi creare utenti, gruppi e ruoli IAM all'interno del tuo account Account AWS e gestire il loro accesso a bucket e oggetti tramite policy basate sull'identità. Per ulteriori informazioni, consulta [Identity-based politiche per Amazon S3](#).

Per aiutarti a orientarvi tra queste opzioni di gestione degli accessi, di seguito sono riportati i casi d'uso comuni dei clienti di Amazon S3 e le raccomandazioni per ciascuno degli strumenti di gestione degli accessi S3.

Il Account AWS il proprietario desidera condividere i bucket solo con utenti all'interno dello stesso account

Tutti gli strumenti di gestione degli accessi possono soddisfare questo caso d'uso di base. Per questo caso d'uso si consigliano i seguenti strumenti di gestione degli accessi:

- Policy di bucket - Se si desidera concedere l'accesso a un solo bucket o a un numero ridotto di bucket, oppure se le autorizzazioni di accesso al bucket sono simili da un bucket all'altro, utilizza una policy di bucket. Con le policy di bucket, si gestisce una policy per ogni bucket. Per ulteriori informazioni, consulta [Policy dei bucket per Amazon S3](#).
- Identity-based policy: se disponi di un numero molto elevato di bucket con autorizzazioni di accesso diverse per ogni bucket e solo pochi ruoli utente da gestire, puoi utilizzare una policy IAM per utenti, gruppi o ruoli. Le policy IAM sono anche una buona opzione se gestisci l'accesso degli utenti ad altre AWS risorse, oltre alle risorse Amazon S3. Per ulteriori informazioni, consulta [Esempio 1: il proprietario del bucket concede agli utenti le autorizzazioni per il bucket](#).

- **S3 Access Grants** - È possibile utilizzare S3 Access Grants per concedere l'accesso ai bucket, ai prefissi o agli oggetti S3. S3 Access Grants consente di specificare autorizzazioni variabili a livello di oggetto su scala, mentre le policy dei bucket sono limitate a 20 KB di dimensione. Per ulteriori informazioni, consulta [Nozioni di base su S3 Access Grants](#).
- **Punti di accesso** - È possibile utilizzare i punti di accesso, che sono endpoint di rete denominati e collegati a un bucket. A un bucket possono essere collegati fino a 10.000 punti di accesso e per ogni punto di accesso è possibile applicare autorizzazioni e controlli di rete distinti per avere un controllo dettagliato sull'accesso agli oggetti S3. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

Il Account AWS il proprietario desidera condividere bucket o oggetti con utenti di un altro AWS account (con più account)

Per concedere l'autorizzazione a un altro utente Account AWS, è necessario utilizzare una bucket policy o uno dei seguenti strumenti di gestione degli accessi consigliati. Non è possibile utilizzare un policy di accesso basata sull'identità per questo caso d'uso. Per ulteriori informazioni sulla concessione dell'accesso multi-account, consulta [Come si fornisce l'accesso a più account agli oggetti contenuti nei bucket Amazon S3?](#)

Per questo caso d'uso si consigliano i seguenti strumenti di gestione degli accessi:

- **Policy di bucket** - Con le policy di bucket, si gestisce una policy per ogni bucket. Per ulteriori informazioni, consulta [Policy dei bucket per Amazon S3](#).
- **S3 Access Grants** - Si possono usare gli S3 Access Grants per concedere autorizzazioni multi-account ai bucket, ai prefissi o agli oggetti S3. È possibile utilizzare S3 Access Grants per specificare autorizzazioni variabili a livello di oggetto su scala; mentre le policy dei bucket sono limitate a 20 KB di dimensione. Per ulteriori informazioni, consulta [Nozioni di base su S3 Access Grants](#).
- **Punti di accesso** - È possibile utilizzare i punti di accesso, che sono endpoint di rete denominati e collegati a un bucket. A un bucket possono essere collegati fino a 10.000 punti di accesso e per ogni punto di accesso è possibile applicare autorizzazioni e controlli di rete distinti per avere un controllo dettagliato sull'accesso agli oggetti S3. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

Il Account AWS il proprietario o il proprietario del bucket deve concedere le autorizzazioni a livello di oggetto o di prefisso e queste autorizzazioni variano da oggetto a oggetto o da prefisso a prefisso

In una policy di bucket, ad esempio, è possibile concedere l'accesso agli oggetti di un bucket che condividono un [prefisso specifico del nome della chiave](#) o che hanno un tag specifico. È possibile concedere l'autorizzazione di lettura agli oggetti che iniziano con il prefisso del nome della chiave logs/. Tuttavia, se le autorizzazioni di accesso variano in base all'oggetto, concedere le autorizzazioni ai singoli oggetti utilizzando una policy di bucket potrebbe non essere pratico, soprattutto perché le policy di bucket hanno dimensioni limitate a 20 KB.

Per questo caso d'uso si consigliano i seguenti strumenti di gestione degli accessi:

- S3 Access Grants - È possibile utilizzare S3 Access Grants per gestire le autorizzazioni a livello di oggetto o di prefisso. A differenza delle policy di bucket, è possibile utilizzare le policy di accesso S3 per specificare autorizzazioni variabili a livello di oggetto su scala. Le policy di bucket sono limitate a dimensioni di 20 KB. Per ulteriori informazioni, consulta [Nozioni di base su S3 Access Grants](#).
- Punti di accesso - È possibile utilizzare i punti di accesso per gestire le autorizzazioni a livello di oggetto o di prefisso. I punti di accesso sono endpoint di rete denominati e collegati a un bucket. A un bucket possono essere collegati fino a 10.000 punti di accesso e per ogni punto di accesso è possibile applicare autorizzazioni e controlli di rete distinti per avere un controllo dettagliato sull'accesso agli oggetti S3. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).
- ACL - Si sconsiglia l'uso di liste di controllo degli accessi (ACL), soprattutto perché le ACL sono limitate a 100 concessioni per oggetto. Tuttavia, se si sceglie di attivare le ACL, nelle impostazioni del bucket, impostare la proprietà dell'oggetto su Proprietario del bucket preferito e ACL abilitate. Con questa impostazione, nuovi oggetti scritti con l'ACL predefinita bucket-owner-full-control saranno automaticamente di proprietà del proprietario del bucket anziché dell'object writer. È quindi possibile utilizzare gli ACL degli oggetti, che sono una politica di accesso, per concedere ad altri utenti XML-formatted l'accesso all'oggetto. Per ulteriori informazioni, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

Il Account AWS il proprietario o il proprietario del bucket desidera limitare l'accesso al bucket solo a ID account specifici

Per questo caso d'uso si consigliano i seguenti strumenti di gestione degli accessi:

- Policy di bucket - Con le policy di bucket, si gestisce una policy per ogni bucket. Per ulteriori informazioni, consulta [Policy dei bucket per Amazon S3](#).
- Punti di accesso - I punti di accesso sono endpoint di rete denominati e collegati a un bucket. A un bucket possono essere collegati fino a 10.000 punti di accesso e per ogni punto di accesso è possibile applicare autorizzazioni e controlli di rete distinti per avere un controllo dettagliato sull'accesso agli oggetti S3. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

Il Account AWS il proprietario o il proprietario del bucket desidera endpoint distinti per ogni utente o applicazione che accede ai propri dati

Per questo caso d'uso si consiglia il seguente strumento di gestione degli accessi:

- Punti di accesso - I punti di accesso sono endpoint di rete denominati e collegati a un bucket. A un bucket possono essere collegati fino a 10.000 punti di accesso e per ogni punto di accesso è possibile applicare autorizzazioni e controlli di rete distinti per avere un controllo dettagliato sull'accesso agli oggetti S3. Ogni punto di accesso applica una policy personalizzata che funziona insieme alla policy di bucket collegata al bucket sottostante. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

Il Account AWS il proprietario o il proprietario del bucket deve gestire l'accesso dagli endpoint Virtual Private Cloud (VPC) per S3

Gli endpoint del cloud privato virtuale (VPC) per Amazon S3 sono entità logiche all'interno di un VPC che consentono la connettività solo a S3. Per questo caso d'uso si consigliano i seguenti strumenti di gestione degli accessi:

- Bucket in un'impostazione VPC - È possibile utilizzare una policy di bucket per controllare chi può accedere ai bucket e a quali endpoint VPC può accedere. Per ulteriori informazioni, consulta [Controllo dell'accesso dagli endpoint VPC con policy di bucket](#).
- Punto di accesso - Se si sceglie di impostare dei punti di accesso, è possibile utilizzare una policy dedicata. È possibile configurare qualsiasi punto di accesso in modo che accetti richieste solo da un cloud privato virtuale (VPC) per limitare l'accesso ai dati Amazon S3 a una rete privata. È inoltre possibile configurare impostazioni personalizzate di blocco dell'accesso pubblico per ciascun punto di accesso. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

Il Account AWS il proprietario o il proprietario del bucket deve rendere disponibile al pubblico un sito Web statico

Con S3 è possibile ospitare un sito web statico e consentire a chiunque di visualizzarne il contenuto, ospitato da un bucket S3.

Per questo caso d'uso si consigliano i seguenti strumenti di gestione degli accessi:

- **Amazon CloudFront:** questa soluzione consente di ospitare un sito Web statico Amazon S3 al pubblico continuando al contempo a bloccare tutti gli accessi pubblici ai contenuti di un bucket. Se desideri mantenere abilitate tutte e quattro le impostazioni di S3 Block Public Access e ospitare un sito Web statico S3, puoi utilizzare Amazon CloudFront origin access control (OAC). Amazon CloudFront fornisce le funzionalità necessarie per configurare un sito Web statico sicuro. Inoltre, i siti Web statici di Amazon S3 che non utilizzano questa soluzione possono supportare solo endpoint HTTP. CloudFront utilizza lo storage durevole di Amazon S3 fornendo al contempo intestazioni di sicurezza aggiuntive, come HTTPS. HTTPS aggiunge sicurezza crittografando una normale richiesta HTTP e proteggendo contro o più comuni attacchi informatici.

Per ulteriori informazioni, consulta [Getting started with a secure static website](#) nella Amazon CloudFront Developer Guide.

- **Rendere il proprio bucket Amazon S3 pubblicamente accessibile** - È possibile configurare un bucket per utilizzarlo come sito web statico ad accesso pubblico.

Warning

Non raccomandiamo questo metodo. Ti consigliamo invece di utilizzare i siti Web statici di Amazon S3 come parte di Amazon CloudFront. Per ulteriori informazioni, consulta l'opzione precedente o consulta [Come iniziare un sito web statico sicuro](#).

Per creare un sito Web statico di Amazon S3, senza Amazon CloudFront, devi prima disattivare tutte le impostazioni di Block Public Access. Durante la scrittura della policy del bucket per il sito Web statico, assicurati di consentire solo operazioni `s3:GetObject`, non autorizzazioni `ListObject` o `PutObject`. In questo modo si evita che gli utenti possano visualizzare tutti gli oggetti del bucket o aggiungere i propri contenuti. Per ulteriori informazioni, consulta [Impostazione delle autorizzazioni per l'accesso al sito Web](#).

Il Account AWS il proprietario o il proprietario del bucket desidera rendere il contenuto di un bucket disponibile al pubblico

Quando si crea un nuovo bucket Amazon S3, l'impostazione Blocca accesso pubblico è attivata per impostazione predefinita. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Si sconsiglia di consentire l'accesso pubblico al proprio bucket. Tuttavia, se è necessario farlo per un caso d'uso particolare, si consiglia il seguente strumento di gestione degli accessi per questo caso d'uso:

- Disabilita l'impostazione Blocca accesso pubblico - Il proprietario di un bucket può consentire richieste non autenticate al bucket. Ad esempio, le richieste [PUT Object](#) non autenticate sono consentite quando un bucket ha una policy di bucket pubblica o quando un'ACL del bucket consente l'accesso pubblico. Tutte le richieste non autenticate vengono effettuate da altri AWS utenti arbitrari o anche da utenti anonimi non autenticati. Questo utente viene rappresentato dall'ID utente canonico specifico 65a011a29cdf8ec533ec3d1ccaae921c nelle ACL. Se un oggetto viene caricato su WRITE o FULL_CONTROL, l'accesso viene concesso specificamente al gruppo Tutti gli utenti o all'utente anonimo. Per ulteriori informazioni sulle policy dei bucket pubblici e sulle liste di controllo degli accessi (ACL) pubbliche, consulta [Significato di "pubblico"](#).

Il Account AWS il proprietario o il proprietario del bucket ha superato i limiti di dimensione delle politiche di accesso

Sia le policy di bucket che quelle basate sull'identità hanno un limite di 20 KB. Se i requisiti di autorizzazione all'accesso sono complessi, si potrebbe superare questo limite di dimensione.

Per questo caso d'uso si consigliano i seguenti strumenti di gestione degli accessi:

- Punto di accesso - Utilizza i punti di accesso se questi funzionano con il tuo caso d'uso. Con i punti di accesso, ogni bucket ha più endpoint di rete denominati, ciascuno con la propria policy di punto di accesso che funziona con la policy di bucket sottostante. Tuttavia, i punti di accesso possono agire solo sugli oggetti, non sui bucket, e non supportano la replica tra Regioni. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).
- S3 Access Grants - Utilizza S3 Access Grants, che supporta un numero molto elevato di grant che danno accesso a bucket, prefissi o oggetti. Per ulteriori informazioni, consulta [Nozioni di base su S3 Access Grants](#).

Il Account AWS il ruolo di proprietario o amministratore desidera concedere l'accesso a bucket, prefisso o oggetto direttamente agli utenti o ai gruppi in una directory aziendale

Invece di gestire utenti, gruppi e ruoli tramite AWS Identity and Access Management (IAM), puoi aggiungere la tua directory aziendale a Centro identità AWS IAM. Per ulteriori informazioni, consulta [What is IAM Identity Center?](#).

Dopo aver aggiunto la directory aziendale a Centro identità AWS IAM, ti consigliamo di utilizzare il seguente strumento di gestione degli accessi per concedere alle identità delle directory aziendali l'accesso alle tue risorse S3:

- S3 Access Grants - Utilizza S3 Access Grants, che supporta la concessione dell'accesso a utenti o ruoli nella directory aziendale. Per ulteriori informazioni, consulta [Nozioni di base su S3 Access Grants](#).

Il Account AWS il proprietario o il proprietario del bucket desidera fornire il AWS CloudFront accesso al servizio per scrivere i CloudFront log su un bucket S3

Per questo caso d'uso abbiamo consigliato il seguente strumento di gestione degli accessi:

- Bucket ACL: l'unico caso d'uso consigliato per gli ACL dei bucket è concedere le autorizzazioni a determinati Servizi AWS account, come l'account Amazon. CloudFront `awslogsdelivery`. Quando crei o aggiorni una distribuzione e attivi la CloudFront registrazione, CloudFront aggiorna l'ACL del bucket per fornire all'`awslogsdelivery` account `FULL_CONTROL` le autorizzazioni per scrivere i log nel bucket. Per ulteriori informazioni, consulta [Autorizzazioni richieste per configurare la registrazione standard e per accedere ai file di registro nella Amazon Developer Guide](#). CloudFront Se il bucket che memorizza i log utilizza l'impostazione imposta dal proprietario del bucket per S3 Object Ownership per disattivare gli ACL, CloudFront non può scrivere i log nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

L'utente, in qualità di proprietario del bucket, vuole mantenere il pieno controllo degli oggetti aggiunti al bucket da altri utenti

È possibile concedere ad altri account l'accesso al caricamento di oggetti nel bucket utilizzando una policy di bucket, un punto di accesso o S3 Access Grants. Se si è concesso l'accesso multi-account

al proprio bucket, è possibile assicurarsi che tutti gli oggetti caricati nel bucket rimangano sotto il proprio controllo.

Per questo caso d'uso abbiamo consigliato il seguente strumento di gestione degli accessi:

- Proprietà dell'oggetto - Mantieni l'impostazione a livello di bucket Proprietà dell'oggetto all'impostazione predefinita Proprietario del bucket.

Risoluzione dei problemi di gestione degli accessi

Le seguenti risorse possono aiutare a risolvere eventuali problemi con la gestione degli accessi S3:

Risoluzione dei problemi relativi agli errori di accesso negato (403 Accesso negato)

Se si verificano problemi di rifiuto di accesso, controllare le impostazioni a livello di account e di bucket. Inoltre, verificare la funzionalità di gestione degli accessi utilizzata per concedere l'accesso per assicurarsi che la policy, l'impostazione o la configurazione siano corretti. Per ulteriori informazioni sulle cause più comuni degli errori di accesso negato (403 Accesso negato) in Amazon S3, consulta [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#).

IAM Access Analyzer per S3

Se non vuoi rendere pubbliche le tue risorse o se vuoi limitare l'accesso pubblico alle tue risorse, puoi usare IAM Access Analyzer for S3. Nella console di Amazon S3, utilizza IAM Access Analyzer for S3 per esaminare tutti i bucket che hanno liste di controllo degli accessi (ACL), policy o policy del punto di accesso che garantiscono l'accesso pubblico o condiviso. IAM Access Analyzer for S3 ti avvisa dei bucket configurati per consentire l'accesso a chiunque su Internet o altro, anche all'esterno della tua organizzazione. Account AWS Account AWS Per ogni bucket pubblico o condiviso, vengono visualizzati risultati che riportano l'origine e il livello di accesso pubblico o condiviso.

In IAM Access Analyzer per S3, è possibile bloccare tutti gli accessi pubblici a un bucket con una singola azione. Si consiglia di bloccare l'accesso pubblico ai propri bucket, a meno che non sia necessario per supportare un caso d'uso specifico. Prima di bloccare tutti gli accessi pubblici, accertati che le tue applicazioni continuino a funzionare correttamente anche senza accesso pubblico. Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

È inoltre possibile rivedere le impostazioni dei permessi a livello di bucket per configurare livelli di accesso dettagliati. Per casi d'uso specifici e verificati che richiedono l'accesso pubblico o condiviso, puoi confermare e registrare l'intenzione del bucket di rimanere pubblico o condiviso archiviando

i risultati per il bucket. Puoi consultare e modificare le configurazioni relative al bucket in qualsiasi momento. È inoltre possibile scaricare i risultati in un report CSV per scopi di verifica.

IAM Access Analyzer per S3 è disponibile senza costi aggiuntivi nella console di Amazon S3. IAM Access Analyzer per S3 è basato su AWS Identity and Access Management (IAM) IAM Access Analyzer. Per utilizzare IAM Access Analyzer for S3 sulla console Amazon S3, è necessario visitare la [Console IAM](#) e creare un analizzatore a livello di account in IAM Access Analyzer per ogni singola Regione.

Per ulteriori informazioni su IAM Access Analyzer per S3, consultare [Revisione dell'accesso al bucket tramite IAM Access Analyzer per S3](#).

Registrazione di log e monitoraggio

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità e delle prestazioni delle soluzioni Amazon S3 in modo da poter eseguire più facilmente il debug di un errore di accesso. La registrazione può fornire informazioni su eventuali errori ricevuti dagli utenti e su quando e quali richieste vengono effettuate. AWS fornisce diversi strumenti per monitorare le risorse di Amazon S3, come i seguenti:

- AWS CloudTrail
- Log di accesso Amazon S3
- AWS Trusted Advisor
- Amazon CloudWatch

Per ulteriori informazioni, consulta [Registrazione e monitoraggio in Amazon S3](#).

Identity and Access Management per Amazon S3

AWS Identity and Access Management (IAM) è una soluzione Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (può accedere) e autorizzato (dispone di autorizzazioni) a utilizzare le risorse Amazon S3. IAM è un programma Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

 Note

Per ulteriori informazioni sull'uso della classe di storage Amazon S3 Express One Zone con i bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come funziona Amazon S3 con IAM](#)
- [In che modo Amazon S3 autorizza una richiesta](#)
- [Autorizzazioni necessarie per le operazioni API di Amazon S3](#)
- [Policy e autorizzazioni in Amazon S3](#)
- [Policy dei bucket per Amazon S3](#)
- [Identity-based politiche per Amazon S3](#)
- [Passaggi che utilizzano le policy per gestire l'accesso alle risorse Amazon S3](#)
- [Utilizzo dei ruoli collegati ai servizi per Amazon S3 Storage Lens](#)
- [Risoluzione dei problemi di identità e accesso ad Amazon S3](#)
- [AWS politiche gestite per Amazon S3](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi di identità e accesso ad Amazon S3](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come funziona Amazon S3 con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta [Identity-based politiche per Amazon S3](#))

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali da una fonte di identità come Centro identità AWS IAM (IAM Identity Center), autenticazione Single Sign-on o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando ne crei uno Account AWS, inizi con un'identità di accesso chiamata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

È consigliabile richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità web o Directory Service che accede Servizi AWS utilizzando credenziali da una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare Centro identità AWS IAM. Per ulteriori informazioni, consulta [Che cos'è il Centro identità IAM?](#) nella Guida per l'utente di Centro identità AWS IAM .

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la](#)

[federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella IAM User Guide.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS API AWS CLI or. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un principale effettua una richiesta. La maggior parte delle policy sono archiviate AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Identity-based politiche

Identity-based le policy sono documenti relativi alle politiche di autorizzazione JSON che si allegano a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare

una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Identity-based le politiche possono essere politiche in linea (incorporate direttamente in una singola identità) o politiche gestite (politiche autonome associate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Resource-based politiche

Resource-based le policy sono documenti di policy JSON che alleggi a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Resource-based le policy sono policy in linea che si trovano in quel servizio. Non è possibile utilizzare le policy AWS gestite da IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): specifica il numero massimo di autorizzazioni per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- Policy di controllo delle risorse (RCP): imposta le autorizzazioni massime disponibili per le risorse degli account. Per ulteriori informazioni, consulta [Policy di controllo delle risorse \(RCP\)](#) nella Guida per l'utente di AWS Organizations .
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle [policy](#) nella IAM User Guide.

Come funziona Amazon S3 con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon S3, è necessario conoscere le funzioni IAM disponibili per l'utilizzo di Amazon S3.

Funzioni IAM utilizzabili con Amazon S3

Funzionalità IAM	Supporto Amazon S3
Identity-based politiche	Sì
Resource-based politiche	Sì
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	Sì
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Service-linked ruoli	Parziale

Per avere una visione generale di come Amazon S3 e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta [AWS i servizi che funzionano con IAM](#) nella IAM User Guide.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Identity-based politiche per Amazon S3

Supporta le policy basate sull'identità: sì

Identity-based le policy sono documenti di policy sulle autorizzazioni JSON che puoi allegare a un'identità, ad esempio un utente, un gruppo di utenti o un ruolo IAM. Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

Identity-based esempi di policy per Amazon S3

Per visualizzare esempi di policy basate sull'identità di Amazon S3, consulta [Identity-based politiche per Amazon S3](#).

Resource-based politiche all'interno di Amazon S3

Supporta le policy basate sulle risorse: sì

Resource-based le policy sono documenti di policy JSON che alleggi a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#). I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Il servizio Amazon S3 supporta le policy di bucket, le policy di punto di accesso e le concessioni di accesso:

- Le policy di bucket sono policy basate sulle risorse e collegate a un bucket Amazon S3. Una policy di bucket definisce quali sono i principali che possono eseguire azioni sul bucket.
- Le policy dei punti di accesso sono policy basate sulle risorse che vengono valutate insieme alla policy di bucket sottostante.
- I permessi di accesso sono un modello semplificato per definire le autorizzazioni di accesso ai dati in Amazon S3 per prefisso, bucket o oggetto. Per informazioni su S3 Access Grants, consulta [Gestione dell'accesso con S3 Access Grants](#).

Principali per le policy dei bucket

L'elemento `Principal` specifica l'utente, l'account, il servizio o un'altra entità a cui è consentito o negato l'accesso a una risorsa. Di seguito vengono illustrati alcuni esempi di specifica del `Principal`. Per ulteriori informazioni, consulta [Principali](#) nella Guida per l'utente di IAM.

Concedi le autorizzazioni a un Account AWS

Per concedere le autorizzazioni a un Account AWS, identifica l'account utilizzando il seguente formato.

```
"AWS": "account-ARN"
```

Di seguito vengono mostrati gli esempi.

```
"Principal": {"AWS": "arn:aws:iam::AccountIDWithoutHyphens:root"}
```

```
"Principal": {"AWS":  
["arn:aws:iam::AccountID1WithoutHyphens:root", "arn:aws:iam::AccountID2WithoutHyphens:root"]}
```

Note

Gli esempi precedenti forniscono le autorizzazioni all'utente root, che delega le autorizzazioni a livello di account. Tuttavia, le policy IAM sono ancora necessarie per i ruoli e gli utenti specifici dell'account.

Concessione delle autorizzazioni a un utente IAM

Per concedere l'autorizzazione a un utente IAM nel tuo account, devi fornire una coppia nome-valore "AWS": "*user-ARN*".

```
"Principal":{"AWS":"arn:aws:iam::account-number-without-hyphens:user/username"}
```

Per esempi dettagliati che forniscono istruzioni dettagliate, consulta [Esempio 1: il proprietario del bucket concede agli utenti le autorizzazioni per il bucket](#) e [Esempio 3: il proprietario del bucket concede autorizzazioni per gli oggetti che non sono di sua proprietà](#).

Note

Se un'identità IAM viene eliminata dopo aver aggiornato la policy del bucket, la policy del bucket mostrerà un identificatore univoco nell'elemento principale anziché un ARN. Questi ID univoci non vengono mai riutilizzati, quindi puoi rimuovere in sicurezza i principali con identificatori univoci da tutte le dichiarazioni di policy. Per ulteriori informazioni sugli identificatori unici, consulta [Identificatori IAM](#) nella Guida per l'utente di IAM.

Concessione di autorizzazioni anonime

Warning

Si deve prestare attenzione a concedere l'accesso anonimo al proprio bucket Amazon S3. Quando si concede l'accesso anonimo, si consente a qualsiasi persona al mondo di accedere al bucket. È consigliabile non concedere mai alcun tipo di accesso anonimo in scrittura al bucket S3.

Per assegnare l'autorizzazione a tutti, vale a dire l'accesso anonimo, è necessario impostare i caratteri jolly ("*") come valore `Principal`. Ad esempio, se si configura un bucket come un sito Web, si vuole che tutti gli oggetti presenti nel bucket siano pubblicamente accessibili.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

L'utilizzo "Principal": "*" con Allow effetto in una politica basata sulle risorse consente a chiunque, anche se non ha effettuato l'accesso AWS, di accedere alla risorsa.

L'utilizzo di "Principal" : { "AWS" : "*" } con un effetto Allow in una policy basata sulle risorse consente a qualsiasi utente root, utente IAM, sessione del ruolo assunto o utente federato in qualsiasi account nella stessa partizione di accedere alla tua risorsa.

Per gli utenti anonimi, questi due metodi sono equivalenti. Per ulteriori informazioni, consulta [Tutti i principali](#) nella Guida per l'utente di IAM.

Non è possibile utilizzare un carattere jolly per associare parte di un nome di un principale o di un ARN.

Important

Nelle politiche di controllo degli AWS accessi, i Principal «*» e {» «:AWS«*"} si comportano in modo identico.

Limitazione delle autorizzazioni per le risorse

Puoi anche utilizzare la policy delle risorse per limitare l'accesso a risorse che altrimenti sarebbero disponibili per i principali IAM. Usa un'istruzione Deny per impedire l'accesso.

L'esempio seguente blocca l'accesso se non viene utilizzato un protocollo di trasporto sicuro:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyBucketAccessIfSTPNotUsed",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
  ]  
}
```

Utilizzare il "Principal": "*" in modo che questa restrizione si applichi a tutti è una best practice, anziché tentare di negare l'accesso solo a account o principali specifici utilizzando questo metodo.

Richiedi l'accesso tramite URL CloudFront

Puoi richiedere che i tuoi utenti accedano ai tuoi contenuti Amazon S3 solo utilizzando gli CloudFront URL anziché gli URL di Amazon S3. A tale scopo, crea un controllo di accesso all' CloudFront origine (OAC). Quindi, modifica le autorizzazioni sui dati S3. Nella tua politica bucket, puoi impostare CloudFront come Principal come segue:

```
"Principal":{"Service":"cloudfront.amazonaws.com"}
```

Utilizza un Condition elemento nella policy per consentire l'accesso CloudFront al bucket solo quando la richiesta è per conto della CloudFront distribuzione che contiene l'origine S3.

```
  "Condition": {  
    "StringEquals": {  
      "AWS:SourceArn":  
        "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"  
    }  
  }
```

Per ulteriori informazioni sulla richiesta di accesso a S3 tramite CloudFront URL, consulta [Restricting access to an Amazon Simple Storage Service origin](#) nella Amazon Developer Guide.

Per ulteriori informazioni sui vantaggi in termini di sicurezza e privacy derivanti dall'utilizzo di Amazon CloudFront, consulta [Configurare l'accesso sicuro e limitare l'accesso ai contenuti](#).

Resource-based esempi di policy per Amazon S3

- Per visualizzare esempi di policy per i bucket Amazon S3, consulta [Policy dei bucket per Amazon S3](#).

- Per visualizzare esempi di policy per i punti di accesso, consulta [Configurazione delle policy IAM per l'utilizzo degli access point](#).

Azioni di policy per Amazon S3

Supporta le operazioni di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Di seguito sono illustrati diversi tipi di relazione di mappatura tra le operazioni API S3 e le azioni di policy richieste.

- One-to-one mappatura con lo stesso nome. Ad esempio, per utilizzare l'operazione API `PutBucketPolicy`, è necessaria l'azione di policy `s3:PutBucketPolicy`.
- One-to-one mappatura con nomi diversi. Ad esempio, per utilizzare l'operazione API `ListObjectsV2`, è necessaria l'azione di policy `s3:ListBucket`.
- One-to-many mappatura. Ad esempio, per utilizzare l'operazione API `HeadObject`, è necessaria l'operazione `s3:GetObject`. Inoltre, quando si utilizza S3 Object Lock e si desidera ottenere lo stato di conservazione legale di un oggetto o le impostazioni di conservazione, prima di poter utilizzare l'operazione API `HeadObject` sono necessarie anche le azioni di policy `s3:GetObjectLegalHold` o `s3:GetObjectRetention` corrispondenti.
- Many-to-one mappatura. Ad esempio, per utilizzare le operazioni API `ListObjectsV2` o `HeadBucket`, è necessaria l'azione di policy `s3:ListBucket`.

Per visualizzare un elenco di azioni Amazon S3 da utilizzare nelle policy, consulta [Azioni definite da Amazon S3](#) in Riferimento alle autorizzazioni di servizio. Per un elenco completo delle operazioni API di Amazon S3, consulta [Azioni API di Amazon S3](#) in Riferimento API di Amazon Simple Storage Service.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Le azioni di policy in Amazon S3 utilizzano il seguente prefisso prima dell'azione:

```
s3
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
    "s3:action1",  
    "s3:action2"  
]
```

Operazioni relative ai bucket

Le operazioni sui bucket sono operazioni API S3 che operano sul tipo di risorsa bucket. For example: CreateBucket, ListObjectsV2 e PutBucketPolicy. Le azioni di policy S3 per le operazioni sui bucket richiedono che l'elemento Resource nelle policy sui bucket o nelle policy basate sull'identità IAM sia l'identificatore nome della risorsa Amazon (ARN) del tipo di bucket S3 nel seguente formato di esempio.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
```

La seguente policy di bucket concede all'utente *Akua* con l'account *12345678901* l'autorizzazione s3:ListBucket per eseguire l'operazione [ListObjectsV2](#) e di elencare gli oggetti in un bucket S3.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "Allow Akua to list objects in the bucket",  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::111122223333:user/Akua"  
      },  
      "Action": [  
        "s3:ListBucket"  
      ],  
    },  
  ],  
}
```

```

    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
  }
]
}

```

Operazioni su bucket nelle policy per i punti di accesso di bucket per uso generico

Le autorizzazioni fornite in un punto di accesso per una policy di bucket per uso generico sono efficaci solo se il bucket sottostante consente le stesse autorizzazioni. Quando si utilizzano i punti di accesso S3, è necessario delegare il controllo dell'accesso dal bucket al punto di accesso o aggiungere le stesse autorizzazioni nelle policy dei punti di accesso alle policy del bucket sottostante. Per ulteriori informazioni, consulta [Configurazione delle policy IAM per l'utilizzo degli access point](#). Nelle policy dei punti di accesso, le azioni delle policy S3 per le operazioni sui bucket richiedono l'utilizzo dell'ARN del punto di accesso per l'elemento Resource nel seguente formato.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

La seguente policy del punto di accesso concede all'utente *Akua* con l'account *12345678901* il permesso `s3:ListBucket` di eseguire l'operazione API [ListObjectsV2](#) attraverso il punto di accesso S3 denominato *example-access-point*. Questo permesso consente a *Akua* di elencare gli oggetti nel bucket associato a *example-access-point*.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAkuaToListObjectsInBucketThroughAccessPoint",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Akua"
      },
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:us-west-2:111122223333:accesspoint/example-access-point"
    }
  ]
}

```

```
]
}
```

Note

Non tutte le operazioni di bucket sono supportate dai punti di accesso di bucket per uso generico. Per ulteriori informazioni, consulta [Compatibilità dei punti di accesso con le operazioni S3](#).

Operazioni su bucket nelle policy per i punti di accesso di bucket di directory

Le autorizzazioni fornite in un punto di accesso per una policy di bucket di directory sono efficaci solo se il bucket sottostante consente le stesse autorizzazioni. Quando si utilizzano i punti di accesso S3, è necessario delegare il controllo dell'accesso dal bucket al punto di accesso o aggiungere le stesse autorizzazioni nelle policy dei punti di accesso alle policy del bucket sottostante. Per ulteriori informazioni, consulta [Configurazione delle policy IAM per l'utilizzo dei punti di accesso per i bucket di directory](#). Nelle policy dei punti di accesso, le azioni delle policy S3 per le operazioni sui bucket richiedono l'utilizzo dell'ARN del punto di accesso per l'elemento Resource nel seguente formato.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
```

La seguente policy di punto di accesso fornisce all'utente *Akua* con l'account *12345678901* l'autorizzazione `s3:ListBucket` per eseguire l'operazione API [ListObjectsV2](#) attraverso il punto di accesso denominato *example-access-point--usw2-az1--xa-s3*. Questo permesso consente a *Akua* di elencare gli oggetti nel bucket associato a *example-access-point--usw2-az1--xa-s3*.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAkuaToListObjectsInTheBucketThroughAccessPoint",
      "Effect": "Allow",
      "Principal": {
```

```

        "AWS": "arn:aws:iam::111122223333:user/Akua"
      },
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3express:us-east-1:111122223333:accesspoint/
example-access-point-usw2-az1-xa-s3"
    }
  ]
}

```

Note

Non tutte le operazioni di bucket sono supportate dai punti di accesso di bucket di directory. Per ulteriori informazioni, consulta [Operazioni sugli oggetti per i punti di accesso di bucket di directory](#).

Operazioni con gli oggetti

Le operazioni sugli oggetti sono operazioni API S3 che agiscono sul tipo di risorsa oggetto. For example: `GetObject`, `PutObject` e `DeleteObject`. Le azioni delle policy S3 per le operazioni sugli oggetti richiedono che l'elemento `Resource` nelle policy sia l'ARN dell'oggetto S3 nei seguenti formati di esempio.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
```

Note

L'ARN dell'oggetto deve contenere una barra in avanti dopo il nome del bucket, come visto negli esempi precedenti.

La seguente policy del bucket concede all'utente *Akua* con l'account *12345678901* l'autorizzazione `s3:PutObject`. Questa autorizzazione consente a *Akua* di utilizzare l'operazione [PutObject](#) per caricare oggetti nel bucket S3 denominato *amzn-s3-demo-bucket*.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow Akua to upload objects",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Akua"
      },
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3::amzn-s3-demo-bucket/*"
    }
  ]
}
```

Operazioni sugli oggetti nelle policy dei punti di accesso

Quando si utilizzano i punti di accesso S3 per controllare l'accesso alle operazioni sugli oggetti, è possibile utilizzare le policy dei punti di accesso. Quando si utilizzano le policy dei punti di accesso, le azioni delle policy S3 per le operazioni sugli oggetti richiedono l'utilizzo dell'ARN del punto di accesso per l'elemento Resource nel seguente formato: `arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource`. Per le operazioni sugli oggetti che utilizzano punti di accesso, è necessario includere il valore `/object/` dopo l'intero ARN del punto di accesso nell'elemento Resource. Ecco alcuni esempi.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/*"
```

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/prefix/*"
```

La seguente policy del punto di accesso concede all'utente *Akua* con l'account *12345678901* l'autorizzazione `s3:GetObject`. Questa autorizzazione consente a *Akua* di eseguire l'operazione [GetObject](#) attraverso il punto di accesso denominato *example-access-point* su tutti gli oggetti del bucket associato al punto di accesso.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow Akua to get objects through access point",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Akua"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-access-point/object/*"
    }
  ]
}
```

 Note

Non tutte le operazioni sugli oggetti sono supportate dai punti di accesso. Per ulteriori informazioni, consulta [Compatibilità dei punti di accesso con le operazioni S3](#).

Operazioni su oggetti nelle policy per i punti di accesso di bucket di directory

Quando si utilizzano i punti di accesso di bucket di directory per controllare l'accesso alle operazioni degli oggetti, è possibile utilizzare le policy di punti di accesso. Quando si utilizzano le policy dei punti di accesso, le azioni delle policy S3 per le operazioni sugli oggetti richiedono l'utilizzo dell'ARN del punto di accesso per l'elemento Resource nel seguente formato: `arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource`. Per le operazioni sugli oggetti che utilizzano punti di accesso, è necessario includere il valore `/object/` dopo l'intero ARN del punto di accesso nell'elemento Resource. Ecco alcuni esempi.

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
```

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/prefix/*"
```

La seguente policy del punto di accesso concede all'utente *Akua* con l'account *12345678901* l'autorizzazione `s3:GetObject`. Questa autorizzazione consente a *Akua* di eseguire l'operazione [GetObject](#) attraverso il punto di accesso denominato *example-access-point--usw2-az1--xa-s3* su tutti gli oggetti del bucket associato al punto di accesso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow Akua to get objects through access point",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::12345678901:user/Akua"
      },
      "Action": "s3express:CreateSession","s3:GetObject"
      "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
    }
  ]
}
```

Note

Non tutte le operazioni di oggetti sono supportate dai punti di accesso di bucket di directory. Per ulteriori informazioni, consulta [Operazioni sugli oggetti per i punti di accesso di bucket di directory](#).

Operazioni sui punti di accesso di bucket per uso generico

Le operazioni sui punti di accesso sono operazioni API S3 che operano sul tipo di risorsa `accesspoint`. For example: `CreateAccessPoint`, `DeleteAccessPoint` e `GetAccessPointPolicy`. Le azioni delle policy S3 per le operazioni sui punti di accesso possono essere utilizzate solo nelle policy IAM basate sull'identità, non nelle policy di bucket o punti di accesso. Le operazioni sui punti di accesso richiedono che l'elemento `Resource` sia l'ARN del punto di accesso nel seguente formato di esempio.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

La seguente policy IAM basata sull'identità concede all'indirizzo `s3:GetAccessPointPolicy` il permesso di eseguire l'operazione [GetAccessPointPolicy](#) sul punto di accesso S3 denominato *example-access-point*.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
"GrantPermissionToRetrieveTheAccessPointPolicyOfAccessPointExampleAccessPoint",
      "Effect": "Allow",
      "Action": [
        "s3:GetAccessPointPolicy"
      ],
      "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-
point"
    }
  ]
}
```

Quando si usano i punti di accesso, per controllare l'accesso alle operazioni sui bucket, consulta [Operazioni su bucket nelle policy per i punti di accesso di bucket per uso generico](#); per controllare l'accesso alle operazioni sugli oggetti, consulta [Operazioni sugli oggetti nelle policy dei punti di accesso](#). Per ulteriori informazioni su come configurare le policy dei punti di accesso, consulta [Configurazione delle policy IAM per l'utilizzo degli access point](#).

Operazioni sui punti di accesso di bucket di directory

Le operazioni sui punti di accesso di bucket di directory sono operazioni API S3 che operano sul tipo di risorsa `accesspoint`. For example: `CreateAccessPoint`, `DeleteAccessPoint` e `GetAccessPointPolicy`. Le azioni delle policy S3 per le operazioni sui punti di accesso possono essere utilizzate solo nelle policy IAM basate sull'identità, non nelle policy di bucket o punti di accesso. Le operazioni sui punti di accesso di bucket di directory richiedono che l'elemento `Resource` sia l'ARN del punto di accesso nel seguente formato di esempio.


```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
```

La seguente policy IAM basata su identità fornisce l'autorizzazione `s3express:GetAccessPointPolicy` per eseguire l'operazione API [GetAccessPointPolicy](#) sul punto di accesso denominato `example-access-point--usw2-az1--xa-s3`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
"GrantPermissionToRetrieveTheAccessPointPolicyOfAccessPointExampleAccessPointUsw2Az1XaS3",
      "Effect": "Allow",
      "Action": [
        "s3express:CreateSession", "s3express:GetAccessPointPolicy"
      ],
      "Resource": "arn:aws:s3:*:111122223333:accesspoint/example-access-
point"
    }
  ]
}
```

La seguente policy IAM basata su identità fornisce l'autorizzazione `s3express:CreateAccessPoint` per creare un punto di accesso di bucket di directory.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Grant CreateAccessPoint.",
      "Principal": "*",
      "Action": "s3express:CreateSession",
      "s3express:CreateAccessPoint": {
        "Effect": "Allow",
        "Resource": "*"
      }
    }
  ]
}
```

```
}
```

La seguente policy IAM basata su identità fornisce l'autorizzazione `s3express:PutAccessPointScope` per creare un ambito del punto di accesso di bucket di directory.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Grant PutAccessPointScope",
      "Principal": "*",
      "Action": "s3express:CreateSession",
      "s3express:CreateAccessPoint",
      "S3Express:PutAccessPointScope": { "Effect": "Allow" },
      "Resource": "*"
    }
  ]
}
```

Quando si utilizzano i punti di accesso di bucket di directory per controllare l'accesso alle operazioni sui bucket, consulta [Operazioni su bucket nelle policy per i punti di accesso di bucket di directory](#) e per controllare l'accesso alle operazioni sugli oggetti, consulta [Operazioni su oggetti nelle policy per i punti di accesso di bucket di directory](#). Per ulteriori informazioni su come configurare le policy di punti di accesso di bucket di directory, consulta [Configurazione delle policy IAM per l'utilizzo dei punti di accesso per i bucket di directory](#).

Operazioni sui punti di accesso Lambda per oggetti

Con Lambda per oggetti Amazon S3, è possibile aggiungere il proprio codice alle richieste di Amazon S3 GET, LIST e HEAD per modificare ed elaborare i dati mentre vengono restituiti a un'applicazione. È possibile effettuare richieste attraverso un punto di accesso Lambda per oggetti, che funziona come le richieste attraverso altri punti di accesso. Per ulteriori informazioni, consulta [Trasformazione di oggetti con S3 Object Lambda](#).

Per ulteriori informazioni su come configurare le policy per le operazioni sui punti di accesso Lambda per oggetti, consulta [Configurazione delle policy IAM per i punti di accesso Lambda per oggetti](#).

Multi-Region Operazioni con gli Access Point

Un Multi-Region Access Point fornisce un endpoint globale che le applicazioni possono utilizzare per soddisfare le richieste provenienti da bucket S3 che si trovano in più blocchi. Regione AWS È possibile utilizzare un Multi-Region Access Point per creare applicazioni multiregionali con la stessa architettura utilizzata in una singola regione e quindi eseguire tali applicazioni in qualsiasi parte del mondo. Per ulteriori informazioni, consulta [Gestione del traffico multiregionale con punti di Multi-Region accesso](#).

Per ulteriori informazioni su come configurare le politiche per le operazioni Multi-Region degli Access Point, vedere [Multi-Region Esempi di politiche relative agli Access Point](#).

Operazioni di processo in batch

(Operazioni in batch) Le operazioni di processo sono operazioni API S3 che operano sul tipo di risorsa di processo, Ad esempio DescribeJob e CreateJob. Le azioni delle policy S3 per le operazioni di processo possono essere utilizzate solo nelle policy basate sull'identità IAM, non nelle policy dei bucket. Inoltre, le operazioni di processo richiedono che l'elemento Resource nelle policy basate sull'identità IAM sia l'ARN di job nel seguente formato di esempio.

```
"Resource": "arn:aws:s3:*:123456789012:job/*"
```

La seguente policy IAM basata sull'identità concede l'`s3:DescribeJob` autorizzazione a eseguire l'operazione [DescribeJob](#) API sul job S3 Batch Operations denominato. *example-job*

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribingBatchOperationJob",
      "Effect": "Allow",
      "Action": [
        "s3:DescribeJob"
      ],
      "Resource": "arn:aws:s3:*:111122223333:job/example-job"
    }
  ]
}
```

Operazioni di configurazione dell'Storage Lens S3

Per ulteriori informazioni su come configurare le operazioni di configurazione di S3 Storage Lens, consulta [Impostazione delle autorizzazioni di Amazon S3 Storage Lens](#).

Operazioni sugli account

Le operazioni sugli account sono operazioni API S3 che operano a livello di account, ad esempio `GetPublicAccessBlock` (per account). L'account non è un tipo di risorsa definito da Amazon S3. Le azioni delle policy S3 per le operazioni sugli account possono essere utilizzate solo nelle policy basate sull'identità IAM, non nelle policy dei bucket. Inoltre, le operazioni sugli account richiedono che l'elemento `Resource` nelle policy IAM basate sull'identità sia `"*"`.

La seguente policy IAM basata sull'identità concede all'indirizzo `s3:GetAccountPublicAccessBlock` l'autorizzazione a eseguire l'operazione API a livello di account e a recuperare le impostazioni del blocco di accesso pubblico a livello di account [GetPublicAccessBlock](#) e recuperare le impostazioni del blocco di accesso pubblico a livello di account.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRetrievingTheAccountLevelPublicAccessBlockSettings",
      "Effect": "Allow",
      "Action": [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Esempi di policy per Amazon S3

- Per visualizzare esempi di policy basate sull'identità di Amazon S3, consulta [Identity-based politiche per Amazon S3](#).
- Per visualizzare esempi di policy basate sulle risorse di Amazon S3, consulta [Policy dei bucket per Amazon S3](#) e [Configurazione delle policy IAM per l'utilizzo degli access point](#).

Risorse di policy per Amazon S3

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*" 
```

Alcune azioni API di Amazon S3 supportano più risorse. Ad esempio, `s3:GetObject` accede a *example-resource-1* e *example-resource-2*, quindi un principale deve avere i permessi per accedere a entrambe le risorse. Per specificare più risorse in una singola istruzione, separa gli ARN con delle virgole, come mostrato nell'esempio seguente.

```
"Resource": [
    "example-resource-1",
    "example-resource-2" ]
```

Le risorse in Amazon S3 sono bucket, oggetti, punti di accesso o processi. In una policy, utilizzare il nome della risorsa Amazon (ARN) del bucket, dell'oggetto, del punto di accesso o del processo per identificare la risorsa.

Per un elenco completo dei tipi di risorse Amazon S3 e dei relativi ARN, consulta [Risorse definite da Amazon S3](#) nel Riferimento alle autorizzazioni di servizio. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta [Azioni definite da Amazon S3](#).

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Caratteri jolly negli ARN delle risorse

È possibile utilizzare caratteri jolly come parte dell'ARN della risorsa. È possibile utilizzare i caratteri jolly (* e ?) all'interno di qualsiasi segmento ARN (le parti separate dai due punti). Un asterisco (*) rappresenta qualsiasi combinazione di zero o più caratteri, mentre un punto interrogativo (?) rappresenta qualsiasi singolo carattere. È possibile utilizzare più caratteri * o ? in ogni segmento. Tuttavia, un carattere jolly non può essere esteso a più segmenti.

- Il seguente ARN utilizza il carattere jolly * nella parte `relative-ID` dell'ARN per identificare tutti gli oggetti nel bucket *amzn-s3-demo-bucket*.

```
arn:aws:s3:::amzn-s3-demo-bucket/*
```

- Il seguente ARN utilizza * per indicare tutti i bucket e gli oggetti S3.

```
arn:aws:s3:::*
```

- Il seguente ARN utilizza entrambi i caratteri jolly, * e ?, nella parte `relative-ID`. Questo ARN identifica tutti gli oggetti in bucket come *amzn-s3-demo-example1bucket*, *amzn-s3-demo-example2bucket*, *amzn-s3-demo-example3bucket*, e così via.

```
arn:aws:s3:::amzn-s3-demo-example?bucket/*
```

Variabili di policy per gli ARN delle risorse

È possibile utilizzare le variabili delle policy negli ARN di Amazon S3. Al momento della valutazione della policy, queste variabili predefinite vengono sostituite dai valori corrispondenti. Supponiamo di organizzare il bucket come una raccolta di cartelle, con una cartella per ogni utente. Il nome della cartella è lo stesso del nome utente. Per assegnare agli utenti le autorizzazioni per le rispettive cartelle, è possibile specificare la variabile di policy nell'ARN della risorsa:

```
arn:aws:s3:::bucket_name/developers/${aws:username}/
```

In fase di esecuzione, quando la policy viene valutata, la variabile `${aws:username}` nell'ARN della risorsa viene sostituita con il nome utente della persona che sta effettuando la richiesta.

Esempi di policy per Amazon S3

- Per visualizzare esempi di policy basate sull'identità di Amazon S3, consulta [Identity-based politiche per Amazon S3](#).
- Per visualizzare esempi di policy basate sulle risorse di Amazon S3, consulta [Policy dei bucket per Amazon S3](#) e [Configurazione delle policy IAM per l'utilizzo degli access point](#).

Chiavi di condizione per Amazon S3

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le politiche AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per vedere tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni [AWS globali](#) nella IAM User Guide.

Ciascuna chiave di condizione di Amazon S3 corrisponde all'intestazione della richiesta con lo stesso nome consentito dall'API su cui può essere impostata la condizione. Le chiavi di condizione specifiche di Amazon S3 determinano il comportamento delle intestazioni di richiesta con lo stesso nome. Ad esempio, la chiave di condizione `s3:VersionId` usata per concedere l'autorizzazione condizionale per l'autorizzazione

`s3:GetObjectVersion`

definisce il comportamento del parametro di query `versionId` impostato in una richiesta GET Object.

Per un elenco delle chiavi di condizione di Amazon S3, consulta [Chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta [Azioni definite da Amazon S3](#).

Esempio: limitazione del caricamento di oggetti a oggetti con una classe di storage specifica

Si supponga che il conto A, rappresentato dall'ID dell'account **123456789012**, possieda un bucket. L'amministratore dell'account A vuole limitare **Dave**, un utente dell'account A, in modo che

Dave possa caricare oggetti nel bucket solo se l'oggetto è archiviato nella classe di archiviazione STANDARD_IA. Per limitare il caricamento di oggetti con una classe di storage specifica, l'amministratore dell'Account A può utilizzare la chiave di condizione `s3:x-amz-storage-class`, come illustrato nella policy di bucket di esempio seguente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Dave"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-storage-class": [
            "STANDARD_IA"
          ]
        }
      }
    }
  ]
}
```

Nell'esempio, il blocco `Condition` specifica la condizione `StringEquals` che viene applicata alla coppia chiave-valore `"s3:x-amz-storage-class":["STANDARD_IA"]`. Esiste un insieme predefinito di chiavi che possono essere utilizzate nell'espressione di una condizione. L'esempio utilizza la chiave di condizione `s3:x-amz-storage-class`. Questa condizione richiede che l'utente includa l'intestazione `x-amz-storage-class` con il valore `STANDARD_IA` in ogni richiesta `PutObject`.

Esempi di policy per Amazon S3

- Per visualizzare esempi di policy basate sull'identità di Amazon S3, consulta [Identity-based politiche per Amazon S3](#).

- Per visualizzare esempi di policy basate sulle risorse di Amazon S3, consulta [Policy dei bucket per Amazon S3](#) e [Configurazione delle policy IAM per l'utilizzo degli access point](#).

ACL in Amazon S3

Supporta le ACL: Sì

In Amazon S3, gli elenchi di controllo degli accessi (ACL) controllano chi Account AWS dispone delle autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, anche se non utilizzano il formato del documento di policy JSON.

Important

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL.

Per informazioni sull'uso delle ACL per controllare l'accesso in Amazon S3, consulta [Gestione degli accessi con le ACL](#).

ABAC con Amazon S3

Supporta ABAC (tag nelle policy): parzialmente

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. Puoi allegare tag alle entità e alle AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di

ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Per informazioni sulle risorse che supportano ABAC in Amazon S3, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

Per visualizzare esempi di policy basate sull'identità per limitare l'accesso ai processi di Operazioni in batch S3 in base ai tag, consulta [Controllo delle autorizzazioni per le operazioni in batch utilizzando i tag di processo](#).

ABAC e tag degli oggetti

Nelle policy ABAC, gli oggetti utilizzano i tag `s3:` invece dei tag `aws:`. Per controllare l'accesso agli oggetti in base ai tag degli oggetti, si forniscono informazioni sui tag nell'[elemento Condition](#) di una policy utilizzando i seguenti tag:

- `s3:ExistingObjectTag/tag-key`
- `s3:RequestObjectTagKeys`
- `s3:RequestObjectTag/tag-key`

Per informazioni sull'uso dei tag degli oggetti per controllare l'accesso, comprese le policy di autorizzazione di esempio, consulta [Tagging e policy di controllo degli accessi](#).

Utilizzo di credenziali temporanee con Amazon S3

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizzano la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM](#) e [Servizi AWS compatibili con IAM](#) nella Guida per l'utente IAM.

Sessioni di accesso in avanti per Amazon S3

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso diretto (FAS) utilizzano le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi a valle. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

- FAS viene utilizzato da Amazon S3 per effettuare chiamate per decrittografare un oggetto quando è stato utilizzato AWS KMS per crittografarlo. SSE-KMS Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#).
- Anche S3 Access Grants utilizza il FAS. Dopo aver creato una concessione di accesso ai dati S3 per una particolare identità, il beneficiario della concessione richiede una credenziale temporanea a S3 Access Grants. S3 Access Grants ottiene una credenziale temporanea per il richiedente e la invia al richiedente. AWS STS Per ulteriori informazioni, consulta [Richiedi l'accesso ai dati di Amazon S3 tramite S3 Access Grants](#).

Ruoli di servizio per Amazon S3

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Amazon S3. Modifica i ruoli di servizio solo quando Amazon S3 fornisce indicazioni in tal senso.

Service-linked ruoli per Amazon S3

Supporta i ruoli legati ai servizi: Parziale

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo di eseguire un'azione per tuo conto. Service-linked i ruoli vengono visualizzati nell'utente Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Amazon S3 supporta i ruoli collegati ai servizi per Amazon S3 Storage Lens. Per informazioni dettagliate sulla creazione o sulla gestione dei ruoli legati al servizio Amazon S3, consulta [Utilizzo dei ruoli collegati ai servizi per Amazon S3 Storage Lens](#).

Servizio Amazon S3 come principale

Nome del servizio nella policy	Funzione S3	Ulteriori informazioni
s3.amazonaws.com	Replica di Amazon S3	Panoramica della configurazione della replica in tempo reale
s3.amazonaws.com	Notifiche di eventi S3	Notifiche di eventi Amazon S3
s3.amazonaws.com	Inventario S3	Catalogazione e analisi dei dati con Inventario S3
access-grants.s3.amazonaws.com	Sovvenzioni per l'accesso a S3	Registrazione di una posizione
batchoperations.s3.amazonaws.com	Operazioni in batch S3	Concessione di autorizzazioni per le operazioni in batch
logging.s3.amazonaws.com	S3 Server Access Logging	Abilitazione della registrazione degli accessi al server Amazon S3
storage-lens.s3.amazonaws.com	S3 Storage Lens	Visualizzazione dei parametri di Amazon S3 Storage Lens utilizzando una esportazione di dati

In che modo Amazon S3 autorizza una richiesta

Quando Amazon S3 riceve una richiesta, ad esempio un'operazione su un bucket o su un oggetto, verifica innanzitutto che il richiedente disponga delle autorizzazioni necessarie. Amazon S3 valuta tutte le policy di accesso pertinenti, le policy utente e le policy basate sulle risorse (policy del bucket, lista di controllo degli accessi (ACL) del bucket e lista ACL dell'oggetto) per decidere se autorizzare la richiesta.

Note

Se il controllo delle autorizzazioni di Amazon S3 non trova autorizzazioni valide, viene restituito un errore di autorizzazione negata Accesso negato (403 Non consentito). Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi agli errori di accesso negato \(403 Accesso negato\) in Amazon S3](#).

Per determinare se il richiedente ha il permesso di eseguire un'operazione specifica, Amazon S3 esegue le seguenti operazioni, in ordine, quando riceve una richiesta:

1. Converte tutte le policy di accesso pertinenti (policy utente, policy bucket e ACL) in fase di esecuzione in un insieme di policy da valutare.
2. Valuta l'insieme di policy risultante nelle fasi successive. In ciascuna fase, Amazon S3 valuta un sottoinsieme di policy in un contesto specifico, in base all'autorità del contesto.
 - a. Contesto dell'utente – Nel contesto dell'utente l'account padre a cui l'utente appartiene è l'autorità del contesto.

Amazon S3 valuta un sottoinsieme di policy di proprietà dell'account padre. Questo sottoinsieme include la policy utente che l'account padre ha associato all'utente. Se il padre possiede anche la risorsa nella richiesta (bucket o oggetto), Amazon S3 valuta anche le policy delle risorse corrispondenti (policy del bucket, ACL del bucket e ACL dell'oggetto) allo stesso tempo.

Per eseguire l'operazione, un utente deve essere autorizzato da un account padre.

Questa fase si applica solo se la richiesta viene eseguita da un utente in un Account AWS. Se la richiesta viene effettuata utilizzando le credenziali dell'utente root di un Account AWS, Amazon S3 salta questo passaggio.

- b. Contesto del bucket: nel contesto del bucket, Amazon S3 valuta le policy di proprietà del proprietario del bucket. Account AWS

Se la richiesta riguarda un'operazione su un bucket, il richiedente deve disporre dell'autorizzazione concessa dal proprietario del bucket. Se la richiesta riguarda un oggetto, Amazon S3 valuta tutte le policy appartenenti al proprietario del bucket per verificare che quest'ultimo non abbia negato in modo esplicito l'accesso all'oggetto. Se è stato impostato un rifiuto esplicito, Amazon S3 non autorizza la richiesta.

- c. Contesto dell'oggetto – Se la richiesta riguarda un oggetto, Amazon S3 valuta il sottoinsieme di policy che appartengono al proprietario dell'oggetto.

Di seguito sono riportati alcuni scenari di esempio che illustrano come Amazon S3 autorizza una richiesta.

Example- Il richiedente è un principale IAM

Se il richiedente è un principale IAM, Amazon S3 deve determinare se il genitore Account AWS a cui appartiene il principale ha concesso al principale l'autorizzazione necessaria per eseguire l'operazione. Inoltre, se la richiesta riguarda un'operazione su un bucket, ad esempio una richiesta per elencare il contenuto del bucket, Amazon S3 deve verificare che il proprietario del bucket abbia concesso al richiedente l'autorizzazione per eseguire l'operazione. Per eseguire un'operazione specifica su una risorsa, un principale IAM necessita dell'autorizzazione sia del padre Account AWS a cui appartiene Account AWS sia del proprietario della risorsa.

Example- Il richiedente è un principale IAM - Se la richiesta è per un'operazione su un oggetto che non è di proprietà del proprietario del bucket

Se la richiesta è per un'operazione su un oggetto che non è di proprietà del proprietario del bucket, oltre ad assicurarsi che il richiedente abbia i permessi del proprietario dell'oggetto, Amazon S3 deve anche controllare la policy del bucket per assicurarsi che il proprietario del bucket non abbia impostato un rifiuto esplicito sull'oggetto. Il proprietario del bucket (che paga la fattura) può negare in modo esplicito l'accesso agli oggetti nel bucket, indipendentemente dall'utente a cui appartiene. Il proprietario del bucket può anche eliminare tutti gli oggetti nel bucket.

Per impostazione predefinita, quando un altro Account AWS carica un oggetto nel bucket generico S3, quell'account (l'autore dell'oggetto) possiede l'oggetto, vi ha accesso e può concedere l'accesso ad altri utenti tramite gli elenchi di controllo degli accessi (ACL). È possibile utilizzare Proprietà dell'oggetto per modificare questo comportamento predefinito in modo che le ACL siano disabilitate e che tu, in qualità di proprietario del bucket, diventi automaticamente proprietario di tutti gli oggetti

presenti nel bucket per uso generico. Di conseguenza, il controllo degli accessi ai dati si basa su policy, come le policy degli utenti IAM, le policy dei bucket S3, le policy degli endpoint del virtual private cloud (VPC) e le policy di controllo dei AWS Organizations servizi (SCP). Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Per ulteriori informazioni su come Amazon S3 valuta le policy di accesso per autorizzare o negare le richieste di operazioni su bucket e oggetti, consulta i seguenti argomenti:

Argomenti

- [In che modo Amazon S3 autorizza una richiesta per un'operazione su un bucket](#)
- [In che modo Amazon S3 autorizza una richiesta per un'operazione su un oggetto](#)

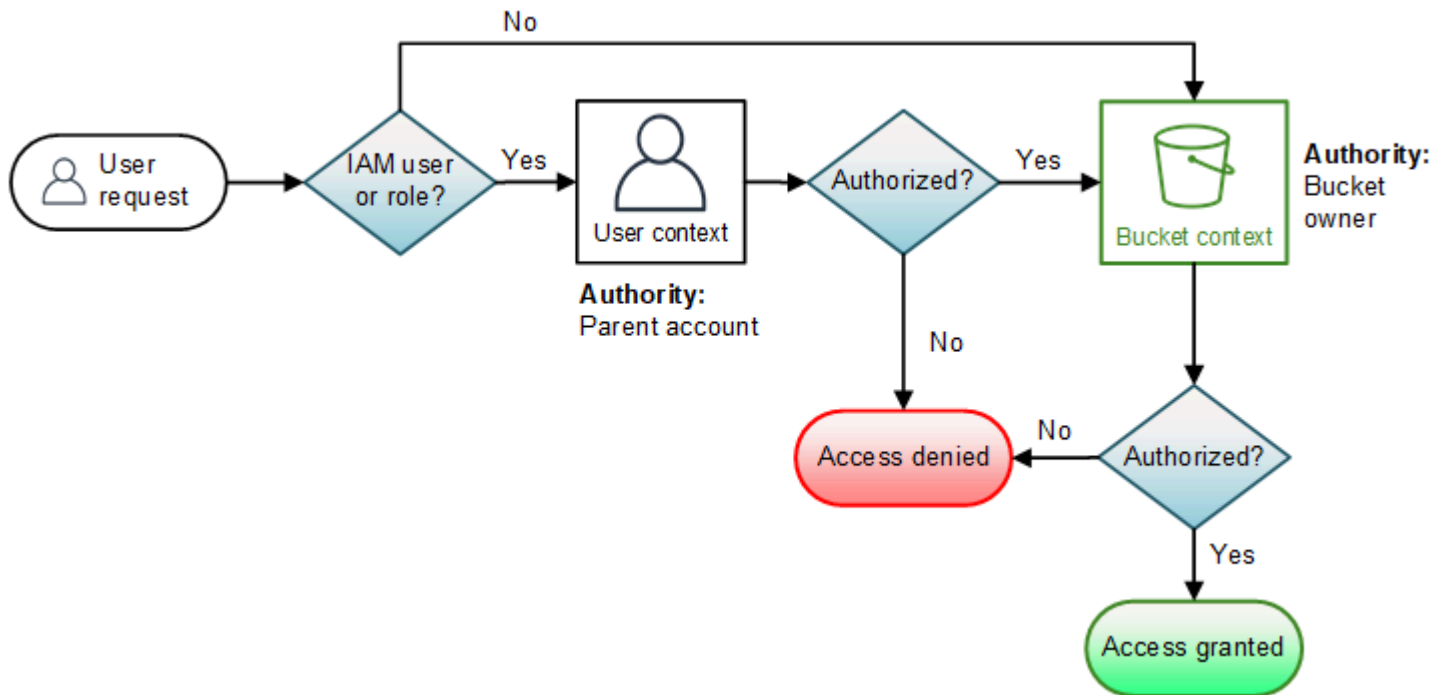
In che modo Amazon S3 autorizza una richiesta per un'operazione su un bucket

Quando Amazon S3 riceve una richiesta per un'operazione su un bucket, Amazon S3 converte tutte le autorizzazioni pertinenti in una serie di policy da valutare in fase di esecuzione. Le autorizzazioni pertinenti includono le autorizzazioni basate sulle risorse (ad esempio, le policy di bucket e le ACL dei bucket) e le policy utente se la richiesta proviene da un principale IAM. Amazon S3 valuta quindi l'insieme di policy risultanti in una serie di passaggi in base a un contesto specifico, quello dell'utente o quello del bucket:

1. **Contesto utente** - Se il richiedente è un principale IAM, il principale deve avere l'autorizzazione dell'Account AWS padre a cui appartiene. In questa fase, Amazon S3 valuta un sottoinsieme di policy appartenenti all'account padre (denominato anche autorità del contesto). Questo sottoinsieme include la policy utente che l'account padre ha associato al principale. Se l'account padre è anche proprietario della risorsa nella richiesta (in questo caso, il bucket), Amazon S3 valuta, allo stesso tempo, anche le policy della risorsa (la policy del bucket e l'ACL del bucket) corrispondenti. Ogni volta che viene eseguita una richiesta per un'operazione su un bucket, i log degli accessi del server registrano l'ID canonico del richiedente. Per ulteriori informazioni, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).
2. **Contesto del bucket** – Il richiedente deve disporre delle autorizzazioni concesse dal proprietario del bucket per eseguire un'operazione specifica sul bucket. In questa fase, Amazon S3 valuta un sottoinsieme di policy di proprietà del proprietario del bucket. Account AWS

Il proprietario del bucket può concedere l'autorizzazione utilizzando una policy del bucket o l'ACL del bucket. Se il Account AWS proprietario del bucket è anche l'account principale di un principale IAM, può configurare le autorizzazioni del bucket in una policy utente.

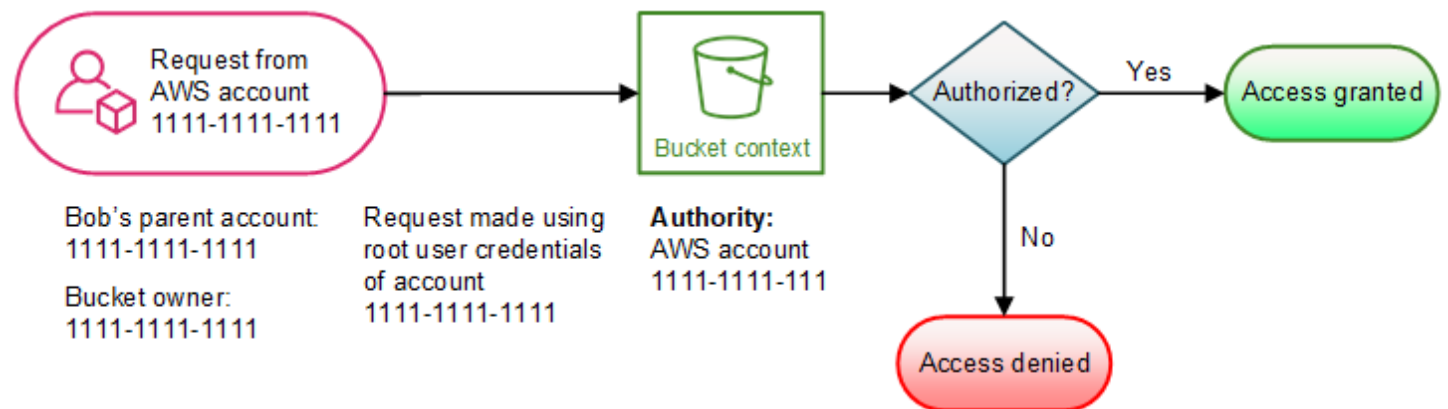
Context-based valutazione del funzionamento del bucket.



Negli esempi seguenti viene illustrata la logica di valutazione.

Esempio 1: operazione su un bucket richiesta dal proprietario del bucket

In questo esempio, il proprietario del bucket invia una richiesta per un'operazione sul bucket utilizzando le credenziali dell'utente root dell' Account AWS.



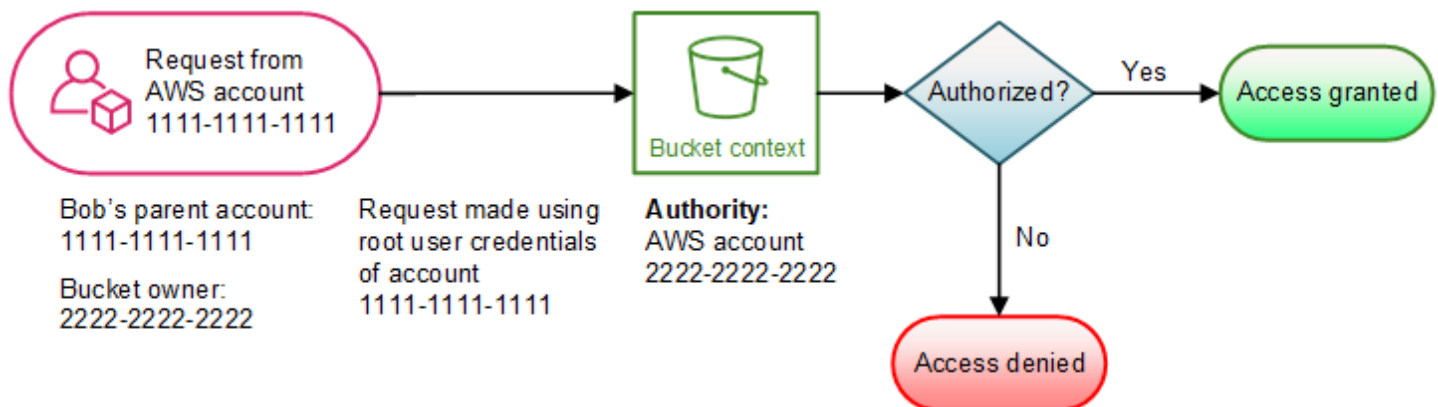
Amazon S3 esegue la valutazione del contesto come indicato di seguito:

1. Poiché la richiesta viene eseguita utilizzando le credenziali dell'utente root di un Account AWS, il contesto dell'utente non viene valutato.

2. Nel contesto del bucket, Amazon S3 esamina la policy del bucket per determinare se il richiedente dispone dell'autorizzazione per eseguire l'operazione. Amazon S3 autorizza la richiesta.

Esempio 2: operazione bucket richiesta da un Account AWS quello non è il proprietario del bucket

In questo esempio, viene eseguita una richiesta utilizzando le credenziali dell'utente root dell'Account AWS 1111-1111-1111 per un'operazione sul bucket che appartiene all'Account AWS 2222-2222-2222. Nessun utente IAM è coinvolto in questa richiesta.

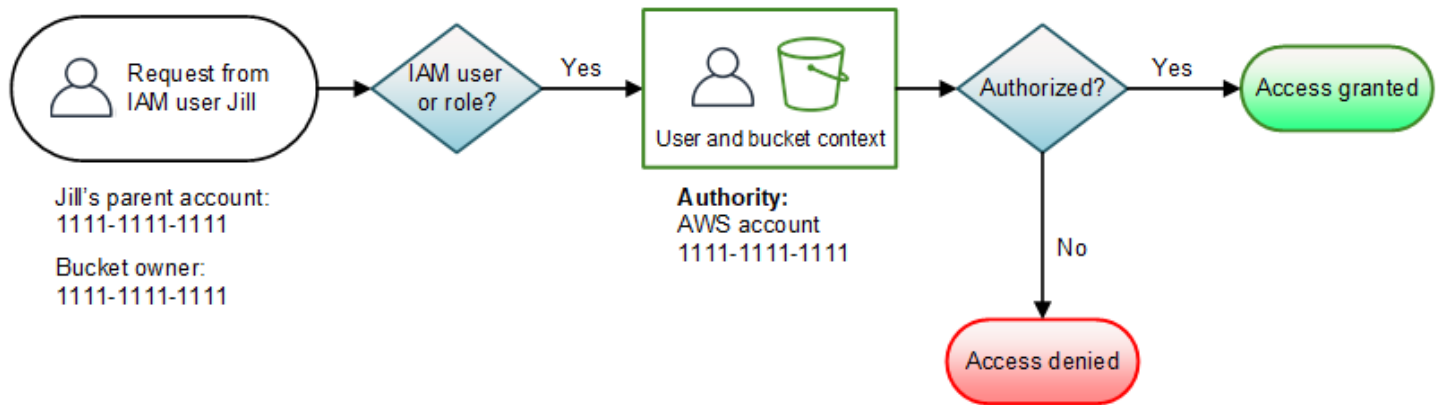


In questo esempio, Amazon S3 valuta il contesto come segue:

1. Poiché la richiesta viene eseguita utilizzando le credenziali dell'utente root di un Account AWS, il contesto dell'utente non viene valutato.
2. Nel contesto del bucket, Amazon S3 esamina la policy del bucket. Se il proprietario del bucket (Account AWS 2222-2222-2222) non ha autorizzato Account AWS 1111-1111-1111 a eseguire l'operazione richiesta, Amazon S3 rifiuta la richiesta. Altrimenti, Amazon S3 accetta la richiesta ed esegue l'operazione.

Esempio 3: operazione del bucket richiesta da un principale IAM il cui elemento principale Account AWS è anche il proprietario del bucket

Nell'esempio, la richiesta viene inviata da Jill, un utente IAM nell'Account AWS 1111-1111-1111, che è anche il proprietario del bucket.



Amazon S3 esegue la seguente valutazione del contesto:

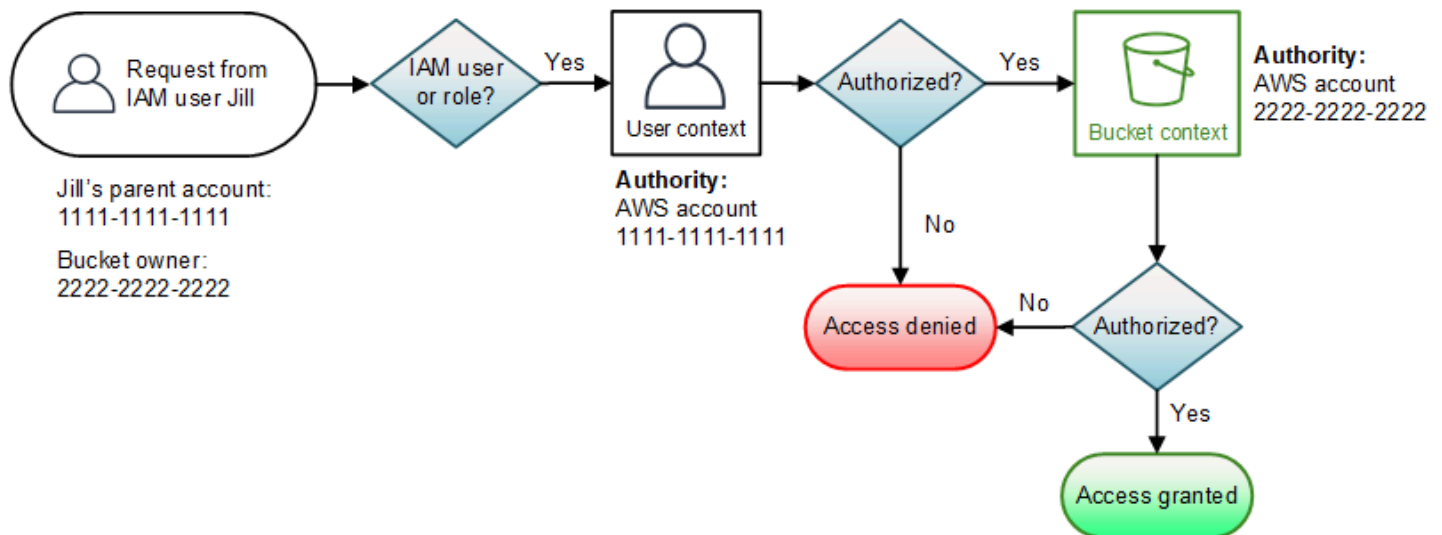
1. Poiché la richiesta proviene da un principale IAM, nel contesto utente, Amazon S3 valuta tutte le politiche che appartengono al principale per determinare se Jill dispone dell'autorizzazione Account AWS per eseguire l'operazione.

In questo esempio, il padre Account AWS 1111-1111-1111, a cui appartiene il principale, è anche il proprietario del bucket. Di conseguenza, oltre alla policy dell'utente, Amazon S3 valuta anche la policy del bucket e la ACL del bucket nello stesso contesto, poiché appartengono allo stesso account.

2. Poiché Amazon S3 ha valutato la policy del bucket e l'ACL del bucket come parte del contesto dell'utente, non valuta il contesto del bucket.

Esempio 4: operazione bucket richiesta da un responsabile IAM il cui elemento principale Account AWS non è il proprietario del bucket

In questo esempio, la richiesta viene inviata da Jill, un utente IAM il cui padre Account AWS è 1111-1111-1111, ma il bucket è di proprietà di un altro utente, 2222-2222-2222. Account AWS



Jill avrà bisogno delle autorizzazioni sia del genitore che del proprietario del bucket Account AWS . Amazon S3 valuta il contesto come indicato di seguito:

1. Poiché la richiesta proviene da un principale IAM, Amazon S3 valuta il contesto dell'utente esaminando le policy create dall'account per verificare che Jill disponga delle autorizzazioni necessarie. Se Jill ha l'autorizzazione, Amazon S3 passa a valutare il contesto del bucket. Se Jill non ha l'autorizzazione, nega la richiesta.
2. Nel contesto del bucket, Amazon S3 verifica che il proprietario del bucket 2222-2222-2222 abbia concesso a Jill (o al suo genitore) l'autorizzazione per eseguire l'operazione richiesta. Account AWS Se dispone di tale autorizzazione, Amazon S3 concede la richiesta ed esegue l'operazione. In caso contrario, Amazon S3 rifiuta la richiesta.

In che modo Amazon S3 autorizza una richiesta per un'operazione su un oggetto

Quando riceve una richiesta per un'operazione su un oggetto, Amazon S3 converte tutte le autorizzazioni rilevanti, ovvero le autorizzazioni basate sulle risorse (lista di controllo accessi (ACL) dell'oggetto, policy del bucket e ACL del bucket) e le policy utente IAM, in un set di policy da valutare in fase di esecuzione. Valuta quindi l'insieme di policy risultante in una serie di fasi. In ogni fase, valuta un sottoinsieme di policy in tre contesti specifici: contesto dell'utente, contesto del bucket e contesto dell'oggetto:

1. Contesto utente: se il richiedente è un principale IAM, deve disporre dell'autorizzazione del genitore a cui appartiene. Account AWS In questa fase, Amazon S3 valuta un sottoinsieme di policy appartenenti all'account padre (denominato anche autorità del contesto). Questo sottoinsieme include la policy utente che l'account padre ha associato al principale. Se il padre

possiede anche la risorsa nella richiesta (bucket o oggetto), Amazon S3 valuta le policy delle risorse corrispondenti (policy del bucket, ACL del bucket e ACL dell'oggetto) allo stesso tempo.

Note

Se il genitore Account AWS possiede la risorsa (bucket o oggetto), può concedere le autorizzazioni di risorsa al suo principale IAM utilizzando la policy utente o la policy delle risorse.

2. Contesto del bucket: in questo contesto Amazon S3 valuta le policy che appartengono all' Account AWS proprietario del bucket.

Se il Account AWS proprietario dell'oggetto nella richiesta non è lo stesso proprietario del bucket, Amazon S3 verifica le politiche se il proprietario del bucket ha negato esplicitamente l'accesso all'oggetto. Se è stato impostato un rifiuto esplicito sull'oggetto, Amazon S3 non autorizza la richiesta.

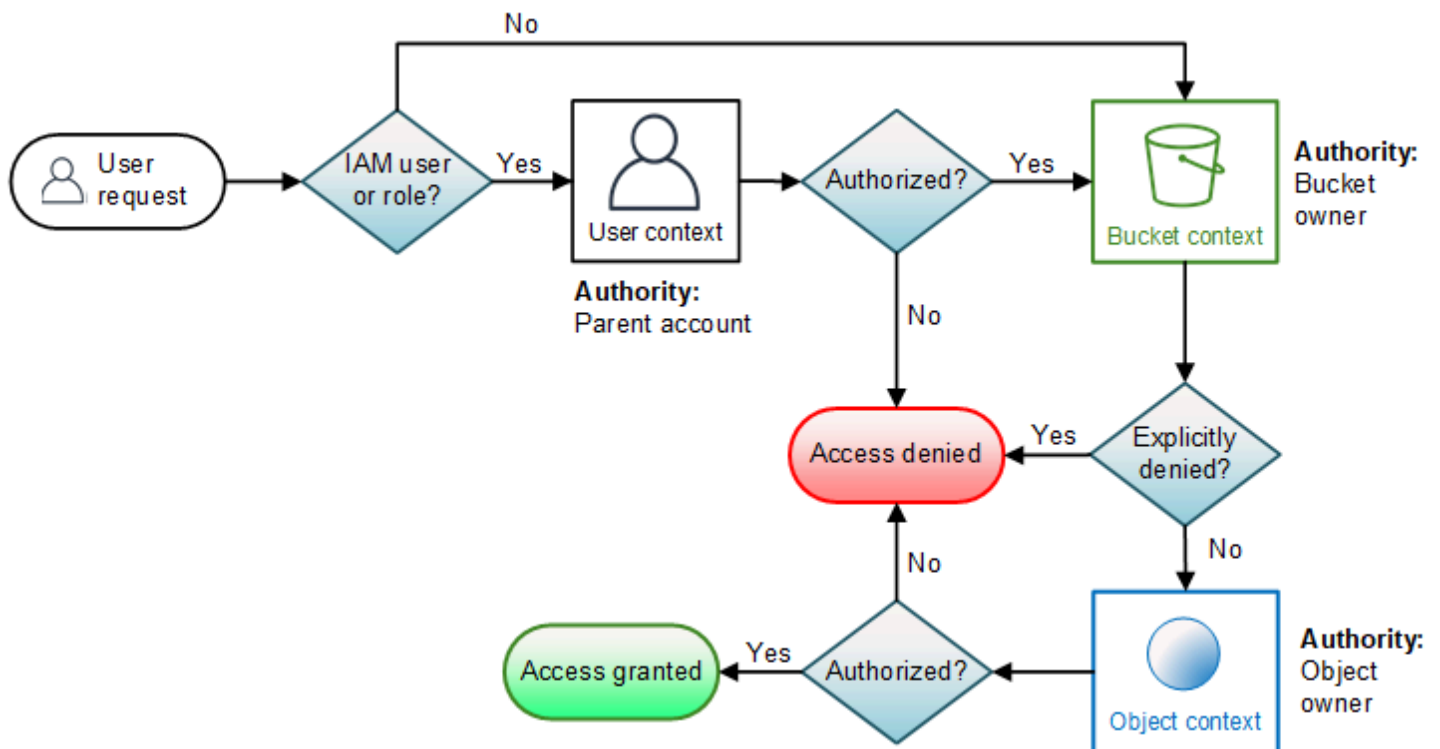
3. Contesto dell'oggetto – Il richiedente deve disporre delle autorizzazioni concesse dal proprietario dell'oggetto per eseguire un'operazione specifica sull'oggetto. In questa fase, Amazon S3 valuta l'ACL dell'oggetto.

Note

Se il proprietario del bucket corrisponde a quello dell'oggetto, l'accesso all'oggetto può essere concesso nella policy del bucket, che viene valutata nel contesto del bucket. Se i proprietari sono differenti, il proprietario dell'oggetto devono utilizzare un'ACL dell'oggetto per concedere le autorizzazioni. Se il Account AWS proprietario dell'oggetto è anche l'account principale a cui appartiene il principale IAM, può configurare le autorizzazioni dell'oggetto in una policy utente, che viene valutata nel contesto dell'utente. Per ulteriori informazioni su come utilizzare queste policy di accesso alternative, consulta la sezione [Passaggi che utilizzano le policy per gestire l'accesso alle risorse Amazon S3](#).

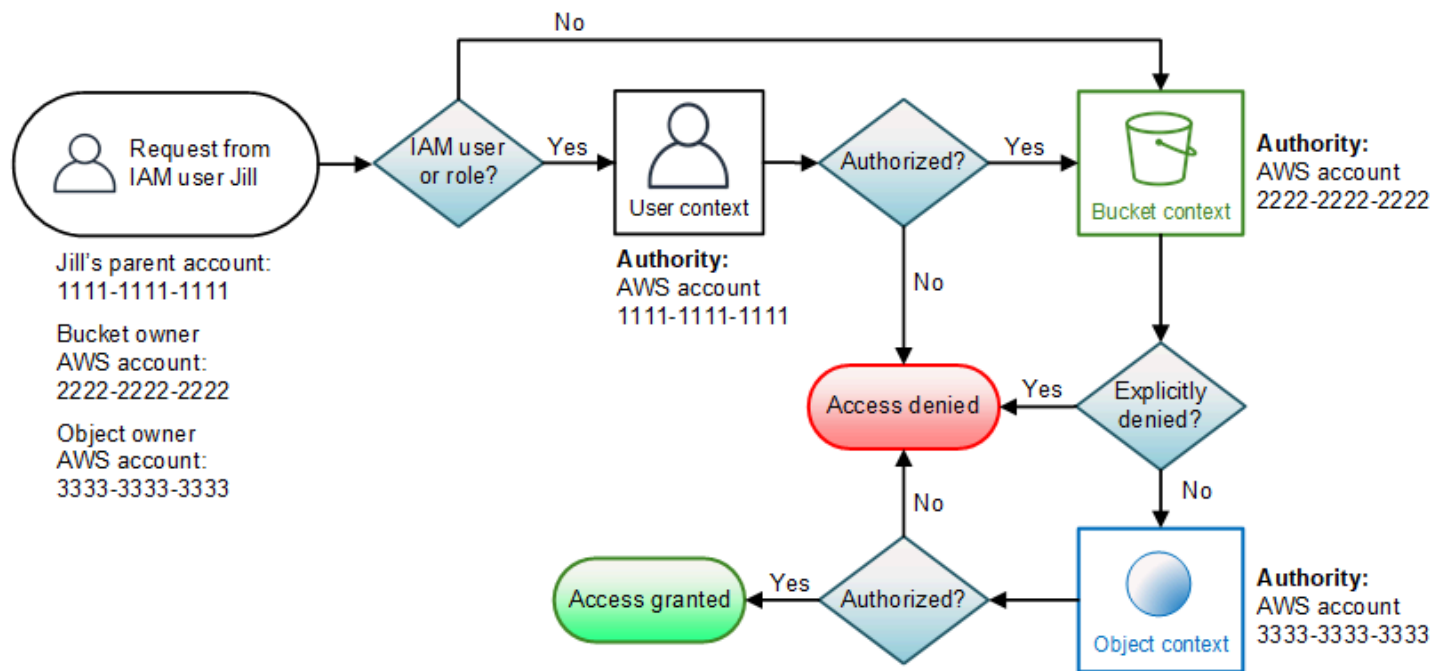
Se il proprietario del bucket desidera possedere tutti gli oggetti del bucket e utilizzare le policy del bucket o le policy basate su IAM per gestire l'accesso a questi oggetti, è possibile applicare l'impostazione del proprietario del bucket per la proprietà degli oggetti. Con questa impostazione, in quanto proprietario del bucket possiedi automaticamente e hai il pieno controllo su ogni oggetto nel bucket. Le ACL del bucket e dell'oggetto non possono essere modificate e non sono più valutate per l'accesso. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Di seguito è riportata un'illustrazione della valutazione basata sul contesto per un'operazione su un oggetto.



Esempio di richiesta di operazione su un oggetto

In questo esempio, l'utente IAM Jill, il cui padre Account AWS è 1111-1111-1111, invia una richiesta di operazione sull'oggetto (ad esempio, `GetObject`) per un oggetto di proprietà di Account AWS 3333-3333-3333 in un bucket di proprietà di 2222-2222-2222. Account AWS



Jill avrà bisogno dell'autorizzazione del genitore Account AWS, del proprietario del bucket e del proprietario dell'oggetto. Amazon S3 valuta il contesto come indicato di seguito:

1. Poiché la richiesta proviene da un principal IAM, Amazon S3 valuta il contesto dell'utente per verificare che il Account AWS 1111-1111-1111 padre abbia concesso a Jill l'autorizzazione per eseguire l'operazione richiesta. Se Jill dispone di tale autorizzazione, Amazon S3 valuta il contesto del bucket. In caso contrario, Amazon S3 rifiuta la richiesta.
2. Nel contesto del bucket, il proprietario del bucket, 2222-2222-2222, è l'autorità del contesto. Account AWS Amazon S3 valuta la policy del bucket per determinare se il proprietario del bucket ha negato in modo esplicito l'accesso all'oggetto.
3. Nel contesto dell'oggetto, l'autorità del contesto è l' Account AWS 3333-3333-3333, ovvero il proprietario dell'oggetto. Amazon S3 valuta l'ACL dell'oggetto per determinare se Jill dispone dell'autorizzazione per accedere all'oggetto. In caso affermativo, Amazon S3 autorizza la richiesta.

Autorizzazioni necessarie per le operazioni API di Amazon S3

Note

Questa pagina riguarda le azioni delle policy di Amazon S3 per i bucket per uso generico. Per saperne di più sulle azioni delle policy di Amazon S3 per i bucket di directory, consulta [Azioni per i bucket della directory](#).

Per eseguire un'operazione API S3, è necessario disporre delle giuste autorizzazioni. Questa pagina mappa le operazioni API S3 alle autorizzazioni richieste. Per concedere le autorizzazioni per l'esecuzione di un'operazione API S3, è necessario comporre una policy valida (come una policy S3 bucket o una policy IAM basata sull'identità) e specificare le azioni corrispondenti nell'elemento Action della policy. Queste azioni sono chiamate azioni policy. Non tutte le operazioni API S3 sono rappresentate da un singolo permesso (una singola azione di policy) e alcuni permessi (alcune azioni di policy) sono necessari per molte operazioni API diverse.

Quando si compongono le policy, è necessario specificare l'elemento Resource in base al tipo di risorsa corretta richiesta dalle azioni della policy Amazon S3 corrispondente. Questa pagina classifica le autorizzazioni alle operazioni API S3 in base ai tipi di risorse. Per ulteriori informazioni sui tipi di risorse, consulta [Tipi di risorse definiti da Amazon S3](#) in Riferimento alle autorizzazioni di servizio. Per un elenco completo delle azioni, delle risorse e delle chiavi di condizione per le policy di Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio. Per un elenco completo delle operazioni API di Amazon S3, consulta [Azioni API di Amazon S3](#) in Riferimento API di Amazon Simple Storage Service.

Per ulteriori informazioni su come correggere gli errori HTTP 403 Forbidden in S3, consulta [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#). Per ulteriori informazioni sulle funzionalità IAM da utilizzare con S3, consulta [Come funziona Amazon S3 con IAM](#). Per ulteriori informazioni sulle best practice di sicurezza S3, consulta [Best practice di sicurezza per Amazon S3](#).

Argomenti

- [Operazioni e autorizzazioni del bucket](#)
- [Operazioni e autorizzazioni degli oggetti](#)
- [Operazioni sui punti di accesso di bucket per uso generico e autorizzazioni](#)
- [Operazioni e autorizzazioni del punto di accesso Lambda per oggetti](#)

- [Multi-Region Operazioni e autorizzazioni dell'Access Point](#)
- [Operazioni e autorizzazioni per i processi batch](#)
- [Operazioni e autorizzazioni di configurazione di S3 Storage Lens](#)
- [Operazioni e autorizzazioni dei gruppi S3 Storage Lens](#)
- [Operazioni sull'istanza S3 Access Grants e autorizzazioni](#)
- [Operazioni sulla posizione S3 Access Grants e autorizzazioni](#)
- [Operazioni sulla concessione S3 Access Grants e autorizzazioni](#)
- [Operazioni e autorizzazioni dell'account](#)

Operazioni e autorizzazioni del bucket

Le operazioni sui bucket sono operazioni API S3 che operano sul tipo di risorsa bucket. È necessario specificare le azioni delle policy S3 per le operazioni sui bucket nelle policy sui bucket o nelle policy IAM basate sull'identità.

Nelle policy, l'elemento `Resource` deve essere il nome della risorsa Amazon (ARN) del bucket. Per ulteriori informazioni sul formato dell'elemento `Resource` e su esempi di policy, consulta [Operazioni relative ai bucket](#).

Note

Per concedere le autorizzazioni alle operazioni di bucket nelle policy dei punti di accesso, tieni presente quanto segue:

- Le autorizzazioni concesse per le operazioni sui bucket in una policy del punto di accesso sono efficaci solo se il bucket sottostante consente le stesse autorizzazioni. Quando si utilizza un punto di accesso, è necessario delegare il controllo dell'accesso dal bucket al punto di accesso o aggiungere le stesse autorizzazioni nella policy del punto di accesso alla policy del bucket sottostante.
- Nelle policy dei punti di accesso che concedono autorizzazioni alle operazioni di bucket, l'elemento `Resource` deve essere l'ARN `accesspoint`. Per ulteriori informazioni sul formato dell'elemento `Resource` e su esempi di policy, consulta [Operazioni su bucket nelle policy per i punti di accesso di bucket per uso generico](#). Per ulteriori informazioni sulle policy dei punti di accesso, consulta [Configurazione delle policy IAM per l'utilizzo degli access point](#).

- Non tutte le operazioni di bucket sono supportate dai punti di accesso. Per ulteriori informazioni, consulta [Compatibilità dei punti di accesso con le operazioni S3](#).

Di seguito è riportata la mappatura delle operazioni sui bucket e delle azioni di policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
CreateBucket	(Obbligatorio) <code>s3:CreateBucket</code>	Richiesto per creare un nuovo bucket s3.
	(Obbligo condizionale) <code>s3:PutBucketAcl</code>	Necessario se si desidera utilizzare una lista di controllo degli accessi (ACL) per specificare le autorizzazioni su un bucket quando si effettua una richiesta <code>CreateBucket</code> .
	(Obbligo condizionale) <code>s3:PutBucketObjectLockConfiguration</code> , <code>s3:PutBucketVersioning</code>	Richiesto se si desidera attivare Object Lock quando si crea un bucket.
	(Obbligo condizionale) <code>s3:PutBucketOwnershipControls</code>	Richiesto se si desidera specificare la proprietà dell'oggetto S3 quando si crea un bucket.
CreateBucketMetadataConfiguration (operazione API V2, il nome dell'azione della policy IAM è uguale per le operazioni API V1 e V2).	(Obbligatorio) <code>s3:CreateBucketMetadataTableConfiguration</code> , <code>s3:tables:CreateTableBucket</code> , <code>s3:tables:CreateNamespace</code>	Richiesto per creare la configurazione di una tabella di metadati su un bucket per uso generico. Per creare il bucket di tabelle AWS gestite e le tabelle di

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	<code>s3tables:CreateTable</code> <code>s3tables:GetTable</code> <code>s3tables:PutTablePolicy</code> <code>s3tables:PutTableEncryption</code> <code>kms:DescribeKey</code>	<p>metadati specificate nella configurazione della tabella dei metadati, è necessario disporre delle autorizzazioni specificate. <code>s3tables</code></p> <p>Se desideri crittografare le tabelle di metadati con la crittografia lato server con () keys AWS Key Management Service (AWS KMS), hai bisogno di autorizzazioni aggiuntive nella tua politica delle chiavi KMS SSE-KMS. Per ulteriori informazioni, consulta the section called “Autorizzazioni per le tabelle di metadati”.</p> <p>Se desideri integrare anche il bucket di tabelle AWS gestito con i servizi di AWS analisi in modo da poter interrogare la tabella dei metadati, hai bisogno di autorizzazioni aggiuntive. Per ulteriori informazioni, consulta Integrazione delle tabelle Amazon S3 con i servizi di analisi di AWS.</p>

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
CreateBucketMetadataTableConfiguration (operazione API V1)	(Obbligatorio) <code>s3:CreateBucketMetadataTableConfiguration</code> , <code>s3tables:CreateNamespace</code> , <code>s3tables:CreateTable</code> , <code>s3tables:GetTable</code> , <code>s3tables:PutTablePolicy</code>	<p>Richiesto per creare la configurazione di una tabella di metadati su un bucket per uso generico.</p> <p>Per creare la tabella dei metadati nel bucket della tabella specificato nella configurazione della tabella dei metadati, è necessario o disporre dei permessi specificati in <code>s3tables</code>.</p> <p>Se desideri crittografare le tabelle di metadati con la crittografia lato server con () keys AWS Key Management Service (AWS KMS), hai bisogno di autorizzazioni aggiuntive. SSE-KMS Per ulteriori informazioni, consulta the section called “Autorizzazioni per le tabelle di metadati”.</p> <p>Se desideri inoltre integrare il tuo table bucket con i servizi di AWS analisi in modo da poter interrogare la tabella dei metadati, hai bisogno di autorizzazioni aggiuntive. Per ulteriori informazioni, consulta Integrazione delle tabelle</p>

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
		Amazon S3 con i servizi di analisi. AWS
DeleteBucket	(Obbligatorio) s3:DeleteBucket	Richiesto per eliminare un bucket S3.
DeleteBucketAnalyticsConfiguration	(Obbligatorio) s3:PutAnalyticsConfiguration	Richiesto per eliminare una configurazione analitica S3 da un bucket S3.
DeleteBucketCors	(Obbligatorio) s3:PutBucketCORS	Richiesto per eliminare la configurazione della condivisione delle risorse in origine incrociata (CORS) per un bucket.
DeleteBucketEncryption	(Obbligatorio) s3:PutEncryptionConfiguration	Necessario per reimpostare la configurazione di crittografia predefinita per un bucket S3 come crittografia lato server con chiavi gestite da Amazon S3 (. SSE-S3
DeleteBucketIntelligentTieringConfiguration	(Obbligatorio) s3:PutIntelligentTieringConfiguration	Necessario per eliminare la configurazione S3 esistente da un bucket S3 Intelligent-Tiering .
DeleteBucketInventoryConfiguration	(Obbligatorio) s3:PutInventoryConfiguration	Richiesto per eliminare una configurazione dell'inventario S3 da un bucket S3.
DeleteBucketLifecycle	(Obbligatorio) s3:PutLifecycleConfiguration	Richiesto per eliminare la configurazione del ciclo di vita S3 per un bucket S3.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteBucketMetadataConfiguration (operazione API V2, il nome dell'azione della policy IAM è uguale per le operazioni API V1 e V2).	(Obbligatorio) <code>s3:DeleteBucketMetadataTableConfiguration</code>	Richiesto per eliminare la configurazione di una tabella di metadati da un bucket per uso generico.
DeleteBucketMetadataTableConfiguration (operazione API V1)	(Obbligatorio) <code>s3:DeleteBucketMetadataTableConfiguration</code>	Richiesto per eliminare la configurazione di una tabella di metadati da un bucket per uso generico.
DeleteBucketMetricsConfiguration	(Obbligatorio) <code>s3:PutMetricsConfiguration</code>	Necessario per eliminare una configurazione delle metriche per le metriche di CloudWatch richiesta Amazon da un bucket S3.
DeleteBucketOwnershipControls	(Obbligatorio) <code>s3:PutBucketOwnershipControls</code>	Richiesto per rimuovere l'impostazione della proprietà dell'oggetto per un bucket S3. Dopo la rimozione, l'impostazione Proprietà oggetto diventa <code>Object writer</code> .
DeleteBucketPolicy	(Obbligatorio) <code>s3:DeleteBucketPolicy</code>	Richiesto per eliminare la policy di un bucket S3.
DeleteBucketReplication	(Obbligatorio) <code>s3:PutReplicationConfiguration</code>	Richiesto per eliminare la configurazione di replica di un bucket S3.
DeleteBucketTagging	(Obbligatorio) <code>s3:PutBucketTagging</code>	Richiesto per eliminare i tag da un bucket S3.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteBucketWebsite	(Obbligatorio) <code>s3:DeleteBucketWebsite</code>	Richiesto per rimuovere la configurazione del sito web per un bucket S3.
DeletePublicAccessBlock (Bucket-level)	(Obbligatorio) <code>s3:PutBucketPublicAccessBlock</code>	Richiesto per rimuovere la configurazione di accesso pubblico a blocchi per un bucket S3.
GetBucketAccelerateConfiguration	(Obbligatorio) <code>s3:GetAccelerateConfiguration</code>	Necessario per utilizzare la sotto-risorsa accelerate per restituire lo stato di Amazon S3 Transfer Acceleration di un bucket, che è Enabled o Suspended.
GetBucketAcl	(Obbligatorio) <code>s3:GetBucketAcl</code>	Richiesto per restituire la lista di controllo degli accessi (ACL) di un bucket S3.
GetBucketAnalyticsConfiguration	(Obbligatorio) <code>s3:GetAnalyticsConfiguration</code>	Richiesto per restituire una configurazione di analisi identificata dall'ID della configurazione di analisi da un bucket S3.
GetBucketCors	(Obbligatorio) <code>s3:GetBucketCORS</code>	Richiesto per restituire la configurazione della condivisione delle risorse in provenienza incrociata (CORS) per un bucket S3.
GetBucketEncryption	(Obbligatorio) <code>s3:GetEncryptionConfiguration</code>	Richiesto per ripristinare la configurazione di crittografia predefinita per un bucket S3.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
GetBucketIntelligentTieringConfiguration	(Obbligatorio) <code>s3:GetIntelligentTieringConfiguration</code>	Necessario per ottenere la Intelligent-Tiering configurazione S3 di un bucket S3.
GetBucketInventoryConfiguration	(Obbligatorio) <code>s3:GetInventoryConfiguration</code>	Richiesto per restituire una configurazione d'inventario identificata dall'ID della configurazione d'inventario dal bucket.
GetBucketLifecycle	(Obbligatorio) <code>s3:GetLifecycleConfiguration</code>	Richiesto per restituire la configurazione S3 Lifecycle del bucket.
GetBucketLocation	(Obbligatorio) <code>s3:GetBucketLocation</code>	Necessario per restituire il valore in Regione AWS cui risiede un bucket S3.
GetBucketLogging	(Obbligatorio) <code>s3:GetBucketLogging</code>	Richiesto per restituire lo stato di registrazione di un bucket S3 e le autorizzazioni che gli utenti hanno per visualizzare e modificare tale stato.
GetBucketMetadataConfiguration (operazione API V2, il nome dell'azione della policy IAM è uguale per le operazioni API V1 e V2).	(Obbligatorio) <code>s3:GetBucketMetadataTableConfiguration</code>	Richiesto per recuperare la configurazione di una tabella di metadati per un bucket per uso generico.
GetBucketMetadataTableConfiguration (operazione API V1)	(Obbligatorio) <code>s3:GetBucketMetadataTableConfiguration</code>	Richiesto per recuperare la configurazione di una tabella di metadati per un bucket per uso generico.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
GetBucketMetricsConfiguration	(Obbligatorio) <code>s3:GetMetricsConfiguration</code>	Richiesto per ottenere una configurazione di metriche specificata dall'ID della configurazione di metriche dal bucket.
GetBucketNotificationConfiguration	(Obbligatorio) <code>s3:GetBucketNotification</code>	Richiesto per restituire la configurazione di notifica di un bucket S3.
GetBucketOwnershipControls	(Obbligatorio) <code>s3:GetBucketOwnershipControls</code>	Richiesto per recuperare l'impostazione della proprietà dell'oggetto per un bucket S3.
GetBucketPolicy	(Obbligatorio) <code>s3:GetBucketPolicy</code>	Richiesto per restituire la policy di un bucket S3.
GetBucketPolicyStatus	(Obbligatorio) <code>s3:GetBucketPolicyStatus</code>	Richiesto per recuperare lo stato delle policy per un bucket S3, che indica se il bucket è pubblico.
GetBucketReplication	(Obbligatorio) <code>s3:GetReplicationConfiguration</code>	Richiesto per restituire la configurazione di replica di un bucket S3.
GetBucketRequestPayment	(Obbligatorio) <code>s3:GetBucketRequestPayment</code>	Richiesto per restituire la configurazione del pagamento della richiesta per un bucket S3.
GetBucketVersioning	(Obbligatorio) <code>s3:GetBucketVersioning</code>	Richiesto per restituire lo stato di controllo delle versioni di un bucket S3.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
GetBucketTagging	(Obbligatorio) <code>s3:GetBucketTagging</code>	Richiesto per restituire il set di tag associato a un bucket S3.
GetBucketWebsite	(Obbligatorio) <code>s3:GetBucketWebsite</code>	Richiesto per restituire la configurazione del sito web per un bucket S3.
GetObjectLockConfiguration	(Obbligatorio) <code>s3:GetObjectLockConfiguration</code>	Richiesto per ottenere la configurazione di Object Lock per un bucket S3.
GetPublicAccessBlock (Bucket-level)	(Obbligatorio) <code>s3:GetPublicAccessBlock</code>	Richiesto per recuperare la configurazione di accesso pubblico ai blocchi per un bucket S3.
HeadBucket	(Obbligatorio) <code>s3:ListBucket</code>	Richiesto per determinare se un bucket esiste e se si ha il permesso di accedervi.
ListBucketAnalyticsConfigurations	(Obbligatorio) <code>s3:GetAnalyticsConfiguration</code>	Richiesto per elencare le configurazioni di analisi per un bucket S3.
ListBucketIntelligentTieringConfigurations	(Obbligatorio) <code>s3:GetIntelligentTieringConfiguration</code>	Necessario per elencare le Intelligent-Tiering configurazioni S3 di un bucket S3.
ListBucketInventoryConfigurations	(Obbligatorio) <code>s3:GetInventoryConfiguration</code>	Richiesto per restituire un elenco di configurazioni di inventario per un bucket S3.
ListBucketMetricsConfigurations	(Obbligatorio) <code>s3:GetMetricsConfiguration</code>	Richiesto per elencare le configurazioni delle metriche per un bucket S3.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
ListObjects	(Obbligatorio) <code>s3:ListBucket</code>	Richiesto per elencare alcuni o tutti (fino a 1.000) gli oggetti di un bucket S3.
	(Obbligo condizionale) <code>s3:GetObjectAcl</code>	Richiesto se si desidera visualizzare le informazioni sul proprietario dell'oggetto.
ListObjectsV2	(Obbligatorio) <code>s3:ListBucket</code>	Richiesto per elencare alcuni o tutti (fino a 1.000) gli oggetti di un bucket S3.
	(Obbligo condizionale) <code>s3:GetObjectAcl</code>	Richiesto se si desidera visualizzare le informazioni sul proprietario dell'oggetto.
ListObjectVersions	(Obbligatorio) <code>s3:ListBucketVersions</code>	Necessario per ottenere metadati su tutte le versioni degli oggetti in un bucket S3.
PutBucketAccelerateConfiguration	(Obbligatorio) <code>s3:PutAccelerateConfiguration</code>	Richiesto per impostare la configurazione di accelerazione di un bucket esistente.
PutBucketAcl	(Obbligatorio) <code>s3:PutBucketAcl</code>	Richiesto per utilizzare le liste di controllo degli accessi (ACL) per impostare le autorizzazioni su un bucket esistente.
PutBucketAnalyticsConfiguration	(Obbligatorio) <code>s3:PutAnalyticsConfiguration</code>	Richiesto per impostare una configurazione analitica per un bucket S3.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
PutBucketCors	(Obbligatorio) s3:PutBucketCors	Richiesto per impostare la configurazione della condivisione delle risorse in provenienza incrociata (CORS) per un bucket S3.
PutBucketEncryption	(Obbligatorio) s3:PutEncryptionConfiguration	Richiesto per configurare la crittografia predefinita per un bucket S3.
PutBucketIntelligentTieringConfiguration	(Obbligatorio) s3:PutIntelligentTieringConfiguration	Necessario per inserire la Intelligent-Tiering configurazione S3 in un bucket S3.
PutBucketInventoryConfiguration	(Obbligatorio) s3:PutInventoryConfiguration	Richiesto per aggiungere una configurazione di inventario a un bucket S3.
PutBucketLifecycle	(Obbligatorio) s3:PutLifecycleConfiguration	Richiesto per creare una nuova configurazione del ciclo di vita S3 o per sostituire una configurazione del ciclo di vita esistente per un bucket S3.
PutBucketLogging	(Obbligatorio) s3:PutBucketLogging	Necessario per impostare i parametri di registrazione per un bucket S3 e specificare le autorizzazioni per chi può visualizzare e modificare i parametri di registrazione.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
PutBucketMetricsConfiguration	(Obbligatorio) s3:PutMetricsConfiguration	Necessario per impostare o aggiornare una configurazione delle metriche per le metriche di CloudWatch richiesta Amazon di un bucket S3.
PutBucketNotificationConfiguration	(Obbligatorio) s3:PutBucketNotification	Necessario per abilitare le notifiche di eventi specifici per un bucket S3.
PutBucketOwnershipControls	(Obbligatorio) s3:PutBucketOwnershipControls	Richiesto per creare o modificare l'impostazione della proprietà dell'oggetto per un bucket S3.
PutBucketPolicy	(Obbligatorio) s3:PutBucketPolicy	Richiesto per applicare una policy del bucket S3 a un bucket.
PutBucketReplication	(Obbligatorio) s3:PutReplicationConfiguration	Necessario per creare una nuova configurazione di replica o sostituirla con una esistente per un bucket S3.
PutBucketRequestPayment	(Obbligatorio) s3:PutBucketRequestPayment	Richiesto per impostare la configurazione del pagamento della richiesta per un bucket.
PutBucketTagging	(Obbligatorio) s3:PutBucketTagging	Richiesto per aggiungere una serie di tag a un bucket S3.
PutBucketVersioning	(Obbligatorio) s3:PutBucketVersioning	Richiesto per impostare lo stato di controllo delle versioni di un bucket S3.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
PutBucketWebsite	(Obbligatorio) <code>s3:PutBucketWebsite</code>	Richiesto per configurare un bucket come sito web e impostare la configurazione del sito web.
PutObjectLockConfiguration	(Obbligatorio) <code>s3:PutObjectLockConfiguration</code>	Richiesto per mettere la configurazione di Object Lock su un bucket S3.
PutPublicAccessBlock (Bucket-level)	(Obbligatorio) <code>s3:PutPublicAccessBlock</code>	Richiesto per creare o modificare la configurazione di accesso pubblico a blocchi per un bucket S3.
UpdateBucketMetadataInventoryTableConfiguration	(Obbligatorio) <code>s3:UpdateBucketMetadataInventoryTableConfiguration</code> , <code>s3tables:CreateTable</code> , <code>s3tables:CreateNamespace</code> , <code>s3tables:CreateTable</code> , <code>s3tables:GetTable</code> , <code>s3tables:PutTablePolicy</code> , <code>s3tables:PutTableEncryption</code> , <code>kms:DescribeKey</code>	<p>Richiesto per abilitare o disabilitare una tabella di inventario per una configurazione della tabella dei metadati su un bucket per uso generico.</p> <p>Se desideri crittografare la tabella dell'inventario con la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS), hai bisogno di autorizzazioni aggiuntive nella tua politica delle chiavi KMS. Per ulteriori informazioni, consulta the section called “Autorizzazioni per le tabelle di metadati”.</p>

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
UpdateBucketMetadataJournalTableConfiguration	(Obbligatorio) <code>s3:UpdateBucketMetadataJournalTableConfiguration</code>	Richiesto per abilitare o disabilitare la scadenza dei record della tabella del diario per una configurazione della tabella dei metadati su un bucket per uso generico.

Operazioni e autorizzazioni degli oggetti

Le operazioni sugli oggetti sono operazioni API S3 che operano sul tipo di risorsa oggetto. È necessario specificare le azioni delle policy S3 per le operazioni sugli oggetti nelle policy basate sulle risorse (come le policy bucket, le policy degli access point, le policy degli Access Point, le policy degli endpoint VPC) o le policy basate sull' Multi-Region identità IAM.

Nelle policy, l'elemento `Resource` deve essere l'ARN dell'oggetto. Per ulteriori informazioni sul formato dell'elemento `Resource` e su esempi di policy, consulta [Operazioni con gli oggetti](#).

Note

- AWS KMS le azioni politiche (`kms:GenerateDataKey`, `kms:Decrypt`) sono applicabili solo per il tipo di AWS KMS risorsa e devono essere specificate nelle politiche IAM basate sull'identità e nelle politiche basate sulle risorse (politiche chiave). AWS KMS AWS KMS Non è possibile specificare azioni AWS KMS politiche nelle politiche basate sulle risorse S3, come le politiche bucket S3.
- Quando si utilizzano i punti di accesso per controllare l'accesso alle operazioni degli oggetti, è possibile utilizzare le policy dei punti di accesso. Per concedere le autorizzazioni alle operazioni sugli oggetti nelle policy dei punti di accesso, tieni presente quanto segue:
 - Nelle policy dei punti di accesso che concedono autorizzazioni alle operazioni sugli oggetti, l'elemento `Resource` deve essere l'ARN degli oggetti a cui si accede tramite un punto di accesso. Per ulteriori informazioni sul formato dell'elemento `Resource` e su esempi di policy, consulta [Operazioni sugli oggetti nelle policy dei punti di accesso](#).
 - Non tutte le operazioni sugli oggetti sono supportate dai punti di accesso. Per ulteriori informazioni, consulta [Compatibilità dei punti di accesso con le operazioni S3](#).

- Non tutte le operazioni sugli oggetti sono supportate dagli Access Point. Multi-Region
Per ulteriori informazioni, consulta [Multi-Region Compatibilità degli Access Point con le operazioni S3](#).

Di seguito è riportata la mappatura delle operazioni degli oggetti e delle azioni di policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
AbortMultipartUpload	(Obbligatorio) <code>s3:AbortMultipartUpload</code>	Richiesto per interrompere un caricamento multiparte.
CompleteMultipartUpload	(Obbligatorio) <code>s3:PutObject</code>	Richiesto per completare un caricamento multiparte.
	(Obbligo condizionale) <code>kms:Decrypt</code>	Obbligatorio se si desidera completare un caricamento in più parti per un oggetto crittografato con chiave gestito dal AWS KMS cliente.
CopyObject	Per l'oggetto di origine:	Per l'oggetto di origine:
	(Obbligatorio) <code>s3:GetObject</code> o <code>s3:GetObjectVersion</code>	<ul style="list-style-type: none"> • <code>s3:GetObject</code> - Richiesto se si vuole copiare un oggetto dal bucket di origine senza specificare <code>versionId</code> nella richiesta. • <code>s3:GetObjectVersion</code> - Richiesto se si vuole copiare una versione specifica di un oggetto dal bucket di origine, specificando <code>versionId</code> nella richiesta.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>kms:Decrypt</code>	Obbligatorio se si desidera copiare un oggetto crittografato con chiave gestita dal AWS KMS cliente dal bucket di origine.
	Per l'oggetto di destinazione:	Per l'oggetto di destinazione:
	(Obbligatorio) <code>s3:PutObject</code>	Richiesto per inserire l'oggetto copiato nel bucket di destinazione.
	(Obbligo condizionale) <code>s3:PutObjectAcl</code>	Necessario se si desidera inserire l'oggetto copiato con la lista di controllo degli accessi (ACL) dell'oggetto nel bucket di destinazione quando si effettua una richiesta <code>CopyObject</code> .
	(Obbligo condizionale) <code>s3:PutObjectTagging</code>	Richiesto se si vuole mettere l'oggetto copiato con il tagging dell'oggetto nel bucket di destinazione quando si fa una richiesta a <code>CopyObject</code> .
	(Obbligo condizionale) <code>kms:GenerateDataKey</code>	Obbligatorio se si desidera crittografare l'oggetto copiato con una chiave gestita AWS KMS dal cliente e inserirlo nel bucket di destinazione.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>s3:PutObjectRetention</code>	Richiesto se si desidera impostare una configurazione di conservazione Object Lock per il nuovo oggetto.
	(Obbligo condizionale) <code>s3:PutObjectLegalHold</code>	Richiesto se si desidera inserire un blocco legale Object Lock del nuovo oggetto.
CreateMultipartUpload	(Obbligatorio) <code>s3:PutObject</code>	Richiesto per creare un caricamento multiparte.
	(Obbligo condizionale) <code>s3:PutObjectAcl</code>	Richiesto se si desidera impostare le autorizzazioni della lista di controllo degli accessi (ACL) per l'oggetto caricato.
	(Obbligo condizionale) <code>s3:PutObjectTagging</code>	Richiesto se si desidera aggiungere uno o più tag all'oggetto caricato.
	(Obbligo condizionale) <code>kms:GenerateDataKey</code>	Obbligatorio se si desidera utilizzare una chiave gestita AWS KMS dal cliente per crittografare un oggetto quando si avvia un caricamento in più parti.
	(Obbligo condizionale) <code>s3:PutObjectRetention</code>	Richiesto se si desidera impostare una configurazione di conservazione Object Lock per l'oggetto caricato.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>s3:PutObjectLegalHold</code>	Richiesto se si desidera applicare un blocco legale Object Lock all'oggetto caricato.
DeleteObject	(Obbligatorio) <code>s3:DeleteObject</code> o <code>s3:DeleteObjectVersion</code>	<ul style="list-style-type: none"> • <code>s3:DeleteObject</code> - Richiesto se si vuole rimuovere un oggetto senza specificare <code>versionId</code> nella richiesta. • <code>s3:DeleteObjectVersion</code> - Richiesto se si vuole rimuovere una versione specifica di un oggetto specificando <code>versionId</code> nella richiesta.
	(Obbligo condizionale) <code>s3:BypassGovernanceRetention</code>	Necessario se si desidera eliminare un oggetto protetto dalla modalità di governance per la conservazione Object Lock.
DeleteObjects	(Obbligatorio) <code>s3:DeleteObject</code> o <code>s3:DeleteObjectVersion</code>	<ul style="list-style-type: none"> • <code>s3:DeleteObject</code> - Richiesto se si vuole rimuovere un oggetto senza specificare <code>versionId</code> nella richiesta. • <code>s3:DeleteObjectVersion</code> - Richiesto se si vuole rimuovere una versione specifica di un oggetto specificando <code>versionId</code> nella richiesta.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>s3:BypassGovernanceRetention</code>	Necessario se si desidera eliminare gli oggetti protetti dalla modalità di governance per la conservazione Object Lock.
DeleteObjectTagging	(Obbligatorio) <code>s3:DeleteObjectTagging</code> o <code>s3:DeleteObjectVersionTagging</code>	<ul style="list-style-type: none"> • <code>s3:DeleteObjectTagging</code> - Richiesto se si vuole rimuovere l'intero set di tag di un oggetto senza specificare <code>versionId</code> nella richiesta. • <code>s3:DeleteObjectVersionTagging</code> - Richiesto se si desidera eliminare i tag di una versione specifica dell'oggetto specificando <code>versionId</code> nella richiesta.
GetObject	(Obbligatorio) <code>s3:GetObject</code> o <code>s3:GetObjectVersion</code>	<ul style="list-style-type: none"> • <code>s3:GetObject</code> - Richiesto se si vuole ottenere un oggetto senza specificare <code>versionId</code> nella richiesta. • <code>s3:GetObjectVersion</code> - Richiesto se si vuole ottenere una versione specifica di un oggetto specificando <code>versionId</code> nella richiesta.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>kms:Decrypt</code>	Obbligatorio se si desidera ottenere e decrittografare un oggetto crittografato con chiave gestita AWS KMS dal cliente.
	(Obbligo condizionale) <code>s3:GetObjectTagging</code>	Richiesto se si vuole ottenere il set di tag di un oggetto quando si fa una richiesta a <code>GetObject</code> .
	(Obbligo condizionale) <code>s3:GetObjectLegalHold</code>	Richiesto se si vuole ottenere lo stato attuale di blocco legale Object Lock di un oggetto.
	(Obbligo condizionale) <code>s3:GetObjectRetention</code>	Richiesto se si desidera recuperare le impostazioni di conservazione Object Lock per un oggetto.
GetObjectAcl	(Obbligatorio) <code>s3:GetObjectAcl</code> o <code>s3:GetObjectVersionAcl</code>	<ul style="list-style-type: none"> <code>s3:GetObjectAcl</code> - Richiesto se si vuole ottenere la lista di controllo degli accessi (ACL) di un oggetto senza specificare <code>versionId</code> nella richiesta. <code>s3:GetObjectVersionAcl</code> - Richiesto se si vuole ottenere la lista di controllo degli accessi (ACL) di un oggetto specificando <code>versionId</code> nella richiesta.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
GetObjectAttributes	(Obbligatorio) <code>s3:GetObject</code> o <code>s3:GetObjectVersion</code>	<ul style="list-style-type: none">• <code>s3:GetObject</code> - Richiesto se si vogliono recuperare gli attributi relativi a un oggetto senza specificare <code>versionId</code> nella richiesta.• <code>s3:GetObjectVersion</code> - Richiesto se si vogliono recuperare gli attributi relativi a una versione specifica dell'oggetto, specificando <code>versionId</code> nella richiesta.
	(Obbligo condizionale) <code>kms:Decrypt</code>	Obbligatorio se si desidera recuperare gli attributi relativi a un oggetto crittografato con chiave gestita AWS KMS dal cliente.
GetObjectLegalHold	(Obbligatorio) <code>s3:GetObjectLegalHold</code>	Richiesto per ottenere lo stato attuale di blocco legale Object Lock di un oggetto.
GetObjectRetention	(Obbligatorio) <code>s3:GetObjectRetention</code>	Richiesto per recuperare le impostazioni di conservazione Object Lock per un oggetto.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
GetObjectTagging	(Obbligatorio) s3:GetObjectTagging o s3:GetObjectVersionTagging	<ul style="list-style-type: none"> s3:GetObjectTagging - Richiesto se si vuole ottenere il set di tag di un oggetto senza specificare versionId nella richiesta. s3:GetObjectVersionTagging - Richiesto se si desidera ottenere i tag di una versione specifica dell'oggetto specificando versionId nella richiesta.
GetObjectTorrent	(Obbligatorio) s3:GetObject	Richiesto per restituire i file torrent di un oggetto.
HeadObject	(Obbligatorio) s3:GetObject	Richiesto per recuperare i metadati da un oggetto senza restituire l'oggetto stesso.
	(Obbligo condizionale) s3:GetObjectLegalHold	Richiesto se si vuole ottenere lo stato attuale di blocco legale Object Lock di un oggetto.
	(Obbligo condizionale) s3:GetObjectRetention	Richiesto se si desidera recuperare le impostazioni di conservazione Object Lock per un oggetto.
ListMultipartUploads	(Obbligatorio) s3:ListBucketMultipartUploads	Richiesto per elencare i caricamenti multiparte in corso in un bucket.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
ListParts	(Obbligatorio) <code>s3:ListMultipartUploadParts</code>	Richiesto per elencare le parti che sono state caricate per uno specifico caricamento multiparte.
	(Obbligo condizionale) <code>kms:Decrypt</code>	Obbligatorio se si desidera elencare parti di un caricamento multiparte crittografato con chiave gestita dal AWS KMS cliente.
PutObject	(Obbligatorio) <code>s3:PutObject</code>	Richiesto per inserire un oggetto.
	(Obbligo condizionale) <code>s3:PutObjectAcl</code>	Richiesto se si desidera inserire la lista di controllo degli accessi (ACL) dell'oggetto quando si effettua una richiesta <code>PutObject</code> .
	(Obbligo condizionale) <code>s3:PutObjectTagging</code>	Richiesto se si vuole inserire l'etichetta dell'oggetto quando si fa una richiesta a <code>PutObject</code> .
	(Obbligo condizionale) <code>kms:GenerateDataKey</code>	Obbligatorio se si desidera crittografare un oggetto con una chiave gestita AWS KMS dal cliente.
	(Obbligo condizionale) <code>s3:PutObjectRetention</code>	Richiesto se si desidera impostare una configurazione di conservazione Object Lock per un oggetto.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>s3:PutObjectLegalHold</code>	Richiesto se si desidera applicare una configurazione di Blocco legale Object Lock a un oggetto specificato.
<u>PutObjectAcl</u>	(Obbligatorio) <code>s3:PutObjectAcl</code> o <code>s3:PutObjectVersionAcl</code>	<ul style="list-style-type: none"> <code>s3:PutObjectAcl</code> - Necessario se si desidera impostare le autorizzazioni della lista di controllo degli accessi (ACL) per un oggetto nuovo o esistente senza specificare <code>versionId</code> nella richiesta. <code>s3:PutObjectVersionAcl</code> - Necessario se si desidera impostare le autorizzazioni della lista di controllo degli accessi (ACL) per un oggetto nuovo o esistente, specificando <code>versionId</code> nella richiesta.
<u>PutObjectLegalHold</u>	(Obbligatorio) <code>s3:PutObjectLegalHold</code>	Richiesto per applicare una configurazione di Blocco legale Object Lock a un oggetto.
<u>PutObjectRetention</u>	(Obbligatorio) <code>s3:PutObjectRetention</code>	Richiesto per applicare una configurazione di conservazione Object Lock per un oggetto.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>s3:BypassGovernanceRetention</code>	Necessario se si desidera bypassare la modalità di governance di una configurazione di conservazione Object Lock.
PutObjectTagging	(Obbligatorio) <code>s3:PutObjectTagging</code> o <code>s3:PutObjectVersionTagging</code>	<ul style="list-style-type: none"> <code>s3:PutObjectTagging</code> - Richiesto se si vuole impostare il set di tag fornito a un oggetto che esiste già in un bucket, senza specificare <code>versionId</code> nella richiesta. <code>s3:PutObjectVersionTagging</code> - Richiesto se si vuole impostare il set di tag fornito a un oggetto che esiste già in un bucket, specificando <code>versionId</code> nella richiesta.
RestoreObject	(Obbligatorio) <code>s3:RestoreObject</code>	Richiesto per ripristinare una copia di un oggetto archiviato.
SelectObjectContent	(Obbligatorio) <code>s3:GetObject</code>	Richiesto per filtrare il contenuto di un oggetto S3 in base a una semplice istruzione SQL (Structured Query Language).

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>kms:Decrypt</code>	Obbligatorio se si desidera filtrare il contenuto di un oggetto S3 crittografato con una chiave gestita AWS KMS dal cliente.
UpdateObjectEncryption	(Obbligatorio) <code>s3:UpdateObjectEncryption</code> , <code>kms:Encrypt</code> , <code>kms:Decrypt</code> , <code>kms:GenerateDataKey</code> , <code>kms:ReEncrypt*</code>	Obbligatorio se desideri modificare gli oggetti crittografati tra la crittografia lato server con crittografia gestita Amazon S3 (SSE-S3) e la crittografia lato server con chiavi di crittografia () AWS Key Management Service (AWS KMS). SSE-KMS Puoi anche utilizzare l' <code>UpdateObjectEncryption</code> operazione e per applicare S3 Bucket Keys per ridurre i costi delle AWS KMS richieste o modificare la chiave KMS gestita dal cliente utilizzata per crittografare i dati in modo da rispettare gli standard personalizzati di rotazione delle chiavi.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
	(Obbligo condizionale) <code>organizations:DescribeAccount</code>	<p>Se stai utilizzando AWS Organizations, per utilizzare l'operazione <code>UpdateObjectEncryption</code> con chiavi KMS gestite dal cliente provenienti da altri membri della tua organizzazione, devi disporre dell'autorizzazione. Account AWS <code>organizations:DescribeAccount</code></p> <div data-bbox="1068 831 1507 1381"> <p> Note</p> <p>È inoltre necessario richiedere la possibilità di utilizzare account AWS KMS keys di proprietà di altri membri all'interno dell'organizzazione contattando. Supporto AWS</p> </div>
UploadPart	(Obbligatorio) <code>s3:PutObject</code>	Richiesto per caricare una parte in un caricamento multiparte.
	(Obbligo condizionale) <code>kms:GenerateDataKey</code>	Obbligatorio se si desidera inserire una parte di caricamento e crittografarla con una chiave gestita AWS KMS dal cliente.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
UploadPartCopy	Per l'oggetto di origine:	Per l'oggetto di origine:
	(Obbligatorio) <code>s3:GetObject</code> o <code>s3:GetObjectVersion</code>	<ul style="list-style-type: none"> <code>s3:GetObject</code> - Richiesto se si vuole copiare un oggetto dal bucket di origine senza specificare <code>versionId</code> nella richiesta. <code>s3:GetObjectVersion</code> - Richiesto se si vuole copiare una versione specifica di un oggetto dal bucket di origine, specificando <code>versionId</code> nella richiesta.
	(Obbligo condizionale) <code>kms:Decrypt</code>	Obbligatorio se si desidera copiare un oggetto crittografato con chiave gestita dal AWS KMS cliente dal bucket di origine.
	Per la parte di destinazione:	Per la parte di destinazione:
	(Obbligatorio) <code>s3:PutObject</code>	Richiesto per caricare una parte di caricamento multipart e nel bucket di destinazione.
	(Obbligo condizionale) <code>kms:GenerateDataKey</code>	Obbligatorio se si desidera crittografare una parte con una chiave gestita AWS KMS dal cliente quando si carica la parte nel bucket di destinazione.

Operazioni sui punti di accesso di bucket per uso generico e autorizzazioni

Le operazioni sui punti di accesso sono operazioni API S3 che operano sul tipo di risorsa `accesspoint`. È necessario specificare le azioni delle policy S3 per le operazioni dei punti di accesso nelle policy IAM basate sull'identità, non nelle policy dei bucket o dei punti di accesso.

Nelle policy, l'elemento `Resource` deve essere l'ARN `accesspoint`. Per ulteriori informazioni sul formato dell'elemento `Resource` e su esempi di policy, consulta [Operazioni sui punti di accesso di bucket per uso generico](#).

Note

Se desideri utilizzare i punti di accesso per controllare l'accesso alle operazioni sui bucket o sugli oggetti, tieni presente quanto segue:

- Per l'utilizzo dei punti di accesso per controllare l'accesso alle operazioni del bucket, consulta [Operazioni su bucket nelle policy per i punti di accesso di bucket per uso generico](#).
- Per l'utilizzo dei punti di accesso per controllare l'accesso alle operazioni sugli oggetti, consulta [Operazioni sugli oggetti nelle policy dei punti di accesso](#).
- Per ulteriori informazioni su come configurare le policy dei punti di accesso, consulta [Configurazione delle policy IAM per l'utilizzo degli access point](#).

Di seguito è riportata la mappatura delle operazioni dei punti di accesso e delle azioni di policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
CreateAccessPoint	(Obbligatorio) <code>s3:CreateAccessPoint</code>	Richiesto per creare un punto di accesso associato a un bucket S3.
DeleteAccessPoint	(Obbligatorio) <code>s3:DeleteAccessPoint</code>	Richiesto per eliminare un punto di accesso.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteAccessPointPolicy	(Obbligatorio) s3:DeleteAccessPointPolicy	Richiesto per eliminare una policy del punto di accesso.
GetAccessPointPolicy	(Obbligatorio) s3:GetAccessPointPolicy	Richiesto per recuperare una policy del punto di accesso.
GetAccessPointPolicyStatus	(Obbligatorio) s3:GetAccessPointPolicyStatus	Richiesto per recuperare le informazioni sul fatto che il punto di accesso specifica to abbia attualmente una policy che consente l'accesso pubblico.
PutAccessPointPolicy	(Obbligatorio) s3:PutAccessPointPolicy	Richiesto per inserire una policy del punto di accesso.

Operazioni e autorizzazioni del punto di accesso Lambda per oggetti

Le operazioni sui punti di accesso Lambda per oggetti sono operazioni API S3 che operano sul tipo di risorsa `objectlambdaaccesspoint`. Per ulteriori informazioni su come configurare le policy per le operazioni sui punti di accesso Lambda per oggetti, consulta [Configurazione delle policy IAM per i punti di accesso Lambda per oggetti](#).

Di seguito è riportata la mappatura delle operazioni sui punti di accesso Lambda per oggetti e delle azioni di policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
CreateAccessPointForObjectLambda	(Obbligatorio) s3:CreateAccessPointForObjectLambda	Richiesto per creare un punto di accesso Lambda per oggetti.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteAccessPointForObjectLambda	(Obbligatorio) s3:DeleteAccessPointForObjectLambda	Richiesto per eliminare un punto di accesso Lambda per oggetti specificato.
DeleteAccessPointPolicyForObjectLambda	(Obbligatorio) s3:DeleteAccessPointPolicyForObjectLambda	Richiesto per eliminare la policy di un punto di accesso Lambda per oggetti specificato.
GetAccessPointConfigurationForObjectLambda	(Obbligatorio) s3:GetAccessPointConfigurationForObjectLambda	Richiesto per recuperare la configurazione del punto di accesso Lambda per oggetti.
GetAccessPointForObjectLambda	(Obbligatorio) s3:GetAccessPointForObjectLambda	Richiesto per recuperare le informazioni sul punto di accesso Lambda per oggetti.
GetAccessPointPolicyForObjectLambda	(Obbligatorio) s3:GetAccessPointPolicyForObjectLambda	Richiesto per restituire la policy del punto di accesso associata al punto di accesso Lambda per oggetti specificato.
GetAccessPointPolicyStatusForObjectLambda	(Obbligatorio) s3:GetAccessPointPolicyStatusForObjectLambda	Richiesto per restituire lo stato della policy per una specifica policy del punto di accesso Lambda per oggetti.
PutAccessPointConfigurationForObjectLambda	(Obbligatorio) s3:PutAccessPointConfigurationForObjectLambda	Richiesto per impostare la configurazione del punto di accesso Lambda per oggetti.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
PutAccessPointPolicyForObjectLambda	(Obbligatorio) <code>s3:PutAccessPointPolicyForObjectLambda</code>	Richiesto per associare una policy di accesso a un punto di accesso Lambda per oggetti specificato.

Multi-Region Operazioni e autorizzazioni dell'Access Point

Multi-Region Le operazioni degli Access Point sono operazioni API S3 che operano sul tipo di `multiregionaccesspoint` risorsa. Per ulteriori informazioni su come configurare le politiche per le operazioni Multi-Region degli Access Point, vedere [Multi-Region Esempi di politiche relative agli Access Point](#).

Di seguito è riportata la mappatura delle operazioni degli Multi-Region Access Point e delle azioni politiche richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
CreateMultiRegionAccessPoint	(Obbligatorio) <code>s3:CreateMultiRegionAccessPoint</code>	Necessario per creare un Multi-Region Access Point e associarlo ai bucket S3.
DeleteMultiRegionAccessPoint	(Obbligatorio) <code>s3:DeleteMultiRegionAccessPoint</code>	Necessario per eliminare un Multi-Region Access Point.
DescribeMultiRegionAccessPointOperation	(Obbligatorio) <code>s3:DescribeMultiRegionAccessPointOperation</code>	Necessario per recuperare lo stato di una richiesta asincrona per la gestione di un Access Point. Multi-Region
GetMultiRegionAccessPoint	(Obbligatorio) <code>s3:GetMultiRegionAccessPoint</code>	Necessario per restituire le informazioni di configurazione

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
		sull'Access Point specificato. Multi-Region
GetMultiRegionAccessPointPolicy	(Obbligatorio) s3:GetMultiRegionAccessPointPolicy	Necessario per restituire la politica di controllo degli accessi dell' Multi-Region Access Point specificato.
GetMultiRegionAccessPointPolicyStatus	(Obbligatorio) s3:GetMultiRegionAccessPointPolicyStatus	Necessario per restituire lo stato della politica per un punto di Multi-Region accesso specifico, indicando se il punto di Multi-Region accesso specificato dispone di una politica di controllo degli accessi che consente l'accesso pubblico.
GetMultiRegionAccessPointRoutes	(Obbligatorio) s3:GetMultiRegionAccessPointRoutes	Necessario per restituire la configurazione di routing per un Multi-Region Access Point.
PutMultiRegionAccessPointPolicy	(Obbligatorio) s3:PutMultiRegionAccessPointPolicy	Necessario per aggiornare la politica di controllo degli accessi dell' Multi-Region Access Point specificato.
SubmitMultiRegionAccessPointRoutes	(Obbligatorio) s3:SubmitMultiRegionAccessPointRoutes	Necessario per inviare una configurazione di percorso aggiornata per un Multi-Region Access Point.

Operazioni e autorizzazioni per i processi batch

(Operazioni in batch) Le operazioni di processo sono operazioni API S3 che operano sul tipo di risorsa `job`. È necessario specificare le azioni delle policy S3 per le operazioni di processo nelle policy IAM basate sull'identità, non nelle policy dei bucket.

Nelle policy, l'elemento `Resource` deve essere l'ARN `job`. Per ulteriori informazioni sul formato dell'elemento `Resource` e su esempi di policy, consulta [Operazioni di processo in batch](#).

Di seguito è riportata la mappatura delle operazioni dei processi batch e delle azioni di policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteJobTagging	(Obbligatorio) <code>s3:DeleteJobTagging</code>	Richiesto per rimuovere i tag da un processo di Operazioni in batch S3 esistente.
DescribeJob	(Obbligatorio) <code>s3:DescribeJob</code>	Richiesto per recuperare i parametri di configurazione e lo stato di un processo di Operazioni in batch.
GetJobTagging	(Obbligatorio) <code>s3:GetJobTagging</code>	Richiesto per restituire il set di tag di un processo di Operazioni in batch S3 esistente.
PutJobTagging	(Obbligatorio) <code>s3:PutJobTagging</code>	Richiesto per inserire o sostituire i tag in un processo di Operazioni in batch S3 esistente.
UpdateJobPriority	(Obbligatorio) <code>s3:UpdateJobPriority</code>	Richiesto per aggiornare la priorità di un processo esistente.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
UpdateJobStatus	(Obbligatorio) s3:UpdateJobStatus	Richiesto per aggiornare lo stato del processo specificato.

Operazioni e autorizzazioni di configurazione di S3 Storage Lens

Le operazioni di configurazione di S3 Storage Lens sono operazioni API S3 che operano sul tipo di risorsa `storagelensconfiguration`. Per ulteriori informazioni su come configurare le operazioni di configurazione di S3 Storage Lens, consulta [Impostazione delle autorizzazioni di Amazon S3 Storage Lens](#).

Di seguito è riportata la mappatura delle operazioni di configurazione di S3 Storage Lens e delle azioni delle policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteStorageLensConfiguration	(Obbligatorio) s3:DeleteStorageLensConfiguration	Richiesto per eliminare la configurazione di Storage Lens S3.
DeleteStorageLensConfigurationTagging	(Obbligatorio) s3:DeleteStorageLensConfigurationTagging	Necessario per eliminare i tag di configurazione di S3 Storage Lens.
GetStorageLensConfiguration	(Obbligatorio) s3:GetStorageLensConfiguration	Richiesto per ottenere la configurazione di S3 Storage Lens.
GetStorageLensConfigurationTagging	(Obbligatorio) s3:GetStorageLensConfigurationTagging	Richiesto per ottenere i tag della configurazione di S3 Storage Lens.
PutStorageLensConfigurationTagging	(Obbligatorio) s3:PutStorageLensConfigurationTagging	Richiesto per inserire o sostituire i tag in una configurazione.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
		zione S3 Storage Lens esistente.

Operazioni e autorizzazioni dei gruppi S3 Storage Lens

Le operazioni dei gruppi S3 Storage Lens sono operazioni API S3 che operano sul tipo di risorsa `storagelensgroup`. Per ulteriori informazioni su come configurare le autorizzazioni dei gruppi S3 Storage Lens, consulta [Autorizzazioni gruppi Storage Lens](#).

Di seguito è riportata la mappatura delle operazioni dei gruppi S3 Storage Lens e delle azioni delle policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteStorageLensGroup	(Obbligatorio) <code>s3:DeleteStorageLensGroup</code>	Richiesto per eliminare un gruppo S3 Storage Lens esistente.
GetStorageLensGroup	(Obbligatorio) <code>s3:GetStorageLensGroup</code>	Richiesto per recuperare i dettagli di configurazione del gruppo S3 Storage Lens.
UpdateStorageLensGroup	(Obbligatorio) <code>s3:UpdateStorageLensGroup</code>	Richiesto per aggiornare il gruppo S3 Storage Lens esistente.
CreateStorageLensGroup	(Obbligatorio) <code>s3:CreateStorageLensGroup</code>	Richiesto per creare un gruppo Storage Lens.
CreateStorageLensGroup , TagResource	(Obbligatorio) <code>s3:CreateStorageLensGroup</code> , <code>s3:TagResource</code>	Richiesto per creare un nuovo gruppo Storage Lens con tag.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
ListStorageLensGroups	(Obbligatorio) <code>s3:ListStorageLensGroups</code>	Richiesto per elencare tutti i gruppi Storage Lens nella Regione di origine.
ListTagsForResource	(Obbligatorio) <code>s3:ListTagsForResource</code>	Richiesto per elencare i tag aggiunti al gruppo Storage Lens.
TagResource	(Obbligatorio) <code>s3:TagResource</code>	Richiesto per aggiungere o aggiornare un tag di gruppo Storage Lens per un gruppo Storage Lens esistente.
UntagResource	(Obbligatorio) <code>s3:UntagResource</code>	Richiesto per eliminare un tag da un gruppo Storage Lens.

Operazioni sull'istanza S3 Access Grants e autorizzazioni

Le operazioni sull'istanza S3 Access Grants sono operazioni API S3 che operano sul tipo di risorsa `accessgrantsinstance`. Un'istanza S3 Access Grants è un container logico per le concessioni di accesso. Per ulteriori informazioni su come utilizzare le istanze S3 Access Grants, consulta [Operazioni con le istanze S3 Access Grants](#).

Di seguito è riportata la mappatura delle operazioni di configurazione dell'istanza S3 Access Grants e delle azioni delle policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
AssociateAccessGrantsIdentityCenter	(Obbligatorio) <code>s3:AssociateAccessGrantsIdentityCenter</code>	Necessario per associare un' Centro identità AWS IAM istanza alla tua istanza S3 Access Grants, consentendo così di creare autorizzazioni di accesso per utenti e

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
		<p>gruppi nella tua directory di identità aziendale. È necessario disporre delle seguenti autorizzazioni:</p> <p><code>sso:CreateApplication</code> , <code>sso:PutApplicationGrant</code> e <code>sso:PutApplicationAuthenticationMethod</code> .</p>
CreateAccessGrantsInstance	(Obbligatorio) <code>s3:CreateAccessGrantsInstance</code>	<p>Richiesto per creare un'istanza S3 Access Grants (risorsa <code>accessgrantsinstance</code>) che funge da container per le concessioni di accesso individuali.</p> <p>Per associare un' Centro identità AWS IAM istanza alla tua istanza S3 Access Grants, devi disporre anche delle autorizzazioni <code>sso:DescribeInstance</code> ,, <code>sso:CreateApplication</code> e <code>sso:PutApplicationGrant</code> <code>sso:PutApplicationAuthenticationMethod</code></p>

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteAccessGrantsInstance	(Obbligatorio) <code>s3:DeleteAccessGrantsInstance</code>	Necessario per eliminare un'istanza (accessgrantsinstance risorsa) di S3 Access Grants da un account. Regione AWS
DeleteAccessGrantsInstanceResourcePolicy	(Obbligatorio) <code>s3:DeleteAccessGrantsInstanceResourcePolicy</code>	Richiesto per eliminare una policy delle risorse per l'istanza S3 Access Grants.
DissociateAccessGrantsIdentityCenter	(Obbligatorio) <code>s3:DissociateAccessGrantsIdentityCenter</code>	Necessario per dissociare un' Centro identità AWS IAM istanza dalla tua istanza S3 Access Grants. È necessario disporre delle seguenti autorizzazioni: <code>sso:DeleteApplication</code>
GetAccessGrantsInstance	(Obbligatorio) <code>s3:GetAccessGrantsInstance</code>	Necessario per recuperare l'istanza S3 Access Grants per un account. Regione AWS
GetAccessGrantsInstanceForPrefix	(Obbligatorio) <code>s3:GetAccessGrantsInstanceForPrefix</code>	Richiesto per recuperare l'istanza S3 Access Grants che contiene un particolare prefisso.
GetAccessGrantsInstanceResourcePolicy	(Obbligatorio) <code>s3:GetAccessGrantsInstanceResourcePolicy</code>	Necessario per restituire la politica delle risorse dell'istanza S3 Access Grants.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
ListAccessGrantsInstances	(Obbligatorio) <code>s3:ListAccessGrantsInstances</code>	Richiesto per restituire un elenco delle istanze S3 Access Grants nell'account in uso.
PutAccessGrantsInstanceResourcePolicy	(Obbligatorio) <code>s3:PutAccessGrantsInstanceResourcePolicy</code>	Richiesto per aggiungere o aggiornare la policy delle risorse dell'istanza S3 Access Grants.

Operazioni sulla posizione S3 Access Grants e autorizzazioni

Le operazioni sulla posizione S3 Access Grants sono operazioni API S3 che operano sul tipo di risorsa `accessgrantslocation`. Per ulteriori informazioni su come utilizzare le posizioni S3 Access Grants, consulta [Operazioni con le posizioni S3 Access Grants](#).

Di seguito è riportata la mappatura delle operazioni sulla posizione S3 Access Grants e delle azioni delle policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
CreateAccessGrantsLocation	(Obbligatorio) <code>s3:CreateAccessGrantsLocation</code>	Richiesto per registrare una posizione nell'istanza S3 Access Grants (creare una risorsa <code>accessgrantslocation</code>). È inoltre necessario disporre della seguente autorizzazione per il ruolo IAM specificato: <code>iam:PassRole</code>

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
DeleteAccessGrantsLocation	(Obbligatorio) s3:DeleteAccessGrantsLocation	Richiesto per rimuovere una posizione registrata dall'istanza S3 Access Grants.
GetAccessGrantsLocation	(Obbligatorio) s3:GetAccessGrantsLocation	Richiesto per recuperare i dettagli di una posizione particolare registrata nell'istanza S3 Access Grants.
ListAccessGrantsLocations	(Obbligatorio) s3:ListAccessGrantsLocations	Richiesto per restituire un elenco delle posizioni registrate e nell'istanza S3 Access Grants.
UpdateAccessGrantsLocation	(Obbligatorio) s3:UpdateAccessGrantsLocation	Richiesto per aggiornare il ruolo IAM di una posizione registrata con l'istanza S3 Access Grants.

Operazioni sulla concessione S3 Access Grants e autorizzazioni

Le operazioni sulla concessione S3 Access Grants sono operazioni API S3 che operano sul tipo di risorsa `accessgrant`. Per ulteriori informazioni su come utilizzare le concessioni individuali utilizzando S3 Access Grants, consulta [Operazioni con le concessioni in S3 Access Grants](#).

Di seguito è riportata la mappatura delle operazioni di configurazione delle concessioni S3 Access Grants e delle azioni di policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
CreateAccessGrant	(Obbligatorio) s3:CreateAccessGrant	Richiesto per creare un'a concessione individuale (risorsa <code>accessgrant</code>) per un utente o un gruppo

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
		<p>nell'istanza S3 Access Grants. È necessario disporre delle seguenti autorizzazioni:</p> <p>Per qualsiasi identità della directory: <code>sso:DescribeInstance</code> e <code>sso:DescribeApplication</code></p> <p>Per gli utenti della directory: <code>identitystore:DescribeUser</code></p>
DeleteAccessGrant	(Obbligatorio) <code>s3:DeleteAccessGrant</code>	Richiesto per eliminare una concessione di accesso individuale (risorsa <code>accessgrant</code>) dall'istanza S3 Access Grants.
GetAccessGrant	(Obbligatorio) <code>s3:GetAccessGrant</code>	Richiesto per ottenere i dettagli su una concessione di accesso individuale nell'istanza S3 Access Grants.
ListAccessGrants	(Obbligatorio) <code>s3:ListAccessGrants</code>	Richiesto per restituire un elenco di concessioni di accesso individuali nell'istanza S3 Access Grants.
ListCallerAccessGrants	(Obbligatorio) <code>s3:ListCallerAccessGrants</code>	Richiesto per elencare le concessioni di accesso che consentono al chiamante di accedere ai dati Amazon S3 tramite S3 Access Grants.

Operazioni e autorizzazioni dell'account

Le operazioni sugli account sono operazioni API S3 che operano a livello di account. L'account non è un tipo di risorsa definito da Amazon S3. È necessario specificare le azioni delle policy S3 per le operazioni degli account nelle policy IAM basate sull'identità, non nelle policy dei bucket.

Nelle policy, l'elemento `Resource` deve essere `"*"`. Per ulteriori informazioni sulle policy di esempio, consulta [Operazioni sugli account](#).

Di seguito è riportata la mappatura delle operazioni dell'account e delle azioni di policy richieste.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
CreateJob	(Obbligatorio) <code>s3:CreateJob</code>	Richiesto per creare un nuovo processo di Operazioni in batch S3.
CreateStorageLensGroup	(Obbligatorio) <code>s3:CreateStorageLensGroup</code>	Necessario per creare un nuovo gruppo S3 Storage Lens e associarlo all'ID specificato. Account AWS
	(Obbligo condizionale) <code>s3:TagResource</code>	Obbligatorio se si desidera creare un gruppo S3 Storage Lens con tag di AWS risorse.
DeletePublicAccessBlock (Account-level)	(Obbligatorio) <code>s3:PutAccountPublicAccessBlock</code>	Richiesto per rimuovere la configurazione di blocco dell'accesso pubblico da Account AWS.
GetAccessPoint	(Obbligatorio) <code>s3:GetAccessPoint</code>	Richiesto per recuperare le informazioni di configurazione del punto di accesso specificato.

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
GetAccessPointPolicy (Account-level)	(Obbligatorio) <code>s3:GetAccountPublicAccessBlock</code>	Richiesto per recuperare la configurazione del blocco di accesso pubblico per Account AWS.
ListAccessPoints	(Obbligatorio) <code>s3:ListAccessPoints</code>	Richiesto per elencare i punti di accesso di un bucket S3 di proprietà di un Account AWS.
ListAccessPointsForObjectLambda	(Obbligatorio) <code>s3:ListAccessPointsForObjectLambda</code>	Richiesto per elencare i punti di accesso Lambda per oggetti.
ListBuckets	(Obbligatorio) <code>s3:ListAllMyBuckets</code>	Richiesto per restituire un elenco di tutti i bucket di proprietà del mittente autenticato della richiesta.
ListJobs	(Obbligatorio) <code>s3:ListJobs</code>	Si richiede di elencare i processi attuali e quelli terminati di recente.
ListMultiRegionAccessPoints	(Obbligatorio) <code>s3:ListMultiRegionAccessPoints</code>	Necessario per restituire un elenco dei punti di Multi-Region accesso attualmente associati a quelli Account AWS specificati.
ListStorageLensConfigurations	(Obbligatorio) <code>s3:ListStorageLensConfigurations</code>	Necessario per ottenere un elenco delle configurazioni di S3 Storage Lens per un Account AWS

operazioni API	Azioni di policy	Descrizione delle azioni delle policy
ListStorageLensGroups	(Obbligatorio) <code>s3:ListStorageLensGroups</code>	Richiesto per elencare tutti i gruppi S3 Storage Lens nella home specificata Regione AWS.
PutPublicAccessBlock (Account-level)	(Obbligatorio) <code>s3:PutAccountPublicAccessBlock</code>	Richiesto per creare o modificare la configurazione del blocco di accesso pubblico per Account AWS.
PutStorageLensConfiguration	(Obbligatorio) <code>s3:PutStorageLensConfiguration</code>	Richiesto per mettere una configurazione di S3 Storage Lens.

Policy e autorizzazioni in Amazon S3

Questa pagina fornisce una panoramica delle policy relative ai bucket e agli utenti in Amazon S3 e descrive gli elementi di base di una policy AWS Identity and Access Management (IAM). Ogni elemento elencato è collegato a ulteriori dettagli ed esempi su come usare l'elemento.

Per un elenco completo di azioni, risorse e condizioni di Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

In termini basilari, una policy contiene i seguenti elementi:

- [Resource](#) - Il bucket Amazon S3, l'oggetto, il punto di accesso o il processo a cui si applica la policy. Usa il nome della risorsa Amazon (ARN) del bucket, dell'oggetto, del punto di accesso o del processo per identificare la risorsa.

Un esempio di operazioni a livello di bucket:

```
"Resource": "arn:aws:s3:::bucket_name"
```

Esempi di operazioni a livello di oggetto:

- "Resource": "arn:aws:s3:::*bucket_name*/*" per tutti gli oggetti del bucket.
- "Resource": "arn:aws:s3:::*bucket_name/prefix*/*" per gli oggetti sotto un certo prefisso nel bucket.

Per ulteriori informazioni, consulta [Risorse di policy per Amazon S3](#).

- [Actions](#) - Per ogni risorsa, Amazon S3 supporta una serie di operazioni. Vengono identificate le operazioni delle risorse che verranno consentite (o rifiutate) utilizzando le parole chiave dell'operazione.

Ad esempio, l'autorizzazione `s3:ListBucket` consente all'utente di utilizzare l'operazione Amazon S3 [ListObjectsV2](#) di Amazon (il permesso `s3:ListBucket` è un caso in cui il nome dell'azione non corrisponde direttamente al nome dell'operazione). Per ulteriori informazioni sull'uso di operazioni con Simple Storage Service (Amazon S3), consulta [Azioni di policy per Amazon S3](#). Per un elenco completo delle azioni di Amazon S3, consulta [Azioni](#) in Riferimento API di Amazon Simple Storage Service.

- [Effect](#) - Quale sarà l'effetto quando l'utente richiederà l'azione specifica: può essere Allow o Deny.

USE non concedi esplicitamente (consenti) l'accesso a una risorsa, l'accesso viene implicitamente rifiutato. È anche possibile negare esplicitamente l'accesso a una risorsa. È possibile eseguire questa operazione per accertarsi che un utente non sia in grado di accedere a una risorsa, anche se l'accesso viene concesso da un'altra policy. Per ulteriori informazioni, consulta [Elementi delle policy JSON IAM: Effect](#) nella Guida per l'utente di IAM.

- [Principal](#) - L'account o l'utente a cui è consentito l'accesso alle azioni e alle risorse nell'istruzione. In una policy di bucket l'entità principale è l'utente, l'account, il servizio o un'altra entità destinataria di questa autorizzazione. Per ulteriori informazioni, consulta [Principali per le policy dei bucket](#).
- [Condition](#) - Condizioni per l'entrata in vigore di una policy. Puoi utilizzare chiavi AWS larghe e chiavi specifiche di Amazon S3 per specificare le condizioni in una politica di accesso di Amazon S3. Per ulteriori informazioni, consulta [Esempi di policy per i bucket che utilizzano le chiavi di condizione](#).

Il seguente esempio di policy del bucket mostra gli elementi Effect, Principal, Action e Resource. Questa policy consente a *Akua*, un utente dell'account *123456789012*, `s3:GetObject`, `s3:GetBucketLocation` e `s3:ListBucket` di ottenere le autorizzazioni per Amazon S3 sul bucket *amzn-s3-demo-bucket1*.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "ExamplePolicy01",
  "Statement": [
    {
      "Sid": "ExampleStatement01",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Akua"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        "arn:aws:s3:::amzn-s3-demo-bucket1"
      ]
    }
  ]
}
```

Per informazioni complete sul linguaggio delle policy, consulta [Policy e autorizzazioni in IAM](#) e [Riferimento alle policy IAM JSON](#) nella Guida all'utente IAM.

Delega delle autorizzazioni

Se un utente Account AWS possiede una risorsa, può concedere tali autorizzazioni a un altro Account AWS. Tale account a sua volta può delegare le autorizzazioni, o una parte di esse, agli utenti al suo interno. Si parla di delega del permesso. Un account che riceve permessi da un altro account non può delegare autorizzazioni multi-account a un altro Account AWS.

Proprietà di bucket e oggetti di Amazon S3

I bucket e gli oggetti sono risorse di Amazon S3. Per impostazione predefinita, solo il proprietario della risorsa è in grado di accedervi. Il proprietario della risorsa si riferisce a colui Account AWS che crea la risorsa. Ad esempio:

- Le Account AWS risorse utilizzate per creare bucket e caricare oggetti sono le proprietarie di tali risorse.
- Se carichi un oggetto utilizzando le credenziali utente o di ruolo AWS Identity and Access Management (IAM), l'oggetto a Account AWS cui appartiene l'utente o il ruolo è proprietario dell'oggetto.
- Un proprietario del bucket può concedere a un altro Account AWS (o agli utenti di un altro account) autorizzazioni multiaccount per caricare gli oggetti. In questo caso, gli oggetti appartengono all'Account AWS che li carica. Il proprietario del bucket non dispone di autorizzazioni sugli oggetti di cui sono proprietari altri account, con le seguenti eccezioni:
 - È il proprietario del bucket a pagare la fattura. Il proprietario del bucket può rifiutare l'accesso agli oggetti nel bucket o eliminarli, indipendentemente dall'utente a cui appartengono.
 - Il proprietario del bucket può archiviare gli oggetti nel bucket o ripristinarli, indipendentemente dall'utente a cui appartengono. L'archiviazione fa riferimento alla classe di storage utilizzata per archiviare gli oggetti. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#).

Proprietà e autenticazione delle richieste

Tutte le richieste a un bucket possono essere autenticate o non autenticate. Le richieste autenticate devono includere un valore di firma che autentichi il mittente della richiesta, mentre non è necessario per le richieste non autenticate. Per ulteriori informazioni sull'autenticazione delle richieste, consulta [Esecuzione di richieste](#) nella documentazione di riferimento delle API di Amazon S3.

Un proprietario di bucket può consentire richieste non autenticate. Ad esempio, le richieste non autenticate [PutObject](#) sono consentite quando un bucket ha una policy di bucket pubblica o quando una ACL del bucket concede l'accesso a WRITE o FULL_CONTROL al gruppo All Users o all'utente anonimo. Per ulteriori informazioni sulle policy dei bucket pubblici e sulle liste di controllo degli accessi (ACL) pubbliche, consulta [Significato di "pubblico"](#).

Tutte le richieste non autenticate sono fatte dall'utente anonimo. Questo utente viene rappresentato dall'ID utente canonico specifico 65a011a29cdf8ec533ec3d1c0aae921c nelle ACL. Se un oggetto viene caricato in un bucket tramite una richiesta non autenticata, la proprietà dell'oggetto è dell'utente anonimo. L'ACL predefinita dell'oggetto garantisce FULL_CONTROL all'utente anonimo in quanto proprietario dell'oggetto. Perciò, Amazon S3 consente alle richieste non autenticate di recuperare l'oggetto o di modificarne l'ACL.

Per impedire all'utente anonimo di modificare oggetti, raccomandiamo di non implementare policy di bucket che consentono scritture pubbliche anonime sul bucket e di non utilizzare delle ACL che

concedono all'utente anonimo accesso di scrittura al bucket. Puoi applicare questo comportamento consigliato utilizzando il blocco dell'accesso pubblico di Amazon S3.

Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#). Per ulteriori informazioni sulle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

Important

Ti consigliamo di non utilizzare le credenziali dell'utente Account AWS root per effettuare richieste autenticate. Crea invece un ruolo IAM, concedendo a esso l'accesso completo. Gli utenti con questo ruolo vengono definiti utenti amministratori. È possibile utilizzare le credenziali assegnate al ruolo di amministratore, anziché le credenziali di utente Account AWS root, per interagire AWS ed eseguire attività, ad esempio creare un bucket, creare utenti e concedere autorizzazioni. Per ulteriori informazioni, consulta [AWS Credenziali di sicurezza](#) e [Pratiche ottimali di sicurezza in IAM](#) nella Guida all'utente IAM.

Policy dei bucket per Amazon S3

Una policy di bucket è una policy basata su risorse che puoi utilizzare per concedere autorizzazioni di accesso al bucket Amazon S3 e agli oggetti che contiene. Solo il proprietario del bucket può associare una policy a un bucket. Le autorizzazioni allegate a un bucket si applicano a tutti gli oggetti del bucket di proprietà del proprietario del bucket. Queste autorizzazioni non si applicano agli oggetti di proprietà di altri. Account AWS

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le ACL sono disabilite. Il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy.

Le policy Bucket utilizzano il linguaggio delle policy JSON-based AWS Identity and Access Management (IAM). Puoi utilizzare policy di bucket per aggiungere o negare autorizzazioni per gli oggetti in un bucket. I criteri di bucket autorizzano o rifiutano le richieste in base agli elementi inclusi nella policy. Questi elementi possono includere richiedente, operazioni S3, risorse e aspetti o condizioni della richiesta (ad esempio, l'indirizzo IP utilizzato per creare la richiesta).

Ad esempio, è possibile creare una policy di bucket che esegue le seguenti operazioni:

- Concedere ad altri account le autorizzazioni multi-account per il caricamento di oggetti nel bucket S3
- Verificare che il proprietario del bucket abbia il pieno controllo degli oggetti caricati

Per ulteriori informazioni, consulta [Esempi di policy del bucket Amazon S3](#).

Important

Non è possibile utilizzare una policy del bucket per impedire eliminazioni o transizioni in base a una regola del [ciclo di vita S3](#). Ad esempio, anche se la policy del bucket nega tutte le azioni per tutti i principali, la configurazione di S3 Lifecycle continua a funzionare normalmente.

Negli argomenti di questa sezione vengono forniti esempi e viene illustrato come aggiungere una policy di bucket nella console S3. Per informazioni sulle policy basate sull'identità, consulta [Identity-based politiche per Amazon S3](#). Per informazioni sul linguaggio delle policy di bucket, consulta [Policy e autorizzazioni in Amazon S3](#).

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Argomenti

- [Aggiunta di una policy di bucket utilizzando la console di Amazon S3](#)
- [Controllo dell'accesso dagli endpoint VPC con policy di bucket](#)
- [Esempi di policy del bucket Amazon S3](#)
- [Esempi di policy per i bucket che utilizzano le chiavi di condizione](#)

Aggiunta di una policy di bucket utilizzando la console di Amazon S3

Puoi utilizzare il [generatore di policy AWS](#) e la console di Amazon S3 per aggiungere una nuova policy di bucket o modificarne una esistente. Una bucket policy è una policy basata sulle risorse (IAM). AWS Identity and Access Management Si aggiunge una policy bucket a un bucket per concedere ad altri utenti Account AWS o agli utenti IAM le autorizzazioni di accesso per il bucket e gli oggetti in esso contenuti. Le autorizzazioni relative a un oggetto si applicano solo agli oggetti

creati dal proprietario del bucket. Per ulteriori informazioni sulle policy di bucket, consulta [Identity and Access Management per Amazon S3](#).

Assicurati di risolvere avvisi di sicurezza, errori, avvisi generali e suggerimenti da AWS Identity and Access Management Access Analyzer prima di salvare la policy. IAM Access Analyzer esegue controlli della policy per convalidarla in rapporto alla [sintassi della policy](#) e alle [best practice](#) di IAM. Questi controlli generano risultati e forniscono raccomandazioni attuabili per aiutarti a creare policy funzionali e conformi alle best practice di sicurezza. Per ulteriori informazioni sulla convalida delle policy tramite IAM Access Analyzer, consulta [Convalida delle policy di IAM Access Analyzer](#) nella Guida per l'utente di IAM. Per visualizzare un elenco delle avvertenze, degli errori e dei suggerimenti restituiti da IAM Access Analyzer, consulta il [Riferimento al controllo delle policy di IAM Access Analyzer](#).

Per istruzioni sulla risoluzione degli errori con una policy, consulta [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#).

Per creare o modificare una policy del bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.
3. Nell'elenco dei bucket scegli il nome del bucket per il quale desideri creare una policy di bucket o modificare la policy di bucket.
4. Scegli la scheda Autorizzazioni.
5. In Policy del bucket, scegli Modifica. Viene visualizzata la pagina Edit bucket policy (Modifica policy di bucket).
6. Nella pagina Edit bucket policy (Modifica policy di bucket), esegui una delle seguenti operazioni:
 - Per consulta esempi di policy dei bucket, scegli Esempi di policy. In alternativa, consulta [Esempi di policy del bucket Amazon S3](#) nella Guida all'utente di Amazon S3.
 - Per generare automaticamente una policy o modificare la sintassi JSON nella sezione Policy, scegli Policy generator (Generatore di policy).

Se scegli Policy Generator, il AWS Policy Generator si apre in una nuova finestra.

- a. Nella pagina del Generatore di policy AWS , per Seleziona il tipo di policy, scegli Policy del bucket S3.

- b. Aggiungi un'istruzione inserendo le informazioni nei campi previsti, quindi scegli Aggiungi istruzione. Ripeti questo passaggio per tutte le istruzioni che desideri aggiungere. Per ulteriori informazioni su questi campi, consulta [Riferimento agli elementi delle policy IAM JSON](#) nella Guida per l'utente IAM.

 Note

Per comodità, la pagina Modifica la policy bucket visualizza un ARN (nome della risorsa Amazon) del bucket corrente sopra il campo di testo Policy. È possibile copiare questo ARN per utilizzarlo nelle istruzioni della pagina del Generatore di policy AWS .

- c. Dopo aver aggiunto le istruzioni, scegli Genera policy.
 - d. Copia il testo della policy generata, scegli Chiudi e torna alla pagina Modifica policy del bucket nella console di Amazon S3.
7. Nella casella Policy, modifica la policy esistente o incolla la policy bucket dal AWS Policy Generator. Assicurati di risolvere gli avvisi di sicurezza, gli errori, gli avvisi generali e i suggerimenti prima di salvare la policy.

 Note

Le policy di bucket sono limitate a dimensioni di 20 KB.

8. (Facoltativo) Scegli Preview external access (Anteprima accesso esterno) nell'angolo in alto a destra per visualizzare in anteprima in che modo la nuova policy influisce sull'accesso pubblico e multi-account alla risorsa. Prima di salvare la policy, puoi verificare se introduce nuovi risultati di IAM Access Analyzer o risolve i risultati esistenti. Se non è presente uno strumento di analisi attivo, scegli Go to Access Analyzer (Passa a strumento analisi accessi) per [creare uno strumento di analisi degli account](#) in IAM Access Analyzer. Per ulteriori informazioni, consulta la sezione [Anteprima dell'accesso](#) nella Guida per l'utente di IAM.
9. Scegli Save changes (Salva modifiche), che ti riporterà alla pagina Permissions (Autorizzazioni).

Controllo dell'accesso dagli endpoint VPC con policy di bucket

È possibile utilizzare le policy dei bucket Amazon S3 per controllare l'accesso ai bucket da endpoint specifici del cloud privato virtuale (VPC) o da VPC specifici. Questa sezione contiene esempi di policy per i bucket che possono essere utilizzati per controllare l'accesso al bucket Amazon S3 dagli

endpoint VPC. Per informazioni su come configurare gli endpoint VPC, consulta [Endpoint VPC](#) nella Guida per l'utente di VPC.

Un VPC consente di lanciare AWS risorse in una rete virtuale definita dall'utente. Un endpoint VPC consente di creare una connessione privata tra la propria VPC e un'altra Servizio AWS. Questa connessione privata non richiede l'accesso via Internet, attraverso una connessione di rete privata virtuale (VPN), attraverso un'istanza NAT o attraverso Direct Connect.

Un endpoint VPC per Amazon S3 è un'entità logica all'interno di un cloud privato virtuale che permette di connettersi esclusivamente ad Amazon S3. L'endpoint VPC instrada le richieste ad Amazon S3 e restituisce le risposte al VPC. Gli endpoint VPC cambiano solo la modalità di instradamento delle richieste. I nomi DNS e gli endpoint pubblici Amazon S3 continueranno a funzionare con gli endpoint VPC. Per informazioni importanti sull'uso degli endpoint VPC con Amazon S3, consulta [Endpoint gateway](#) e [Endpoint gateway per Amazon S3](#) nella Guida all'utente VPC.

Gli endpoint VPC per Amazon S3 offrono due modi per controllare l'accesso ai dati di Amazon S3:

- È possibile controllare le richieste, gli utenti o i gruppi autorizzati tramite un endpoint VPC specifico. Per informazioni su questo tipo di controllo degli accessi, consulta [Controllo dell'accesso agli endpoint VPC mediante policy di endpoint](#) nella Guida all'utente VPC.
- È possibile controllare i VPC o gli endpoint VPC che hanno accesso ai bucket utilizzando le policy del bucket Amazon S3. Per alcuni esempi di questo tipo di controllo di accesso basato su policy di bucket, consulta i seguenti argomenti sulla limitazione dell'accesso.

Argomenti

- [Limitazione dell'accesso a un endpoint VPC specifico](#)
- [Limitazione dell'accesso a un VPC specifico](#)
- [Limitazione dell'accesso a un endpoint VPC IPv6](#)

Important

Quando si applicano le policy del bucket Amazon S3 per gli endpoint VPC descritte in questa sezione, si potrebbe bloccare involontariamente l'accesso al bucket. Le autorizzazioni del bucket che hanno lo scopo di limitare l'accesso del bucket a connessioni originate dall'endpoint VPC possono bloccare tutte le connessioni al bucket. Per informazioni su come

risolvere questo problema, consulta la sezione [Come correggere una policy del bucket con l'ID del VPC o dell'endpoint VPC errato](#) nell'Supporto AWS Knowledge Center.

Limitazione dell'accesso a un endpoint VPC specifico

Di seguito è riportato un esempio di policy del bucket Amazon S3 che limita l'accesso a un bucket specifico, `amzn-s3-demo-bucket`, solo dall'endpoint VPC con l'ID `vpce-0abcdef1234567890`. Se l'endpoint specificato non viene utilizzato, la policy nega l'accesso al bucket. La condizione `aws:SourceVpce` specifica l'endpoint. La condizione `aws:SourceVpce` non richiede un nome della risorsa Amazon (ARN) per la risorsa endpoint VPC, ma solo l'ID dell'endpoint VPC. Per ulteriori informazioni sull'utilizzo delle condizioni in una policy, consulta [Esempi di policy per i bucket che utilizzano le chiavi di condizione](#).

Important

- Prima di utilizzare la policy di esempio seguente, sostituire l'ID endpoint VPC con un valore appropriato per il caso d'uso. In caso contrario, non sarà possibile accedere al bucket.
- Questa policy disabilita l'accesso della console al bucket specificato perché le richieste della console non provengono dall'endpoint VPC specificato.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-0abcdef1234567890"
        }
      }
    }
  ]
}
```

```

    }
  }
]
}
```

Limitazione dell'accesso a un VPC specifico

Puoi creare una policy di bucket che limita l'accesso a uno specifico VPC utilizzando la condizione `aws:SourceVpc`. Ciò è utile se nello stesso VPC sono configurati più endpoint VPC e desideri gestire l'accesso ai bucket Amazon S3 per tutti gli endpoint. Di seguito è riportato un esempio di policy che nega l'accesso a `amzn-s3-demo-bucket` e ai relativi oggetti da qualsiasi punto esterno al VPC `vpc-1a2b3c4d`. Se il VPC specificato non è utilizzato, la policy nega l'accesso al bucket. Questa istruzione non garantisce l'accesso al bucket. Per concedere l'accesso, è necessario aggiungere un'istruzione separata `Allow`. La chiave di condizione `vpc-1a2b3c4d` non richiede un ARN per la risorsa VPC, ma solo l'ID VPC.

Important

- Prima di utilizzare la policy di esempio seguente, sostituire l'ID VPC con un valore appropriato per il caso d'uso. In caso contrario, non sarà possibile accedere al bucket.
- Questa policy disabilita l'accesso della console al bucket specificato perché le richieste della console non provengono dalla VPC specificata.

JSON

```

{
  "Version": "2012-10-17",
  "Id": "Policy1415115909153",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket",
                  "arn:aws:s3:::amzn-s3-demo-bucket/*"],
      "Condition": {
```

```

        "StringNotEquals": {
            "aws:SourceVpc": "vpc-1a2b3c4d"
        }
    }
}
]
}

```

Limitazione dell'accesso a un endpoint VPC IPv6

La seguente policy di esempio nega tutte le azioni di Amazon S3 (s3:) sul *amzn-s3-demo-bucket* bucket e sui relativi oggetti, a meno che la richiesta non provenga dall'endpoint VPC specificato (vpce-0a1b2c3d4e5f6g) e l'indirizzo IP di origine non corrisponda al blocco CIDR IPv6 fornito.

```

{
  "Version": "2012-10-17",
  "Id": "Policy1415115909154",
  "Statement": [
    {
      "Sid": "AccessSpecificIPv6VPCEOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket",
                   "arn:aws:s3:::amzn-s3-demo-bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpc": "vpce-0a1b2c3d4e5f6g"
        },
        "NotIpAddress": {
          "aws:VpcSourceIp": "2001:db8::/32"
        }
      }
    }
  ]
}

```

Per informazioni su come limitare l'accesso al tuo bucket in base a IP o VPC specifici, vedi [Come posso consentire solo a specifici endpoint o indirizzi IP VPC di accedere al mio bucket Amazon S3?](#) nel AWS re:Post Knowledge Center.

Esempi di policy del bucket Amazon S3

Con le policy di bucket Amazon S3, puoi proteggere l'accesso agli oggetti nei tuoi bucket, in modo che solo gli utenti con le autorizzazioni appropriate possano accedervi. Puoi persino impedire agli utenti autenticati senza le autorizzazioni appropriate di accedere alle tue risorse Amazon S3.

Questa sezione include esempi di casi d'uso tipici per le policy di bucket. Queste policy di esempio utilizzano *amzn-s3-demo-bucket* come valore di risorsa. Per testare queste policy, sostituisci *user input placeholders* con le tue informazioni (come il nome del bucket).

Per concedere o negare le autorizzazioni per un insieme di oggetti, puoi utilizzare caratteri jolly (*) nei nomi delle risorse Amazon (ARN) e altri valori. Ad esempio, è possibile controllare l'accesso a gruppi di oggetti che iniziano con un [prefisso](#) comune o terminano con un'estensione specifica, come .html.

Per ulteriori informazioni sul linguaggio delle policy AWS Identity and Access Management (IAM), consulta [Policy e autorizzazioni in Amazon S3](#).

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Note

Per testare le autorizzazioni utilizzando la console di Amazon S3, dovrai concedere le autorizzazioni aggiuntive richieste dalla console, ovvero `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Per una procedura dettagliata di esempio che concede autorizzazioni a utenti e le testa utilizzando la console, consulta [Procedura guidata: controllo dell'accesso a un bucket con policy utente](#).

Ulteriori risorse per la creazione di policy sui bucket sono le seguenti:

- Per un elenco delle azioni, delle risorse e delle chiavi di condizione delle policy IAM che è possibile utilizzare quando si crea una policy di bucket, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.
- Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).
- Per istruzioni sulla creazione della policy S3, consulta [Aggiunta di una policy di bucket utilizzando la console di Amazon S3](#).

- Per risolvere gli errori relativi a una policy, consulta [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#).

Se hai problemi ad aggiungere o aggiornare una policy, vedi [Perché ricevo l'errore «Principal in policy non valido» quando provo ad aggiornare la mia policy del bucket Amazon S3?](#) nel Knowledge Center. AWS re:Post

Argomenti

- [Concessione dell'autorizzazione di sola lettura a un utente pubblico anonimo](#)
- [Richiesta della crittografia](#)
- [Gestione dei bucket tramite ACL predefinite](#)
- [Gestione dell'accesso agli oggetti con assegnazione di tag agli oggetti](#)
- [Gestione dell'accesso agli oggetti utilizzando chiavi di condizione globali](#)
- [Gestione dell'accesso in base a richieste HTTP o HTTPS](#)
- [Gestione dell'accesso utente a cartelle specifiche](#)
- [Gestione dell'accesso per i log degli accessi](#)
- [Gestire l'accesso a un Amazon OAI CloudFront](#)
- [Gestione dell'accesso per Amazon S3 Storage Lens](#)
- [Gestione delle autorizzazioni per i report di S3 Inventory, S3 Analytics e S3 Inventory](#)
- [Richiesta dell'autenticazione a più fattori \(MFA\)](#)
- [Impedire agli utenti di eliminare gli oggetti](#)

Concessione dell'autorizzazione di sola lettura a un utente pubblico anonimo

È possibile utilizzare le impostazioni delle policy per concedere l'accesso a utenti pubblici anonimi, il che è utile se si sta configurando il bucket come un sito web statico. Per consentire l'accesso agli utenti pubblici anonimi è necessario disattivare le impostazioni di Blocco dell'accesso pubblico per il bucket. Per ulteriori informazioni su come fare e sulle policy necessarie, consulta [Impostazione delle autorizzazioni per l'accesso al sito Web](#). Per informazioni su come impostare policy più restrittive per lo stesso scopo, vedi [Come posso concedere l'accesso pubblico in lettura ad alcuni oggetti nel mio bucket Amazon S3?](#) nel Knowledge Center. AWS

Per impostazione predefinita, Amazon S3 blocca l'accesso pubblico all'account e ai bucket. Per utilizzare un bucket per ospitare un sito Web statico, puoi seguire questa procedura per modificare le impostazioni di blocco dell'accesso pubblico:

 Warning

Prima di completare questi passaggi, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#) per assicurarsi di aver compreso e accettato i rischi connessi alla concessione dell'accesso pubblico. Quando si disattivano le impostazioni di blocco dell'accesso pubblico per rendere pubblico il bucket, chiunque su Internet può accedere al bucket. Consigliamo di bloccare tutti gli accessi pubblici ai bucket.

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Seleziona il nome del bucket configurato come sito Web statico.
3. Seleziona Autorizzazioni.
4. In Blocca accesso pubblico (impostazioni bucket), seleziona Modifica.
5. Deseleziona Blocca tutto l'accesso pubblico, quindi seleziona Salva modifiche.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 



Account settings for Block Public Access are currently turned on

Account settings for Block Public Access that are enabled apply even if they are disabled for this bucket.

- ☐ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
 - ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
 - ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
 - ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
 - ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Amazon S3 disattiva le impostazioni di blocco dell'accesso pubblico per il bucket. Per creare un sito web pubblico statico, potrebbe essere necessario [modificare anche le impostazioni di blocco dell'accesso pubblico](#) per l'account prima di aggiungere una policy del bucket. Se le impostazioni di Blocco dell'accesso pubblico per l'account sono attualmente attivate, viene visualizzata una nota sotto Blocco dell'accesso pubblico (impostazioni del bucket).

Richiesta della crittografia

Puoi richiedere la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS), come mostrato negli esempi seguenti.

Richiede tutti SSE-KMS gli oggetti scritti in un bucket

La seguente politica di esempio richiede che ogni oggetto scritto nel bucket venga crittografato con la crittografia lato server utilizzando le chiavi AWS Key Management Service (AWS KMS) (). SSE-KMS. Se l'oggetto non è crittografato con SSE-KMS, la richiesta viene rifiutata.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [{
    "Sid": "DenyObjectsThatAreNotSSEKMS",
    "Principal": "*",
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
      }
    }
  }]
}
```

Richiedi SSE-KMS con uno specifico AWS KMS key per tutti gli oggetti scritti in un bucket

La seguente politica di esempio impedisce la scrittura di qualsiasi oggetto nel bucket se non è crittografato SSE-KMS utilizzando un ID chiave KMS specifico. Anche se gli oggetti vengono crittografati SSE-KMS utilizzando un'intestazione per richiesta o la crittografia predefinita del bucket, gli oggetti non possono essere scritti nel bucket se non sono stati crittografati con la chiave KMS specificata. Assicurati di sostituire il nome della risorsa Amazon (ARN) della chiave KMS utilizzata in questo esempio con il nome della risorsa Amazon (ARN) della tua chiave KMS ARN.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
```

```
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMSWithSpecificKey",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "ArnNotEqualsIfExists": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:us-east-1:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"
    }
  }
}]
}
```

Gestione dei bucket tramite ACL predefinite

Concessione delle autorizzazioni a più account per caricare oggetti o impostare le ACL degli oggetti per l'accesso pubblico

Il seguente esempio di policy concede i permessi `s3:PutObject` e `s3:PutObjectAcl` a più Account AWS. Inoltre, la policy di esempio richiede che tutte le richieste per queste operazioni includano la [lista di controllo degli accessi \(ACL\) predefinita](#) `public-read`. Per ulteriori informazioni, consulta [Azioni di policy per Amazon S3](#) e [Chiavi di condizione per Amazon S3](#).

Warning

L'ACL `public-read` predefinita consente a chiunque nel mondo di visualizzare gli oggetti nel tuo bucket, indipendentemente dalla sua dislocazione geografica. Procedi con cautela quando concedi l'accesso anonimo al bucket Amazon S3 o disabiliti le impostazioni di blocco dell'accesso pubblico. Quando si concede l'accesso anonimo, si consente a qualsiasi persona al mondo di accedere al bucket. È consigliabile non concedere mai l'accesso anonimo al bucket Amazon S3 a meno che non sia assolutamente necessario, ad esempio con l'[hosting di un sito Web statico](#). Se desideri abilitare le impostazioni di Blocco dell'accesso pubblico Amazon S3 per l'hosting di siti Web statici, consulta [Tutorial: Configurazione di un sito Web statico su Amazon S3](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddPublicReadCannedAcl",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": [
            "public-read"
          ]
        }
      }
    }
  ]
}
```

Concedere autorizzazioni multi-account per il caricamento di oggetti a garanzia del controllo completo da parte del proprietario del bucket

L'esempio seguente mostra come consentire a un altro di Account AWS caricare oggetti nel bucket assicurandoti al contempo di avere il pieno controllo degli oggetti caricati. Questa policy concede a specific Account AWS (**111122223333**) la possibilità di caricare oggetti solo se tale account include l'ACL predefinito al bucket-owner-full-control momento del caricamento. La condizione `StringEquals` nella policy specifica la chiave di condizione `s3:x-amz-acl` per esprimere il requisito dell'ACL predefinita. Per ulteriori informazioni, consulta [Chiavi di condizione per Amazon S3](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyForAllowUploadWithACL",
      "Effect": "Allow",
      "Principal": { "AWS": "111122223333" },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": { "s3:x-amz-acl": "bucket-owner-full-control" }
      }
    }
  ]
}
```

Gestione dell'accesso agli oggetti con assegnazione di tag agli oggetti

Concedere a un utente autorizzazioni di sola lettura per gli oggetti che hanno una chiave o un valore di tag specifico

La seguente policy di autorizzazione limita un utente a leggere solo gli oggetti con chiave e valore di tag `environment: production`. La policy utilizza la chiave di condizione `s3:ExistingObjectTag` per specificare la chiave e il valore di tag.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/JohnDoe"
      },
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ]
    }
  ]
}
```



```

    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "StringEquals": {
            "s3:ExistingObjectTag/environment": "production"
        }
    }
}
]
}

```

Limitare le chiavi di tag degli oggetti che gli utenti possono aggiungere

La seguente policy di esempio concede a un utente le autorizzazioni per eseguire l'operazione `s3:PutObjectTagging`, che permette di aggiungere tag a un oggetto esistente. La condizione utilizza la chiave di condizione `s3:RequestObjectTagKeys` per specificare le chiavi di tag consentite, ad esempio `Owner` o `CreationDate`. Per ulteriori informazioni, consulta la sezione [Creazione di una condizione con più chiavi o valori](#) nella Guida per l'utente IAM.

La policy garantisce che ogni chiave di tag specificata nella richiesta sia una chiave di tag autorizzata. Il qualificatore `ForAnyValue` nella condizione garantisce che almeno una delle chiavi specificate sia presente nella richiesta.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:role/JohnDoe"
        ]
      },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "s3:RequestObjectTagKeys": [
            "Owner",

```

```

        "CreationDate"
      ]
    }
  }
]
}

```

Richiedere una chiave e un valore di tag specifici per consentire agli utenti di aggiungere tag di oggetti

Il seguente esempio di policy concede a un utente l'autorizzazione a eseguire l'azione `s3:PutObjectTagging`, che consente di aggiungere tag a un oggetto esistente. La condizione prevede che l'utente includa una chiave di tag specifica (ad esempio, *Project*) con valore impostato su *X*.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": { "AWS": [
        "arn:aws:iam::111122223333:user/JohnDoe"
      ] },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": { "StringEquals": { "s3:RequestObjectTag/Project": "X" } }
    }
  ]
}

```

Concedere a un utente di aggiungere solo oggetti che hanno una chiave o un valore di tag specifico

La seguente policy di esempio concede a un utente l'autorizzazione per eseguire l'operazione `s3:PutObject` in modo che possa aggiungere oggetti a un bucket. Tuttavia, l'istruzione `Condition` limita le chiavi e i valori di tag consentiti sugli oggetti caricati. In questo esempio, l'utente può aggiungere al bucket solo oggetti con la chiave di tag specifica (*Department*) con il valore impostato su *Finance*

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:user/JohnDoe"
      ]
    },
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "Condition": {
      "StringEquals": {
        "s3:RequestObjectTag/Department": "Finance"
      }
    }
  ]
}
```

Gestione dell'accesso agli oggetti utilizzando chiavi di condizione globali

[Le chiavi di condizione globali](#) sono chiavi di contesto delle condizioni con un prefisso. aws Servizi AWS può supportare chiavi di condizione globali o chiavi specifiche del servizio che includono il prefisso del servizio. È possibile utilizzare l'elemento `Condition` di una policy JSON per confrontare le chiavi in una richiesta con i valori di chiave specificati nella policy.

Limitare l'accesso alle sole consegne dei log degli accessi al server Amazon S3

Nella seguente policy di bucket di esempio, la chiave di condizione globale [aws:SourceArn](#) viene utilizzata per confrontare il [nome della risorsa Amazon \(ARN\)](#) della risorsa, che effettua una richiesta da servizio a servizio con l'ARN specificato nella policy. La chiave di condizione globale `aws:SourceArn` viene utilizzata per impedire a un servizio Amazon S3 di essere utilizzato come [confused deputy](#) durante le transazioni tra servizi. Solo il servizio Amazon S3 può aggiungere oggetti al bucket Amazon S3.

Questo esempio di policy di bucket concede autorizzazioni `s3:PutObject` al principale del servizio di log (`logging.s3.amazonaws.com`).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutObjectS3ServerAccessLogsPolicy",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
      },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket1"
        }
      }
    },
    {
      "Sid": "RestrictToS3ServerAccessLogs",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
      "Condition": {
        "ForAllValues:StringNotEquals": {
```

```

    "aws:PrincipalServiceNamesList": "logging.s3.amazonaws.com"
  }
}
]
}

```

Consentire l'accesso solo alla tua organizzazione

Se desideri limitare IAM-based l'accesso a una risorsa Account AWS in modo che solo i responsabili della tua organizzazione (incluso l'account di AWS Organizations gestione) possano accedervi, puoi utilizzare la `aws:PrincipalOrgID` chiave di condizione globale.

Ecco un esempio di policy di bucket basata su risorse che puoi utilizzare per concedere l'accesso diretto al bucket a specifici principali IAM nella tua organizzazione. Aggiungendo la chiave di condizione `aws:PrincipalOrgID` globale alla tua policy bucket, ora è necessario che l'account principale sia all'interno dell'organizzazione per ottenere l'accesso tramite questa dichiarazione politica. Anche se si specifica accidentalmente un account errato al momento della concessione dell'accesso, la chiave di condizione `aws:PrincipalOrgID` globale funge da protezione aggiuntiva. Quando questa chiave globale viene utilizzata in un'istruzione Allow, garantisce che solo i titolari degli account dell'organizzazione elencata possano ottenere l'accesso tramite tale dichiarazione.

Important

Questa istruzione Allow con una condizione non nega l'accesso concesso tramite altri meccanismi. Se il bucket ha gli ACL abilitati o altre politiche che concedono l'accesso, i committenti esterni all'organizzazione potrebbero comunque essere in grado di accedere agli oggetti. Per limitare completamente l'accesso solo alla tua organizzazione, ti consigliamo di utilizzare questa condizione in un'istruzione Deny (vedi esempio sotto), disabilitare gli ACL impostando Object Ownership su «Bucket owner enforced» e abilitare S3 Block Public Access.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{

```

```

    "Sid": "AllowGetObject",
    "Principal": {
        "AWS": "*"
    },
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": ["o-aa111bb222"]
        }
    }
}

```

Nega l'accesso ai responsabili esterni alla tua organizzazione

Per una protezione più efficace, utilizza una dichiarazione di rifiuto con la condizione.

`aws:PrincipalOrgID` Un'istruzione `Deny` ha la precedenza su qualsiasi `Allow`, indipendentemente da come viene concesso l'accesso. L'esempio seguente nega tutte le azioni di S3 a qualsiasi responsabile che non è all'interno dell'organizzazione. Questo approccio fornisce una difesa approfondita anche nel caso in cui gli ACL o altre politiche avessero inavvertitamente concesso l'accesso.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessFromOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
            "aws:PrincipalOrgID": "o-aa111bb222"
          }
        }
      }
    ]
  }
}

```

```
]
}
```

Gestione dell'accesso in base a richieste HTTP o HTTPS

Limitare l'accesso solo alle richieste HTTPS

Se desideri impedire a potenziali aggressori di manipolare il traffico di rete, puoi utilizzare HTTPS (TLS) per consentire solo le connessioni crittografate limitando al contempo l'accesso al tuo bucket da parte delle richieste HTTP. Per determinare se la richiesta è HTTP o HTTPS, utilizza la chiave di condizione globale [aws:SecureTransport](#) nella policy di bucket S3. La chiave di condizione `aws:SecureTransport` controlla se una richiesta è stata inviata utilizzando HTTP.

Se una richiesta restituisce `true`, la richiesta è stata inviata tramite HTTP. Se la richiesta restituisce `false`, la richiesta è stata inviata tramite HTTPS. Puoi quindi consentire o negare l'accesso al bucket in base allo schema di richiesta desiderato.

Nell'esempio seguente, la policy di bucket nega esplicitamente l'accesso alle richieste HTTP.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "RestrictToTLSRequestsOnly",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    },
    "Principal": "*"
  }]
}
```

Limitare l'accesso a un referer HTTP specifico

Supponi di avere un sito Web con il nome di dominio (*www.example.com* o *example.com*) con collegamenti a foto e video archiviati nel bucket denominato *amzn-s3-demo-bucket*. Per impostazione predefinita, tutte le risorse Amazon S3 sono private, quindi solo chi le ha create può Account AWS accedervi.

Per consentire l'accesso in lettura a questi oggetti dal sito Web, è possibile aggiungere una policy di bucket che concede l'autorizzazione `s3:GetObject` con una condizione secondo cui la richiesta GET deve generare da pagine Web specifiche. La seguente policy limita le richieste utilizzando la condizione `StringLike` con la chiave di condizione `aws:Referer`.

Verifica che i browser utilizzati includano l'intestazione HTTP `referer` nella richiesta.

Warning

Ti consigliamo di procedere cautela quando utilizzi la chiave di condizione `aws:Referer`. È pericoloso includere un valore di intestazione di un referer pubblicamente noto. Parti non autorizzate possono utilizzare browser modificati o personalizzati per fornire qualsiasi valore `aws:Referer` scelto. Pertanto, non `aws:Referer` utilizzarlo per impedire a parti non autorizzate di effettuare richieste dirette AWS.

La chiave di condizione `aws:Referer` è disponibile solo per consentire ai clienti di proteggere i propri contenuti digitali, come i contenuti archiviati in Amazon S3, da riferimenti su siti di terze parti non autorizzate. Per ulteriori informazioni, consulta la sezione [aws:Referer](#) nella Guida per l'utente di IAM.

Gestione dell'accesso utente a cartelle specifiche

Concedere agli utenti l'accesso a cartelle specifiche

Supponiamo che tu stia cercando di concedere agli utenti l'accesso a una cartella specifica. Se l'utente IAM e il bucket S3 appartengono allo stesso Account AWS, puoi utilizzare una policy IAM per concedere all'utente l'accesso a una cartella bucket specifica. Con questo approccio, non è necessario aggiornare la policy di bucket per concedere l'accesso. Puoi aggiungere la policy IAM a un ruolo IAM a cui possono passare più utenti.

Se l'identità IAM e il bucket S3 sono diversi Account AWS, è necessario concedere l'accesso tra account sia nella policy IAM che nella policy del bucket. Per informazioni su come concedere

l'accesso multi-account, consulta la sezione relativa al [proprietario del bucket che concede autorizzazioni per il bucket multi-account](#).

La seguente policy di bucket di esempio concede a *JohnDoe* l'accesso completo a livello di console solo alla sua cartella (home/*JohnDoe*/). Creando una cartella home e concedendo le autorizzazioni appropriate ai tuoi utenti, puoi fare in modo che più utenti condividano un singolo bucket. Questa policy è composta da tre istruzioni Allow:

- *AllowRootAndHomeListingOfCompanyBucket*: consente all'utente (*JohnDoe*) di elencare gli oggetti al livello root del bucket *amzn-s3-demo-bucket* e nella cartella home. Questa istruzione consente inoltre all'utente di cercare in base al prefisso home/ utilizzando la console.
- *AllowListingOfUserFolder*: consente all'utente (*JohnDoe*) di elencare tutti gli oggetti nella cartella home/*JohnDoe*/ e nelle eventuali sottocartelle.
- *AllowAllS3ActionsInUserFolder*: consente all'utente di eseguire tutte le operazioni di Amazon S3 concedendo le autorizzazioni Read, Write e Delete. Le autorizzazioni sono limitate alla cartella principale del proprietario del bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRootAndHomeListingOfCompanyBucket",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:user/JohnDoe"
        ]
      },
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
      "Condition": {
        "StringEquals": {
          "s3:prefix": ["", "home/", "home/JohnDoe"],
          "s3:delimiter": ["/"]
        }
      }
    }
  ],
}
```

```

{
  "Sid": "AllowListingOfUserFolder",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:user/JohnDoe"
    ]
  },
  "Action": ["s3:ListBucket"],
  "Effect": "Allow",
  "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
  "Condition": {
    "StringLike": {
      "s3:prefix": ["home/JohnDoe/*"]
    }
  }
},
{
  "Sid": "AllowAllS3ActionsInUserFolder",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:user/JohnDoe"
    ]
  },
  "Action": ["s3:*"],
  "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/home/JohnDoe/*"]
}
]
}

```

Gestione dell'accesso per i log degli accessi

Concedere l'accesso ad Application Load Balancer per abilitare i log degli accessi

Quando abiliti i log degli accessi per Application Load Balancer, devi specificare il nome del bucket S3 in cui il sistema di bilanciamento del carico [archivierà i log](#). Il bucket deve avere una [policy collegata](#) che concede a Elastic Load Balancing l'autorizzazione a scrivere nel bucket.

Nell'esempio seguente, la policy di bucket concede a Elastic Load Balancing (ELB) l'autorizzazione a scrivere i log degli accessi nel bucket:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/*"
    }
  ]
}
```

 Note

Assicurati di sostituire *elb-account-id* con l'ID Account AWS per Elastic Load Balancing per la tua Regione AWS. Per l'elenco delle regioni Elastic Load Balancing, consulta [Collegamento di una policy al bucket Amazon S3](#) nella Guida per l'utente di Elastic Load Balancing.

Se la tua Regione AWS non compare nell'elenco delle regioni Elastic Load Balancing supportate, utilizza la seguente policy, che concede le autorizzazioni al servizio di consegna dei log specificato.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Effect": "Allow",
      "Action": "s3:PutObject",
    }
  ]
}
```

```

    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/
    *\"
  }
]
}

```

Quindi, assicurati di configurare i [log degli accessi di Elastic Load Balancing](#) abilitandoli. Puoi [verificare le autorizzazioni del bucket](#) creando un file di test.

Gestire l'accesso a un Amazon OAI CloudFront

Concedi l'autorizzazione a un Amazon CloudFront OAI

Il seguente esempio di bucket policy concede a un'identità di accesso all' CloudFront origine (OAI) l'autorizzazione per ottenere (leggere) tutti gli oggetti nel bucket S3. Puoi utilizzare un CloudFront OAI per consentire agli utenti di accedere agli oggetti nel tuo bucket tramite CloudFront Amazon S3 ma non direttamente. Per ulteriori informazioni, consulta [Restricting access to Amazon S3 by using a Origin Access Identity](#) nella Amazon Developer Guide. CloudFront

La policy seguente utilizza l'ID dell'identità di accesso origine (OAI) come Principal della policy. Per ulteriori informazioni sull'utilizzo delle policy dei bucket S3 per concedere l'accesso a un CloudFront OAI, consulta [Migrating from origin access identity \(OAI\) to origin access control \(OAC\) nella Amazon Developer Guide.](#) CloudFront

Per utilizzare questo esempio:

- Sostituisci **EH1HDMB1FH2TC** con l'ID dell'identità di accesso origine (OAI). Per trovare l'ID dell'OAI, consulta la pagina [Origin Access Identity](#) sulla CloudFront console o utilizzalo nell'API. [ListCloudFrontOriginAccessIdentities](#) CloudFront
- Sostituisci **amzn-s3-demo-bucket** con il nome del tuo bucket.

JSON

```

{
  "Version": "2012-10-17",
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {

```

```

        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
Identity EH1HDMB1FH2TC"
        },
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
]
}

```

Gestione dell'accesso per Amazon S3 Storage Lens

Concedere le autorizzazioni per Amazon S3 Storage Lens

S3 Storage Lens aggrega i tuoi parametri e mostra le informazioni nella sezione Account snapshot (Snapshot dell'account) nella pagina Buckets (Bucket) della console di Amazon S3. S3 Storage Lens fornisce anche una dashboard interattiva che puoi utilizzare per visualizzare informazioni e tendenze, segnalare valori anomali e ricevere consigli per ottimizzare i costi di storage e applicare le migliori pratiche di protezione dei dati. La dashboard offre opzioni di approfondimento per generare e visualizzare informazioni dettagliate a livello di organizzazione, account, classe di archiviazione, bucket Regione AWS, prefisso o gruppo Storage Lens. Puoi anche inviare un rapporto giornaliero sulle metriche in Parquet formato CSV o a un bucket S3 generico o esportare le metriche direttamente in un bucket di tabelle S3 gestito. AWS

S3 Storage Lens può esportare i parametri aggregati relativi l'utilizzo dell'archiviazione in un bucket Amazon S3 per ulteriori analisi. Il bucket in cui S3 Storage Lens colloca le esportazioni delle metriche è noto come bucket di destinazione. Quando configuri l'esportazione delle metriche di S3 Storage Lens, devi disporre di una policy di bucket per il bucket di destinazione. Per ulteriori informazioni, consulta [Monitoraggio dell'attività e dell'utilizzo dello storage con Amazon S3 Storage Lens](#).

La seguente policy di bucket di esempio concede ad Amazon S3 l'autorizzazione a scrivere oggetti (richieste PUT) in un bucket di destinazione. Questo tipo di policy di bucket viene utilizzato nel bucket di destinazione quando si imposta l'esportazione dei parametri di S3 Storage Lens.

JSON

```

{
    "Version": "2012-10-17",

```

```

    "Statement": [
      {
        "Sid": "S3StorageLensExamplePolicy",
        "Effect": "Allow",
        "Principal": {
          "Service": "storage-lens.s3.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/StorageLens/111122223333/*"
        ],
        "Condition": {
          "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn": "arn:aws:s3:region-code:111122223333:storage-lens/storage-lens-dashboard-configuration-id"
          }
        }
      }
    ]
  }
}

```

Utilizza la modifica seguente alla precedente istruzione Resource della policy di bucket quando configuri un'esportazione di parametri a livello di organizzazione S3 Storage Lens.

```

"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/StorageLens/your-organization-id/*",

```

Gestione delle autorizzazioni per i report di S3 Inventory, S3 Analytics e S3 Inventory

Concedere autorizzazioni per S3 Inventory e S3 Analytics

S3 Inventory crea elenchi di oggetti in un bucket, mentre l'esportazione di analisi della classe di archiviazione di S3 Analytics genera file di output dei dati utilizzati nell'analisi. Il bucket per il quale l'inventario elenca gli oggetti è denominato bucket di origine. Il bucket nel quale viene scritto il file di inventario e il file di esportazione di analisi è definito bucket di destinazione. È necessario creare una policy di bucket per il bucket di destinazione quando si configura un inventario o un'esportazione di

analisi. Per ulteriori informazioni, consulta [Catalogazione e analisi dei dati con Inventario S3](#) e [Analisi di Amazon S3 – Analisi della classe di storage](#).

La policy di bucket di esempio seguente concede ad Amazon S3 l'autorizzazione per scrivere oggetti (richieste PUT) dall'account per il bucket di origine nel bucket di destinazione. Questo tipo di policy di bucket viene utilizzato nel bucket di destinazione quando imposti S3 Inventory e l'esportazione di S3 Analytics.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InventoryAndAnalyticsExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ],
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
        },
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Controllo della creazione della configurazione dei report di Inventario S3

[Catalogazione e analisi dei dati con Inventario S3](#) crea elenchi degli oggetti presenti in un bucket S3 e i metadata per ogni oggetto. L'autorizzazione `s3:PutInventoryConfiguration` consente all'utente di creare una configurazione dell'inventario che include tutti i campi dei metadata dell'oggetto

disponibili per impostazione predefinita e di specificare il bucket di destinazione per memorizzare l'inventario. Un utente con accesso in lettura agli oggetti nel bucket di destinazione può accedere a tutti i campi di metadati degli oggetti disponibili nel report di inventario. Per ulteriori informazioni sui campi dei metadati disponibili in S3 Inventory, consulta [Elenco di Amazon S3 Inventory](#).

Per impedire a un utente di configurare un report di Inventario S3, rimuovi l'autorizzazione `s3:PutInventoryConfiguration` dall'utente.

Alcuni campi dei metadati degli oggetti nelle configurazioni dei report dell'Inventario S3 sono opzionali, cioè sono disponibili per impostazione predefinita, ma possono essere limitati quando si concede a un utente l'autorizzazione `s3:PutInventoryConfiguration`. È possibile controllare se gli utenti possono includere questi campi di metadati opzionali nei loro report utilizzando la chiave di condizione `s3:InventoryAccessibleOptionalFields`. Per un elenco dei campi di metadati opzionali disponibili in Inventario S3, consulta [OptionalFields](#) in Riferimento API di Amazon Simple Storage Service.

Note

Per i bucket di directory, usa la chiave di condizione invece di `s3express:InventoryAccessibleOptionalFields` `s3:InventoryAccessibleOptionalFields` Per ulteriori informazioni sulla configurazione di S3 Inventory per i bucket di directory, vedere. [Configurazione di Amazon S3 Inventory](#)

Per concedere a un utente l'autorizzazione a creare una configurazione dell'inventario con specifici campi di metadati opzionali, utilizzare la chiave di condizione `s3:InventoryAccessibleOptionalFields` per affinare le condizioni della policy del bucket.

Il seguente esempio di policy concede a un utente (*Ana*) l'autorizzazione a creare una configurazione di inventario in modo condizionato. La condizione `ForAllValues:StringEquals` nella policy utilizza la chiave di condizione `s3:InventoryAccessibleOptionalFields` per specificare i due campi di metadati opzionali consentiti, ovvero `Size` e `StorageClass`. Quindi, quando *Ana* crea una configurazione di inventario, gli unici campi di metadati opzionali che può includere sono `Size` e `StorageClass`.

JSON

```
{
  "Id": "InventoryConfigPolicy",
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowInventoryCreationConditionally",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:user/Ana"
    },
    "Action":
      "s3:PutInventoryConfiguration",
    "Resource":
      "arn:aws:s3::DOC-EXAMPLE-SOURCE-BUCKET",
    "Condition": {
      "ForAllValues:StringEquals": {
        "s3:InventoryAccessibleOptionalFields": [
          "Size",
          "StorageClass"
        ]
      }
    }
  ]
}
```

Per impedire a un utente di configurare un report dell'Inventario S3 che includa specifici campi di metadati opzionali, aggiungere un'istruzione esplicita Deny alla policy di bucket per il bucket di origine. Il seguente esempio di policy del bucket impedisce all'utente *Ana* di creare una configurazione dell'inventario nel bucket di origine *amzn-s3-demo-source-bucket* che includa i campi di metadati opzionali `ObjectAccessControlList` o `ObjectOwner`. L'utente *Ana* può comunque creare una configurazione dell'inventario con altri campi di metadati opzionali.

```
{
  "Id": "InventoryConfigSomeFields",
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowInventoryCreation",
    "Effect": "Allow",
```

```
"Principal": {
  "AWS": "arn:aws:iam::111122223333:user/Ana"
},
"Action": "s3:PutInventoryConfiguration",
"Resource":
  "arn:aws:s3::amzn-s3-demo-source-bucket",

},
{
  "Sid": "DenyCertainInventoryFieldCreation",
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
  },
  "Action": "s3:PutInventoryConfiguration",
  "Resource":
    "arn:aws:s3::amzn-s3-demo-source-bucket",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "s3:InventoryAccessibleOptionalFields": [
        "ObjectOwner",
        "ObjectAccessControlList"
      ]
    }
  }
}
]
```

Note

L'uso della chiave di condizione `s3:InventoryAccessibleOptionalFields` nelle policy dei bucket non influisce sulla consegna dei report di inventario basati sulle configurazioni di inventario esistenti.

Important

Si consiglia di utilizzare `ForAllValues` con un effetto `Allow` o `ForAnyValue` con un effetto `Deny`, come mostrato negli esempi precedenti.

Non usare `ForAllValues` con un effetto `Deny` né `ForAnyValue` con un effetto `Allow`, perché queste combinazioni possono essere troppo restrittive e bloccare la cancellazione della configurazione dell'inventario.

Per ulteriori informazioni sugli operatori di set di condizioni `ForAllValues` e `ForAnyValue`, consulta [Tasti contestuali multivalore](#) nella Guida all'utente IAM.

Controlla la creazione del report di configurazione di S3 Inventory per i bucket di directory

Per i bucket di directory, si utilizza la chiave di

`s3express:InventoryAccessibleOptionalFields` condizione in una policy basata sull'identità IAM anziché in una policy bucket. Il seguente esempio di policy IAM concede a un utente l'autorizzazione a creare una configurazione di inventario per un bucket di directory. La `ForAllValues:StringEquals` condizione utilizza la chiave di `s3express:InventoryAccessibleOptionalFields` condizione per specificare i campi di metadati opzionali consentiti.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowInventoryCreationForDirectoryBucket",
    "Effect": "Allow",
    "Action": "s3express:PutInventoryConfiguration",
    "Resource": "arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3",
    "Condition": {
      "ForAllValues:StringEquals": {
        "s3express:InventoryAccessibleOptionalFields": [
          "Size",
          "StorageClass"
        ]
      }
    }
  }]
}
```

Richiesta dell'autenticazione a più fattori (MFA)

Amazon S3 supporta l'accesso alle MFA-protected API, una funzionalità che può imporre l'autenticazione a più fattori (MFA) per l'accesso alle tue risorse Amazon S3. Multi-factor

l'autenticazione fornisce un ulteriore livello di sicurezza che puoi applicare al tuo ambiente.

AWS L'autenticazione a più fattori (MFA) è una funzione di protezione che prevede che gli utenti dimostrino di possedere fisicamente un dispositivo MFA fornendo un codice MFA valido. Per ulteriori informazioni, vedere [AWS Multi-Factor Autenticazione](#). Puoi richiedere l'autenticazione MFA per tutte le richieste di accesso alle risorse di Amazon S3.

Per imporre l'uso del requisito dell'autenticazione a più fattori (MFA), utilizza la chiave di condizione `aws:MultiFactorAuthAge` in una policy di bucket. Gli utenti IAM possono accedere alle risorse di Amazon S3 utilizzando le credenziali temporanee emesse da Servizio di token di sicurezza AWS (AWS STS). Al momento della richiesta AWS STS, dovrai fornire il codice MFA.

Quando Amazon S3 riceve una richiesta con l'autenticazione a più fattori (MFA), la chiave di condizione `aws:MultiFactorAuthAge` fornisce un valore numerico che indica il tempo trascorso (in secondi) dalla creazione delle credenziali temporanee. Se le credenziali temporanee fornite nella richiesta non sono state create utilizzando un dispositivo MFA, il valore di questa chiave è null (assente). In una policy di bucket, è possibile aggiungere una condizione per controllare questo valore, come mostrato nell'esempio riportato di seguito.

La policy di esempio nega qualsiasi operazione Amazon S3 nella cartella */taxdocuments* del bucket *amzn-s3-demo-bucket* se la richiesta non è autenticata tramite l'autenticazione a più fattori (MFA). Per ulteriori informazioni sull'MFA, consulta [Using Multi-Factor Authentication \(MFA\) AWS](#) nella IAM User Guide.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket//taxdocuments/*",
      "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }
    }
  ]
}
```

La condizione `Null` nel blocco `Condition` viene valutata come `true` se il valore della chiave di condizione `aws:MultiFactorAuthAge` è `null`, a indicare che le credenziali di sicurezza temporanee nella richiesta sono state create senza un dispositivo MFA.

La policy di bucket seguente è un'estensione di quella precedente. La seguente policy comprende due istruzioni dedicate. Una dichiarazione consente l'autorizzazione `s3:GetObject` per un bucket (*`amzn-s3-demo-bucket`*) per tutti gli utenti. La seconda dichiarazione limita ulteriormente l'accesso alla cartella *`amzn-s3-demo-bucket/taxdocuments`* nel bucket richiedendo l'autenticazione MFA.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "DenyInsecureConnections",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
      "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }
    },
    {
      "Sid": "AllowGetObject",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}
```

Facoltativamente, è possibile utilizzare una condizione numerica per limitare la durata della validità della chiave `aws:MultiFactorAuthAge`. La durata specificata con la chiave

`aws:MultiFactorAuthAge` è indipendente dalla durata delle credenziali di sicurezza temporanee utilizzate per l'autenticazione della richiesta.

Ad esempio, la policy di bucket seguente, oltre a richiedere l'autenticazione MFA, controlla anche da quanto tempo esiste la sessione temporanea. La policy rifiuta tutte le operazioni se il valore della chiave `aws:MultiFactorAuthAge` indica che la sessione temporanea è stata creata oltre un'ora (3.600 secondi) prima.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
      "Condition": {"Null": {"aws:MultiFactorAuthAge": true }}
    },
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
      "Condition": {"NumericGreaterThan": {"aws:MultiFactorAuthAge": 3600 }}
    },
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}
```

Impedire agli utenti di eliminare gli oggetti

Per default, gli utenti non dispongono di autorizzazioni. Ma quando si creano le policy, è possibile che si concedano agli utenti autorizzazioni che non si intendevano concedere. Per evitare questi espedienti riguardo alle autorizzazioni, è possibile scrivere una policy di accesso più rigida aggiungendo un rifiuto esplicito.

Per bloccare esplicitamente gli utenti o gli account dall'eliminazione di oggetti, è necessario aggiungere le seguenti azioni su una policy del bucket: `s3:DeleteObject`, `s3:DeleteObjectVersion` e `s3:PutLifecycleConfiguration`. Tutte e tre le azioni sono necessarie perché è possibile eliminare gli oggetti chiamando esplicitamente le operazioni dell'API `DELETE Object` o configurando il loro ciclo di vita (consulta [Gestione del ciclo di vita degli oggetti](#)) in modo che Amazon S3 possa rimuovere gli oggetti quando la loro durata scade.

Nel seguente esempio di policy, si negano esplicitamente le autorizzazioni di `DELETE Object` all'utente *MaryMajor*. Un'istruzione esplicita `Deny` sostituisce sempre qualsiasi altra autorizzazione concessa.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
      "Action": [
        "s3:GetObjectVersion",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    },
    {
      "Sid": "statement2",
      "Effect": "Deny",
```

```
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
    },
    "Action": [
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:PutLifecycleConfiguration"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket1",
      "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    ]
  }
}
```

Esempi di policy per i bucket che utilizzano le chiavi di condizione

È possibile utilizzare in linguaggio delle policy di accesso per specificare le condizioni quando si concedono le autorizzazioni. È possibile utilizzare l'elemento opzionale `Condition`, o blocco `Condition`, per specificare le condizioni per l'entrata in vigore di una policy.

Per le policy che utilizzano le chiavi di condizioni di Amazon S3 per operazioni su oggetti e bucket, consulta gli esempi seguenti. Per ulteriori informazioni su queste chiavi di condizione, consulta [Chiavi di condizione per Amazon S3](#). Per un elenco completo delle azioni, delle chiavi di condizione e delle risorse di Amazon S3 che è possibile specificare nelle policy, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Esempi: Chiavi di condizione di Amazon S3 per operazioni sugli oggetti

Gli esempi seguenti mostrano come si possono usare le chiavi di condizione specifiche di Amazon S3 per le operazioni sugli oggetti. Per un elenco completo delle azioni, delle chiavi di condizione e delle risorse di Amazon S3 che è possibile specificare nelle policy, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Molte delle policy di esempio mostrano come è possibile utilizzare le chiavi di condizione con le operazioni [PUT Object](#). Le operazioni sugli oggetti PUT consentono intestazioni specifiche degli elenchi di controllo degli accessi (ACL) che puoi utilizzare per concedere le autorizzazioni. ACL-based Utilizzando queste chiavi di condizione, è possibile impostare una condizione per richiedere autorizzazioni di accesso specifiche quando l'utente carica un oggetto. Puoi anche concedere autorizzazioni basate su ACL con l'operazione. PutObjectAcl Per ulteriori informazioni, consulta [PutObjectAcl](#) Amazon S3 Amazon Simple Storage Service API Reference. Per ulteriori informazioni sulle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

Argomenti

- [Esempio 1: concessione di s3: PutObject autorizzazione che richiede l'archiviazione degli oggetti utilizzando la crittografia lato server](#)
- [Esempio 2: concessione di s3: PutObject autorizzazione a copiare oggetti con una restrizione sull'origine della copia](#)
- [Esempio 3: concessione dell'accesso a una versione specifica di un oggetto](#)
- [Esempio 4: concessione di autorizzazioni in base ai tag degli oggetti](#)
- [Esempio 5: limitazione dell'accesso da parte di Account AWS ID del proprietario del bucket](#)
- [Esempio 6: Richiesta di una versione TLS minima](#)
- [Esempio 7: esclusione di determinati committenti da una dichiarazione di rifiuto](#)
- [Esempio 8: imporre ai client di caricare in modo condizionato gli oggetti in base ai nomi delle chiavi degli oggetti o agli ETag](#)
- [Esempio 9: limitazione dell'accesso alle annotazioni in base al prefisso del nome](#)
- [Esempio 10: Richiesta di scritture condizionali per le operazioni di annotazione](#)
- [Esempio 11: limitazione della dimensione dell'impaginazione per ListObjectAnnotations](#)

Esempio 1: concessione di **s3: PutObject** autorizzazione che richiede l'archiviazione degli oggetti utilizzando la crittografia lato server

Si supponga che l'Account A possieda un bucket. L'amministratore dell'account desidera concedere a Jane, un utente dell'Account A, il permesso di caricare oggetti a condizione che Jane richieda sempre la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 L'amministratore del conto A può specificare questo requisito utilizzando la chiave di condizione `s3:x-amz-server-side-encryption`, come mostrato. La coppia chiave-valore nel Condition blocco seguente specifica la `s3:x-amz-server-side-encryption` condizione key e () come tipo di crittografia: SSE-S3 AES256

```
"Condition": {
  "StringNotEquals": {
    "s3:x-amz-server-side-encryption": "AES256"
  }
}
```

Quando si verifica questa autorizzazione utilizzando il AWS CLI, è necessario aggiungere la crittografia richiesta utilizzando il `--server-side-encryption` parametro, come mostrato nell'esempio seguente. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg --body c:\HappyFace.jpg --server-side-encryption "AES256" --profile AccountAdmin
```

Esempio 2: concessione di **s3: PutObject** autorizzazione a copiare oggetti con una restrizione sull'origine della copia

In una richiesta di oggetto PUT, quando si specifica un oggetto di origine, la richiesta è un'operazione di copia (consulta [CopyObject](#)). Di conseguenza è possibile che il proprietario del bucket assegni all'utente l'autorizzazione a copiare gli oggetti con qualche limitazione sull'origine, ad esempio:

- Consente di copiare gli oggetti solo dal bucket di origine specificato (ad esempio, *amzn-s3-demo-source-bucket*).
- Consente di copiare gli oggetti dal bucket di origine specificato e solo gli oggetti il cui prefisso del nome della chiave inizia con un prefisso specifico, come ad esempio *public/* (ad esempio, *amzn-s3-demo-source-bucket/public/**).
- Consente di copiare solo un oggetto specifico dal bucket di origine (ad esempio, *amzn-s3-demo-source-bucket/example.jpg*).

La seguente policy del bucket concede a un utente (*Dave*) l'autorizzazione `s3:PutObject`. Questa policy gli consente di copiare gli oggetti solo a condizione che la richiesta includa l'intestazione `s3:x-amz-copy-source` e che il valore dell'intestazione specifichi il prefisso del nome della chiave */amzn-s3-demo-source-bucket/public/**. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "cross-account permission to user in your own account",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:user/Dave"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3::amzn-s3-demo-source-bucket/*"
  },
  {
    "Sid": "Deny your user permission to upload object if copy source is
not /bucket/prefix",
    "Effect": "Deny",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:user/Dave"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3::amzn-s3-demo-source-bucket/*",
    "Condition": {
      "StringNotLike": {
        "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/*"
      }
    }
  }
]
}

```

Verifica la politica con AWS CLI

È possibile verificare l'autorizzazione utilizzando il AWS CLI `copy-object` comando. È possibile specificare l'origine aggiungendo il parametro `--copy-source`; il prefisso del nome della chiave deve corrispondere al prefisso consentito nella policy. È necessario fornire le credenziali all'utente Dave utilizzando il parametro `--profile`. Per ulteriori informazioni sulla configurazione di AWS CLI, consulta [Developing with Amazon S3 using the AWS CLI](#) in Amazon S3 API Reference.

```

aws s3api copy-object --bucket amzn-s3-demo-source-bucket --key HappyFace.jpg
--copy-source amzn-s3-demo-source-bucket/public/PublicHappyFace1.jpg --
profile AccountADave

```

Concessione dell'autorizzazione a copiare solo un oggetto specifico

La policy di cui sopra utilizza la condizione `StringNotLike`. Per concedere l'autorizzazione a copiare solo un oggetto specifico, è necessario modificare la condizione da `StringNotLike` a `StringNotEquals` e quindi specificare la chiave dell'oggetto esatto, come mostrato nell'esempio seguente. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
"Condition": {
  "StringNotEquals": {
    "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/
PublicHappyFace1.jpg"
  }
}
```

Esempio 3: concessione dell'accesso a una versione specifica di un oggetto

Si supponga che l'account A possieda un bucket con controllo delle versioni abilitato. Il bucket ha diverse versioni dell'oggetto *HappyFace.jpg*. L'amministratore dell'account A vuole ora concedere all'utente *Dave* il permesso di ottenere solo una versione specifica dell'oggetto. L'amministratore dell'account può ottenere questo risultato concedendo all'utente *Dave* l'autorizzazione `s3:GetObjectVersion` in modo condizionato, come mostrato nell'esempio seguente. La coppia chiave-valore nel blocco `Condition` specifica la chiave di condizione `s3:VersionId`. In questo caso, per recuperare l'oggetto dal bucket con controllo delle versioni abilitato specificato, *Dave* deve conoscere l'ID esatto della versione dell'oggetto. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

Per ulteriori informazioni, consulta [GetObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
```

```

        "AWS": "arn:aws:iam::123456789012:user/Dave"
    },
    "Action": "s3:GetObjectVersion",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg"
},
{
    "Sid": "statement2",
    "Effect": "Deny",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Dave"
    },
    "Action": "s3:GetObjectVersion",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg",
    "Condition": {
        "StringNotEquals": {
            "s3:VersionId": "AaaHbAQitwiL_h47_44lR02DDfLlB05e"
        }
    }
}
]
}

```

Prova la policy con AWS CLI

È possibile verificare le autorizzazioni in questa policy utilizzando il AWS CLI `get-object` comando con il `--version-id` parametro per identificare la versione specifica dell'oggetto da recuperare. Il comando recupera la versione specificata dell'oggetto e la salva nel file *OutputFile.jpg*.

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg OutputFile.jpg --
version-id AaaHbAQitwiL_h47_44lR02DDfLlB05e --profile AccountADave
```

Esempio 4: concessione di autorizzazioni in base ai tag degli oggetti

Per esempi su come utilizzare le chiavi di condizione del tagging degli oggetti con le operazioni di Amazon S3, consulta [Tagging e policy di controllo degli accessi](#).

Esempio 5: limitazione dell'accesso da parte di Account AWS ID del proprietario del bucket

Puoi utilizzare la chiave di `s3:ResourceAccount` condizione `aws:ResourceAccount` or per scrivere policy per endpoint IAM o VPC (Virtual Private Cloud) che limitino l'accesso di utenti, ruoli o applicazioni ai bucket Amazon S3 di proprietà di un ID specifico. Account AWS È possibile utilizzare

queste chiavi di condizione per limitare l'accesso dei client all'interno del VPC ai bucket non di proprietà dell'utente.

Tuttavia, tieni presente che alcuni AWS servizi si basano sull'accesso a bucket gestiti. AWS Pertanto, l'utilizzo della chiave `aws:ResourceAccount` o `s3:ResourceAccount` nelle policy IAM potrebbe influire sull'accesso a queste risorse. Per maggiori informazioni, consulta le seguenti risorse:

- [Limitazione dell'accesso ai bucket in un Account AWS](#) specificato nella Guida di AWS PrivateLink
- [Limitazione dell'accesso ai bucket utilizzati da Amazon ECR](#) nella Guida di Amazon ECR
- [Fornisci l'accesso richiesto a Systems Manager per i bucket](#) Amazon S3 AWS gestiti nella Guida AWS Systems Manager

Per ulteriori informazioni sulle chiavi di condizione `aws:ResourceAccount` e `s3:ResourceAccount` ed esempi che mostrano come usarle, consulta [Limitare l'accesso ai bucket Amazon S3 di proprietà di specifici Account AWS](#) nello AWS Storage Blog.

Esempio 6: Richiesta di una versione TLS minima

È possibile utilizzare la chiave di condizione `s3:TlsVersion` per scrivere policy IAM, endpoint di cloud privato virtuale (VPCE) o bucket che limitano l'accesso di utenti o applicazioni ai bucket Amazon S3 in base alla versione TLS utilizzata dal client. È possibile utilizzare questa chiave di condizione per scrivere policy che richiedono una versione TLS minima.

Note

Quando AWS i servizi effettuano chiamate ad altri AWS servizi per tuo conto (chiamate da servizio a servizio), alcuni contesti di autorizzazione specifici della rete vengono oscurati, tra cui, e. `s3:TlsVersion` `aws:SecureTransport` `aws:SourceIp` `aws:VpcSourceIp` Se la tua policy utilizza queste chiavi di condizione con le Deny dichiarazioni, AWS i responsabili del servizio potrebbero essere bloccati involontariamente. Per consentire ai AWS servizi di funzionare correttamente mantenendo i requisiti di sicurezza, escludi i service principal dalle tue Deny dichiarazioni aggiungendo la chiave di `aws:PrincipalIsAWSService` condizione con il valore di. `false` Ad esempio:

```
{
  "Effect": "Deny",
  "Action": "s3:*",
  "Resource": "*",
  "Condition": {
```

```
"Bool": {
  "aws:SecureTransport": "false",
  "aws:PrincipalIsAWSService": "false"
}
}
```

Questa policy nega l'accesso alle operazioni di S3 quando HTTPS non viene utilizzato (`aws:SecureTransport` è falso), ma solo per gli utenti che non utilizzano servizi AWS. Ciò garantisce che le restrizioni condizionali si applichino a tutti i principali tranne i principali del servizio AWS.

Example

Il seguente esempio di policy del bucket nega le richieste di `PutObject` da parte di client che hanno una versione di TLS precedente a 1.2, ad esempio 1.1 o 1.0. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ],
      "Condition": {
        "NumericLessThan": {
          "s3:TlsVersion": 1.2
        }
      }
    }
  ]
}
```

Example

Il seguente esempio di policy del bucket consente le richieste di `PutObject` da parte di client che hanno una versione TLS successiva alla 1.1, ad esempio 1.2, 1.3 o successiva:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ],
      "Condition": {
        "NumericGreaterThan": {
          "s3:TlsVersion": 1.1
        }
      }
    }
  ]
}
```

Esempio 7: esclusione di determinati committenti da una dichiarazione di rifiuto

La seguente policy dei bucket nega a `s3:GetObject` l'accesso a *amzn-s3-demo-bucket*, tranne che ai principali con il numero di account *123456789012*. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessFromPrincipalNotInSpecificAccount",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:GetObject",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": [
            "123456789012"
          ]
        }
      }
    }
  ]
}
```

Esempio 8: imporre ai client di caricare in modo condizionato gli oggetti in base ai nomi delle chiavi degli oggetti o agli ETag

Con le scritture condizionali, è possibile aggiungere un'intestazione aggiuntiva alle richieste di WRITE per specificare le precondizioni dell'operazione S3. Questa intestazione specifica una condizione che, se non viene soddisfatta, comporta il fallimento dell'operazione S3. Ad esempio, si può evitare la sovrascrittura di dati esistenti convalidando che non vi siano oggetti con lo stesso nome di chiave già presenti nel bucket durante il caricamento degli oggetti. In alternativa, è possibile controllare il tag entità (ETag) di un oggetto in Amazon S3 prima di scrivere un oggetto.

Per esempi di policy di bucket che utilizzano le condizioni in una policy di bucket per imporre scritture condizionali, consulta [the section called “Applicazione delle scritture condizionali”](#).

Esempio 9: limitazione dell'accesso alle annotazioni in base al prefisso del nome

La seguente policy del bucket concede `s3user` all'utente l'autorizzazione a creare, recuperare ed eliminare annotazioni i cui nomi iniziano con `m1-output`. Ciò consente di limitare l'accesso alle annotazioni in base al prefisso del nome dell'annotazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/s3user"
      },
      "Action": [
        "s3:PutObjectAnnotation",
        "s3:GetObjectAnnotation",
        "s3:DeleteObjectAnnotation"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringLike": {
          "s3:annotation-prefix": "m1-output.*"
        }
      }
    }
  ]
}
```

Esempio 10: Richiesta di scritture condizionali per le operazioni di annotazione

La seguente politica del bucket nega `PutObjectAnnotation` e `DeleteObjectAnnotation` richiede a meno che il chiamante non includa l'intestazione condizionale `x-amz-object-if-match`. Ciò impone un controllo ottimistico della concorrenza per tutte le scritture di annotazioni sul bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireConditionalWritesForAnnotations",
      "Effect": "Deny",
```

```

    "Principal": "*",
    "Action": [
        "s3:PutObjectAnnotation",
        "s3:DeleteObjectAnnotation"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "Null": {
            "s3:x-amz-object-if-match": "true"
        }
    }
}

```

Esempio 11: limitazione della dimensione dell'impaginazione per ListObjectAnnotations

La seguente politica del bucket limita il `max-annotation-results` parametro a 100 o meno per tutte le richieste. `ListObjectAnnotations` Ciò impedisce ai chiamanti di richiedere set di risultati eccessivamente grandi.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitAnnotationListPageSize",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:ListObjectAnnotation",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:max-annotation-results": "100"
        }
      }
    }
  ]
}

```

Esempi: Chiavi di condizione di Amazon S3 per le operazioni sui bucket

I seguenti esempi di policy mostrano come sia possibile utilizzare chiavi di condizione specifiche di Amazon S3 per le operazioni sui bucket.

Argomenti

- [Esempio 1: concessione dell'GetObjectautorizzazione s3: con una condizione su un indirizzo IP](#)
- [Esempio 2: recupero di un elenco di oggetti in un bucket con un prefisso specifico](#)
- [Esempio 3: impostazione del numero massimo di chiavi](#)

Esempio 1: concessione dell'GetObject**autorizzazione** s3: con una condizione su un indirizzo IP

È possibile concedere agli utenti autenticati il permesso di utilizzare l'azione `s3:GetObject` se la richiesta proviene da un intervallo specifico di indirizzi IP (ad esempio, `192.0.2.*`), a meno che l'indirizzo IP non sia uno di quelli che si desidera escludere (ad esempio, `192.0.2.188`). Nel blocco `Condition`, `IpAddress` e `NotIpAddress` sono condizioni e a ciascuna condizione viene fornita una coppia chiave-valore da valutare. Entrambe le coppie chiave-valore in questo esempio utilizzano la chiave ampia. `aws:SourceIp` AWS Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

Note

I valori delle chiavi `IpAddress` e `NotIpAddress` specificati nel blocco `Condition` utilizzano la notazione CIDR, come descritto in RFC 4632. Per ulteriori informazioni, consulta <http://www.rfc-editor.org/rfc/rfc4632.txt>.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "192.0.2.0/24"
        }
      }
    }
  ]
}
```

```
        "NotIpAddress" : {  
            "aws:SourceIp": "192.0.2.188/32"  
        }  
    }  
}
```

Puoi anche utilizzare altre chiavi di condizione AWS a livello globale nelle policy di Amazon S3. Ad esempio, è possibile specificare le chiavi di condizione `aws:SourceVpce` e `aws:SourceVpc` nelle policy di bucket per gli endpoint VPC. Per esempi specifici consulta [Controllo dell'accesso dagli endpoint VPC con policy di bucket](#).

Note

Per alcune chiavi di condizione AWS globali, sono supportati solo determinati tipi di risorse. Pertanto, verificare se Amazon S3 supporta la chiave di condizione globale e il tipo di risorsa che si desidera utilizzare, o se invece è necessario utilizzare una chiave di condizione specifica di Amazon S3. Per un elenco completo dei tipi di risorse e delle chiavi di condizione supportate per Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Esempio 2: recupero di un elenco di oggetti in un bucket con un prefisso specifico

È possibile utilizzare la chiave di condizione `s3:prefix` per limitare la risposta dell'operazione API ai nomi di chiavi con un prefisso specifico [ListObjectsV2](#) API ai nomi delle chiavi con un prefisso specifico. Se si è il proprietario del bucket, si può usare questa chiave di condizione per limitare un utente a elencare il contenuto di un prefisso specifico nel bucket. La chiave di condizione `s3:prefix` è utile se gli oggetti del bucket sono organizzati per prefissi di nomi di chiavi.

La console di Amazon S3 utilizza i prefissi dei nomi delle chiavi per mostrare un concetto di cartella. Solo la console supporta il concetto di cartelle, mentre l'API Amazon S3 supporta solo bucket e oggetti. Ad esempio, se due oggetti hanno i nomi delle chiavi `public/object1.jpg` e `public/object2.jpg`, la console mostra gli oggetti sotto la cartella `public`. Nell'API Amazon S3 questi sono oggetti con prefissi, non oggetti nelle cartelle. Per ulteriori informazioni sull'utilizzo di prefissi e

delimitatori per filtrare le autorizzazioni di accesso, consulta [Procedura guidata: controllo dell'accesso a un bucket con policy utente](#).

Nel seguente scenario, il proprietario del bucket e l'account padre a cui appartiene l'utente sono gli stessi. Il proprietario del bucket può quindi utilizzare una policy del bucket o una policy dell'utente per concedere l'accesso. Per ulteriori informazioni sulle altre chiavi di condizione che è possibile utilizzare con l'operazione API `ListObjectsV2`, consulta la sezione [ListObjectsV2](#).

Note

Se per il bucket è abilitato il controllo delle versioni, per elencare gli oggetti nel bucket è necessario concedere l'autorizzazione `s3:ListBucketVersions` nelle policy seguenti, invece dell'autorizzazione `s3:ListBucket`. Il permesso `s3:ListBucketVersions` supporta anche la chiave di condizione `s3:prefix`.

Policy utente

La seguente policy utente concede l'autorizzazione `s3:ListBucket` (consulta [ListObjectsV2](#)) con un'istruzione `Condition` che richiede all'utente di specificare un prefisso nella richiesta con un valore di *projects*. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "s3:prefix": "projects"
        }
      }
    }
  ],
  {
```

```

        "Sid": "statement2",
        "Effect": "Deny",
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
        "Condition" : {
            "StringNotEquals" : {
                "s3:prefix": "projects"
            }
        }
    }
}
]
}

```

L'istruzione `Condition` limita l'utente a elencare solo le chiavi degli oggetti che hanno il prefisso *projects*. L'aggiunta dell'istruzione esplicita `Deny` impedisce all'utente di elencare le chiavi con qualsiasi altro prefisso, indipendentemente dalle altre autorizzazioni di cui dispone. Ad esempio, è possibile che l'utente ottenga l'autorizzazione a elencare le chiavi degli oggetti senza alcuna restrizione, sia attraverso l'aggiornamento della precedente policy dell'utente sia attraverso una policy del bucket. Poiché le istruzioni esplicite `Deny` sovrascrivono sempre le istruzioni `Allow`, se l'utente tenta di elencare chiavi diverse da quelle che hanno il prefisso *projects*, la richiesta viene rifiutata.

Policy del bucket

Se si aggiunge l'elemento `Principal` alla policy utente di cui sopra, che identifica l'utente, si ottiene una policy del bucket, come mostrato nell'esempio seguente. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    }
  ]
}

```

```

    "Condition" : {
      "StringEquals" : {
        "s3:prefix": "projects"
      }
    },
    {
      "Sid": "statement2",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition" : {
        "StringNotEquals" : {
          "s3:prefix": "projects"
        }
      }
    }
  ]
}

```

Verificate la policy con il AWS CLI

È possibile testare la politica utilizzando il seguente `list-object` AWS CLI comando. Nel comando, vengono fornite le credenziali utente utilizzando il parametro `--profile`. Per ulteriori informazioni sulla configurazione e l'utilizzo di AWS CLI, consulta [Developing with Amazon S3 using the AWS CLI](#) in Amazon S3 API Reference.

```
aws s3api list-objects --bucket amzn-s3-demo-bucket --prefix projects --
profile AccountA
```

Esempio 3: impostazione del numero massimo di chiavi

È possibile utilizzare la chiave di condizione `s3:max-keys` per impostare il numero massimo di chiavi che un richiedente può restituire in una richiesta [ListObjectsV2](#) o [ListObjectVersions](#). Per impostazione predefinita, queste operazioni API restituiscono fino a 1.000 chiavi. Per un elenco di operatori di condizione numerici che è possibile utilizzare con `s3:max-keys` e i relativi esempi, consulta [Operatori di condizione numerici](#) nella Guida per l'utente di IAM.

Identity-based politiche per Amazon S3

Per impostazione predefinita, gli utenti e i ruoli non hanno il permesso di creare o modificare le risorse Amazon S3. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM.

Per i dettagli sulle azioni e sui tipi di risorse definiti da Amazon S3, compreso il formato degli ARN per ciascun tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Argomenti

- [Best practice per le policy](#)
- [Procedura guidata: controllo dell'accesso a un bucket con policy utente](#)
- [Identity-based esempi di policy per Amazon S3](#)

Best practice per le policy

Identity-based le politiche determinano se qualcuno può creare, accedere o eliminare risorse Amazon S3 nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni agli utenti e ai carichi di lavoro, utilizza le policy AWS gestite che concedono autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dal AWS cliente specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche,

note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root Account AWS, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Procedura guidata: controllo dell'accesso a un bucket con policy utente

Questa spiegazione passo per passo illustra il funzionamento delle autorizzazioni utente con Amazon S3. In questo esempio, viene creato un bucket con cartelle. Quindi crei utenti AWS Identity and Access Management IAM nel tuo bucket Amazon S3 Account AWS e concedi a tali utenti autorizzazioni incrementali sul tuo bucket Amazon S3 e sulle cartelle in esso contenute.

Argomenti

- [Principi di base relativi a bucket e cartelle](#)
- [Riepilogo della spiegazione passo per passo](#)
- [Preparazione della procedura guidata](#)
- [Fase 1: creazione di un bucket](#)

- [Fase 2: creazione di un gruppo e di utenti IAM](#)
- [Fase 3: verifica che gli utenti IAM non dispongano di autorizzazioni](#)
- [Fase 4: concessione di autorizzazioni a livello di gruppo](#)
- [Fase 5: concessione di autorizzazioni specifiche all'utente IAM Alice](#)
- [Fase 6: concessione di autorizzazioni specifiche all'utente IAM Bob](#)
- [Fase 7: protezione della cartella Private \(Privato\)](#)
- [Fase 8: Pulizia](#)
- [Risorse correlate](#)

Principi di base relativi a bucket e cartelle

Il modello di dati di Amazon S3 è una struttura flat: crei un bucket e il bucket archivia gli oggetti. Non c'è nessuna gerarchia di bucket secondari o sottocartelle, ma è possibile emulare una gerarchia delle cartelle. Strumenti come la console di Amazon S3 possono presentare una panoramica di queste cartelle e sottocartelle logiche nel bucket.

La console mostra che un bucket denominato companybucket ha tre cartelle, Private, Development e Finance e un oggetto, s3-dg.pdf. La console utilizza i nomi oggetto (chiavi) per creare una gerarchia logica con cartelle e sottocartelle. Considerare i seguenti esempi:

- Quando crei la cartella Development, la console crea un oggetto con la chiave Development/. Nota il delimitatore finale '/' (/).
- Quando carichi un oggetto denominato Projects1.xls nella cartella Development, la console carica l'oggetto e gli assegna la chiave Development/Projects1.xls.

Nella chiave, Development è il [prefisso](#) e / è il delimitatore. L'API Amazon S3 supporta prefissi e delimitatori nelle operazioni. Ad esempio, è possibile ottenere un elenco di tutti gli oggetti da un bucket con un prefisso e un delimitatore specifici. Nella console, quando apri la cartella Development, viene visualizzato un elenco degli oggetti in essa contenuti. Nell'esempio seguente, la cartella Development contiene un solo oggetto.

Quando la console visualizza la cartella Development nel bucket companybucket, invia una richiesta ad Amazon S3 in cui specifica un prefisso Development e un delimitatore /. La risposta della console si presenta proprio come un elenco di cartelle nel file system del computer. L'esempio precedente mostra che il bucket companybucket ha un oggetto con la chiave Development/Projects1.xls.

La console utilizza le chiavi degli oggetti per dedurre una gerarchia logica. Amazon S3 non ha una gerarchia fisica. Amazon S3 dispone solo di bucket che contengono oggetti in una struttura di file piatti. Quando si creano oggetti utilizzando l'API Amazon S3, è possibile utilizzare le chiavi degli oggetti che implicano una gerarchia logica. Quando viene creata una gerarchia logica di oggetti, è possibile gestire l'accesso alle singole cartelle, come dimostrato in questa procedura guidata.

Prima di iniziare, assicurarsi di acquisire familiarità con il concetto di contenuto di un bucket a livello di root. Si supponga che il bucket `companybucket` abbia i seguenti oggetti:

- `Private/privDoc1.txt`
- `Private/privDoc2.zip`
- `Development/project1.xls`
- `Development/project2.xls`
- `Finance/Tax2011/document1.pdf`
- `Finance/Tax2011/document2.pdf`
- `s3-dg.pdf`

Queste chiavi degli oggetti creano una gerarchia logica con `Private`, `Development` e `Finance` come cartelle a livello root e `s3-dg.pdf` come un oggetto a livello root. Quando si sceglie il nome di un bucket nella console di Amazon S3, le voci a livello di root vengono visualizzate. La console mostra i prefissi di livello superiore (`Private/`, `Development/` e `Finance/`) come cartelle a livello di root. La chiave dell'oggetto `s3-dg.pdf` non ha prefisso e quindi appare come voce a livello root.

Riepilogo della spiegazione passo per passo

In questa procedura guidata, creare un bucket con tre cartelle (`Private`, `Development` e `Finance`) al suo interno.

Ci sono due utenti, Alice e Bob. Alice deve accedere solo alla cartella `Development`, mentre Bob deve accedere solo alla cartella `Finance`. Il contenuto della cartella `Private` deve essere mantenuto privato. Nella guida, si gestisce l'accesso creando utenti IAM (l'esempio utilizza i nomi Alice e Bob) e concedendo loro le autorizzazioni necessarie.

IAM supporta inoltre la creazione di gruppi di utenti e la concessione di autorizzazioni a livello di gruppo valide per tutti gli utenti presenti nel gruppo. In questo modo è possibile gestire le autorizzazioni in modo più efficiente. Per questo esercizio sia Alice che Bob hanno bisogno di

autorizzazioni comuni. Pertanto, verrà creato anche un gruppo denominato `Consultants` e Alice e Bob saranno aggiunti al gruppo. Inizialmente, le autorizzazioni vengono assegnate collegando una policy di gruppo al gruppo stesso. Quindi, vengono aggiunte autorizzazioni specifiche per gli utenti collegando le policy agli utenti specifici.

Note

La spiegazione passo per passo utilizza `companybucket` come nome del bucket, Alice e Bob come utenti IAM e `Consultants` come nome del gruppo. Poiché Amazon S3 richiede che i nomi di bucket siano univoci a livello globale, è necessario sostituire il nome del bucket con un nome personalizzato.

Preparazione della procedura guidata

In questo esempio, utilizzi le tue Account AWS credenziali per creare utenti IAM. Inizialmente, questi utenti non hanno autorizzazioni. Le autorizzazioni vengono concesse in modo incrementale per l'esecuzione di operazioni di Amazon S3 specifiche. Per testare queste autorizzazioni, viene effettuato l'accesso alla console con le credenziali di ciascun utente. Man mano che concedi le autorizzazioni in modo incrementale come Account AWS proprietario e verifichi le autorizzazioni come utente IAM, devi accedere e disconnetterti, ogni volta utilizzando credenziali diverse. È possibile eseguire questo test con un browser, ma il processo sarà più rapido se è possibile utilizzare due browser diversi. Usa un browser per connetterti Console di gestione AWS con le tue Account AWS credenziali e un altro browser per connetterti con le credenziali utente IAM.

Per accedere Console di gestione AWS con le tue Account AWS credenziali, vai a <https://console.aws.amazon.com/>. Un utente IAM non può accedere utilizzando lo stesso link. Un utente IAM deve utilizzare una pagina di IAM-enabled accesso. Come proprietario dell'account, è possibile fornire questo link agli utenti.

Per ulteriori informazioni su IAM, consulta [The Console di gestione AWS Sign-in Page](#) nella IAM User Guide.

Per fornire un collegamento di accesso agli utenti IAM

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro Navigation (Navigazione) scegli IAM Dashboard (Pannello di controllo IAM).

3. Prendere nota dell'URL in IAM users sign in link (Collegamento di accesso utenti IAM). Sarà necessario fornire questo collegamento agli utenti IAM affinché possano accedere alla console con il loro nome utente e la loro password IAM.

Fase 1: creazione di un bucket

In questa fase, si accede alla console Amazon S3 con le credenziali Account AWS , si crea un bucket, si aggiungono cartelle al bucket e si caricano uno o due documenti di esempio in ciascuna cartella.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Creare un bucket.

Per istruzioni dettagliate, consulta [Creazione di un bucket per uso generico](#).

3. Caricare un documento nel bucket.

Questo esercizio presume che il documento `s3-dg.pdf` si trovi a livello root di questo bucket. Se viene caricato un documento differente, è necessario sostituire il nome file con `s3-dg.pdf`.

4. Aggiungere tre cartelle denominate `Private`, `Finance` e `Development` al bucket.

Per istruzioni dettagliate sulla creazione di una cartella, consulta [Organizzazione degli oggetti nella console di Amazon S3 utilizzando le cartelle](#) nella Guida per l'utente di Amazon Simple Storage Service.

5. Caricare uno o due documenti in ciascuna cartella.

Per questo esercizio, si presume che siano stati caricati un paio di documenti in ciascuna cartella, in modo che il bucket abbia oggetti con le seguenti chiavi:

- `Private/privDoc1.txt`
- `Private/privDoc2.zip`
- `Development/project1.xls`
- `Development/project2.xls`
- `Finance/Tax2011/document1.pdf`
- `Finance/Tax2011/document2.pdf`
- `s3-dg.pdf`

Per istruzioni dettagliate, consulta [Caricamento degli oggetti](#).

Fase 2: creazione di un gruppo e di utenti IAM

Ora utilizza la [Console IAM](#) per aggiungere due utenti IAM, Alice e Bob, a Account AWS. Per le istruzioni passo-passo, consulta la sezione [Creazione di un utente IAM in Account AWS](#) nella Guida all'utente IAM.

Crea anche un gruppo amministrativo chiamato Consultants. Quindi, aggiungi entrambi gli utenti al gruppo. Per istruzioni dettagliate, consulta [Creazione di gruppi di utenti IAM](#).

Warning

Quando si aggiungono utenti e un gruppo, non collegare alcuna policy che assegni autorizzazioni agli utenti. Inizialmente, questi utenti non dispongono di alcuna autorizzazione. Nelle sezioni seguenti, le autorizzazioni vengono concesse in modo incrementale. In primo luogo, devi accertarti di avere assegnato le password a questi utenti IAM. Queste credenziali utente vengono utilizzate per testare le operazioni di Amazon S3 e verificare che le autorizzazioni funzionino come previsto.

Per le istruzioni passo-passo sulla creazione di un nuovo utente IAM, consulta [Creazione di un utente IAM in Account AWS](#) nella Guida all'utente IAM. Quando crei gli utenti per questa procedura guidata, seleziona Accesso alla Console di gestione AWS e deseleziona [Accesso programmatico](#).

Per istruzioni dettagliate sulla creazione di un gruppo amministrativo, consulta [Creazione del primo utente e gruppo di amministrazione IAM](#) nella Guida per l'utente di IAM.

Fase 3: verifica che gli utenti IAM non dispongano di autorizzazioni

Se stai utilizzando due browser, puoi ora utilizzare il secondo browser per effettuare l'accesso alla console con una delle credenziali utente IAM.

1. Utilizzando il link di accesso dell'utente IAM (consulta [Per fornire un collegamento di accesso agli utenti IAM](#)), effettua l'accesso alla Console di gestione AWS utilizzando una delle credenziali utente IAM.
2. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

Verifica il messaggio della console che indica che l'accesso è negato.

Ora, è possibile iniziare a concedere le autorizzazioni incrementali agli utenti. Innanzitutto, collegare una policy di gruppo che concede le autorizzazioni necessarie per entrambi gli utenti.

Fase 4: concessione di autorizzazioni a livello di gruppo

Gli utenti devono essere in grado di effettuare quanto segue:

- Elencare tutti i bucket di proprietà dell'account padre. A tale scopo, Bob e Alice devono avere l'autorizzazione per l'operazione `s3:ListAllMyBuckets`.
- Elencare le voci, le cartelle e gli oggetti a livello root nel bucket `companybucket`. A tale scopo, Bob e Alice devono avere l'autorizzazione per l'operazione `s3:ListBucket` nel bucket `companybucket`.

Innanzitutto, creare una policy che concede tali autorizzazioni e quindi collegarla al gruppo `Consultants`.

Fase 4.1: concessione di autorizzazione per elencare tutti i bucket

In questa fase viene creata una policy gestita che concede agli utenti le autorizzazioni minime per consentire loro di elencare tutti i bucket di proprietà dell'account padre. Quindi, tale policy verrà collegata al gruppo `Consultants`. Quando si collega la policy gestita a un utente o a un gruppo, si concede all'utente o al gruppo l'autorizzazione per ottenere un elenco dei bucket di proprietà dell'Account AWS parent.

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

Note

Poiché stai concedendo autorizzazioni utente, è necessario effettuare l'accesso con le credenziali dell' Account AWS , non come utente IAM.

2. Creare la policy gestita.
 - a. Nel riquadro di navigazione sulla sinistra, selezionare Policies (Policy) e scegliere Create Policy (Crea policy).

- b. Selezionare la scheda JSON.
- c. Copiare la policy di accesso seguente e incollarla nel campo di testo relativo alla policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGroupToSeeBucketListInTheConsole",
      "Action": ["s3:ListAllMyBuckets"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    }
  ]
}
```

Una policy è un documento JSON. Nel documento, uno `Statement` è una serie di oggetti, ognuno dei quali descrive un'autorizzazione utilizzando un insieme di coppie di nome-valore. La suddetta policy descrive un'autorizzazione specifica. L'`Action` specifica il tipo di accesso. Nella policy, `s3:ListAllMyBuckets` è un'operazione di Amazon S3 predefinita. Questa azione copre l'operazione Amazon S3 GET Service, che restituisce un elenco di tutti i bucket di proprietà del mittente autenticato. Il valore dell'elemento `Effect` determina se un'autorizzazione specifica è consentita o rifiutata.

- d. Scegliere `Review policy (Esamina policy)`. Nella pagina successiva, immettere `AllowGroupToSeeBucketListInTheConsole` nel campo `Name (Nome)`, quindi scegliere `Create policy (Crea policy)`.

 Note

La voce `Summary (Riepilogo)` visualizza un messaggio in cui si afferma che la policy non concede alcuna autorizzazione. Per questa procedura guidata, il messaggio può essere ignorato.

3. Collegare la policy gestita `AllowGroupToSeeBucketListInTheConsole` che è stata creata al gruppo `Consultants`.

Per le istruzioni passo-passo per allegare una policy gestita, consulta [Aggiunta e rimozione di autorizzazioni di identità IAM](#) nella Guida all'utente IAM.

I documenti della policy vengono collegati agli utenti e ai gruppi IAM nella console IAM. Poiché entrambi gli utenti devono essere in grado di elencare i bucket, la policy deve essere collegata al gruppo.

4. Testare l'autorizzazione.

- a. Utilizzando il collegamento di accesso utente IAM (consultare [Per fornire un collegamento di accesso agli utenti IAM](#)), accedere alla console con una delle credenziali utente IAM.
- b. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.

La console ora dovrebbe elencare tutti i bucket, ma non gli oggetti contenuti in ogni bucket.

Fase 4.2: abilitazione degli utenti a elencare il contenuto di un bucket a livello root

Di seguito, consentire a tutti gli utenti nel gruppo Consultants di elencare le voci del bucket companybucket a livello root. Quando un utente sceglie il bucket aziendale nella console di Amazon S3, può visualizzare le voci a livello root nel bucket.

Note

Questo esempio utilizza companybucket a scopo illustrativo. È necessario utilizzare il nome del bucket che è stato creato.

Per comprendere la richiesta che la console invia ad Amazon S3 quando si sceglie il nome di un bucket, la risposta che Amazon S3 restituisce e il modo in cui la console interpreta la risposta, esaminare il flusso un po' più da vicino.

Quando viene scelto un nome di bucket, la console invia la richiesta [GET Bucket \(ListObjects\)](#) ad Amazon S3. Questa richiesta include i seguenti parametri:

- Il parametro `prefix` che presenta una stringa vuota come valore.
- Il parametro `delimiter` con `/` come valore.

Di seguito è riportata una richiesta di esempio.

```
GET ?prefix=&delimiter=/ HTTP/1.1
Host: companybucket.s3.amazonaws.com
Date: Wed, 01 Aug 2012 12:00:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
```

Amazon S3 restituisce una risposta che include il seguente elemento `<ListBucketResult/>`.

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>companybucket</Name>
  <Prefix></Prefix>
  <Delimiter></Delimiter>
  ...
  <Contents>
    <Key>s3-dg.pdf</Key>
    ...
  </Contents>
  <CommonPrefixes>
    <Prefix>Development/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Finance/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Private/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

L'oggetto `s3-dg.pdf` della chiave non contiene il delimitatore barra (/) e Amazon S3 restituisce la chiave nell'elemento `<Contents>`. Tutte le altre chiavi nel bucket di esempio contengono tuttavia il delimitatore /. Amazon S3 raggruppa queste chiavi e restituisce un elemento `<CommonPrefixes>` per ciascuno dei diversi valori di prefisso `Development/`, `Finance/` e `Private/` che corrisponde a una sottostringa dall'inizio di queste chiavi alla prima occorrenza del delimitatore / specificato.

La console interpreta questo risultato e mostra le voci a livello root come tre cartelle e una chiave dell'oggetto.

Se Bob o Alice apre la cartella `Development`, la console invia la richiesta [GET Bucket \(ListObjects\)](#) ad Amazon S3 con i parametri `prefix` e `delimiter` impostati sui seguenti valori:

- Il parametro `prefix` con il valore `Development/`.
- Il parametro `delimiter` con il valore `"/"`.

In risposta, Amazon S3 restituisce le chiavi degli oggetti che iniziano con il prefisso specificato.

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>companybucket</Name>
  <Prefix>Development</Prefix>
  <Delimiter>/</Delimiter>
  ...
  <Contents>
    <Key>Project1.xls</Key>
    ...
  </Contents>
  <Contents>
    <Key>Project2.xls</Key>
    ...
  </Contents>
</ListBucketResult>
```

La console mostra le chiavi degli oggetti.

Ora, tornare alla concessione dell'autorizzazione agli utenti per elencare le voci del bucket a livello root. Per elencare il contenuto del bucket, gli utenti devono disporre dell'autorizzazione per chiamare l'operazione `s3:ListBucket`, come illustrato nella seguente dichiarazione di policy. Per garantire che visualizzino solo il contenuto a livello principale, aggiungi una condizione in base alla quale gli utenti devono specificare uno spazio vuoto `prefix` nella richiesta, ovvero non sono autorizzati ad aprire nessuna delle cartelle a livello di root. Infine, aggiungere una condizione per esigere un accesso di tipo cartella imponendo che le richieste dell'utente includano il parametro `delimiter` con il valore `"/"`.

```
{
  "Sid": "AllowRootLevelListingOfCompanyBucket",
  "Action": ["s3:ListBucket"],
  "Effect": "Allow",
  "Resource": ["arn:aws:s3:::companybucket"],
  "Condition": {
    "StringEquals": {
      "s3:prefix": [""], "s3:delimiter": ["/"]
    }
  }
}
```

Quando scegli un bucket sulla console Amazon S3, la console invia innanzitutto la richiesta di posizione del bucket GET per trovare il punto in cui è [distribuito il bucket](#). Regione AWS Quindi la console utilizza l' Region-specific endpoint del bucket per inviare la richiesta GET Bucket (List Objects). Di conseguenza, se gli utenti utilizzeranno la console, è necessario assegnare l'autorizzazione per l'operazione `s3:GetBucketLocation` come illustrato nella seguente dichiarazione di policy.

```
{
  "Sid": "RequiredByS3Console",
  "Action": ["s3:GetBucketLocation"],
  "Effect": "Allow",
  "Resource": ["arn:aws:s3:::*"]
}
```

Per consentire agli utenti di elencare il contenuto di un bucket a livello root

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>

Usa Account AWS le tue credenziali, non le credenziali di un utente IAM, per accedere alla console.

2. Sostituire la policy gestita `AllowGroupToSeeBucketListInTheConsole` esistente che è collegata al gruppo `Consultants` con la seguente policy, che consente anche l'operazione `s3:ListBucket`. Ricordarsi di sostituire *companybucket* nella policy Resource con il nome del proprio bucket.

Per istruzioni dettagliate, consulta [Modifica delle policy IAM](#) nella Guida all'utente IAM. Quando si seguono le istruzioni dettagliate, accertarsi di seguire le fasi per l'applicazione delle modifiche a tutte le entità principali a cui è collegata la policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
      "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
      "Action": [ "s3:ListAllMyBuckets", "s3:GetBucketLocation" ],
```

```
    "Effect": "Allow",
    "Resource": [ "arn:aws:s3:::*" ]
  },
  {
    "Sid": "AllowRootLevelListingOfCompanyBucket",
    "Action": ["s3:ListBucket"],
    "Effect": "Allow",
    "Resource": ["arn:aws:s3::companybucket"],
    "Condition": {
      "StringEquals": {
        "s3:prefix": [""], "s3:delimiter": ["/"]
      }
    }
  }
]
```

3. Test delle autorizzazioni aggiornate.

- a. Mediante il link di accesso dell'utente IAM (consulta [Per fornire un collegamento di accesso agli utenti IAM](#)), accedere alla Console di gestione AWS.

Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

- b. Scegliere il bucket creato. La console mostra le voci del bucket a livello root. Se si sceglie qualsiasi cartella nel bucket, non sarà possibile visualizzare il contenuto della cartella perché le relative autorizzazioni non sono state ancora concesse.

Questo test ha esito positivo quando gli utenti utilizzano la console di Amazon S3. Quando si sceglie un bucket sulla console, l'implementazione della console invia una richiesta che include il parametro `prefix` con una stringa vuota come valore e il parametro `delimiter` con `/` come valore.

Fase 4.3: sintesi della policy di gruppo

L'effetto della policy di gruppo aggiunta è quello di concedere agli utenti IAM Alice e Bob le seguenti autorizzazioni minime:

- Elencare tutti i bucket di proprietà dell'account padre.
- Visualizzare le voci a livello root nel bucket `companybucket`.

Tuttavia, gli utenti ancora non possono fare molto. Di seguito, concedere autorizzazioni specifiche per utente, come segue:

- Consentire a Alice di prendere e mettere oggetti nella cartella Development.
- Consentire a Bob di prendere e mettere oggetti nella cartella Finance.

Per le autorizzazioni specifiche dell'utente, collegare una policy all'utente specifico, non al gruppo. Nella sezione seguente, ad Alice vengono concesse le autorizzazioni per lavorare nella cartella Development. È possibile ripetere le fasi per concedere un'autorizzazione simile a Bob per lavorare nella cartella Finance.

Fase 5: concessione di autorizzazioni specifiche all'utente IAM Alice

È necessario ora concedere autorizzazioni aggiuntive ad Alice in modo che possa vedere il contenuto della cartella Development per poter prendere e mettere oggetti nella stessa.

Fase 5.1: concessione dell'autorizzazione a elencare il contenuto della cartella Development all'utente IAM Alice

Affinché Alice possa elencare il contenuto della cartella Development, è necessario applicare all'utente Alice una policy che conceda l'autorizzazione per l'azione `s3:ListBucket` sul bucket `companybucket`, a condizione che la richiesta includa il prefisso `Development/`. Questa policy deve essere applicata solo all'utente Alice, pertanto viene utilizzata una policy inline. Per ulteriori informazioni sulle policy inline, consulta [Policy gestite e policy inline](#) nella Guida per l'utente di IAM.

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

Usa Account AWS le tue credenziali, non le credenziali di un utente IAM, per accedere alla console.

2. Creare una policy inline per concedere all'utente Alice l'autorizzazione per elencare il contenuto della cartella Development.
 - a. Nel riquadro di navigazione sinistro, scegliere Users (Utenti).
 - b. Scegli il nome utente Alice.
 - c. Nella pagina dei dettagli dell'utente, scegliere la scheda Permissions (Autorizzazioni), quindi selezionare Add inline policy (Aggiungi policy inline).
 - d. Selezionare la scheda JSON.

- e. Copia la seguente policy per incollarla nel campo di testo della policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListBucketIfSpecificPrefixIsIncludedInRequest",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition": { "StringLike": {"s3:prefix": ["Development/*"]} }
    }
  ]
}
```

- f. Scegliere Review policy (Esamina policy). Nella pagina successiva, immettere un nome nel campo Name (Nome), quindi scegliere Create policy (Crea policy).
3. Test della modifica apportata alle autorizzazioni di Alice:
 - a. Mediante il link di accesso dell'utente IAM (consulta [Per fornire un collegamento di accesso agli utenti IAM](#)), accedere alla Console di gestione AWS.
 - b. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
 - c. Nella console di Amazon S3 verificare che Alice possa visualizzare l'elenco degli oggetti nella cartella Development/ del bucket.

Quando l'utente sceglie la cartella /Development per visualizzare l'elenco degli oggetti in essa contenuti, la console di Amazon S3 invia la richiesta ListObjects ad Amazon S3 con il prefisso /Development. Poiché all'utente è stata concessa l'autorizzazione per visualizzare l'elenco degli oggetti con il prefisso Development e il delimitatore /, Amazon S3 restituisce l'elenco degli oggetti con il prefisso della chiave Development/ e la console visualizza tale elenco.

Fase 5.2: concessione delle autorizzazioni a recuperare e inserire oggetti nella cartella Development all'utente IAM Alice

Affinché Alice possa prendere e mettere oggetti nella cartella Development, ha bisogno di un'autorizzazione per chiamare le operazioni `s3:GetObject` e `s3:PutObject`. Le seguenti dichiarazioni di policy assegnano queste autorizzazioni purché la richiesta includa il parametro `prefix` con un valore di `Development/`.

```
{
  "Sid": "AllowUserToReadWriteObjectData",
  "Action": ["s3:GetObject", "s3:PutObject"],
  "Effect": "Allow",
  "Resource": ["arn:aws:s3:::companybucket/Development/*"]
}
```

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

Usa Account AWS le tue credenziali, non le credenziali di un utente IAM, per accedere alla console.

2. Modificare la policy inline creata nella fase precedente.
 - a. Nel riquadro di navigazione sinistro, scegliere Users (Utenti).
 - b. Scegliere il nome utente Alice.
 - c. Nella pagina dei dettagli, scegliere la scheda Permissions (Autorizzazioni) ed espandere la sezione Inline Policies (Policy inline).
 - d. Accanto al nome della policy creata nella fase precedente, scegliere Edit Policy (Modifica policy) .
 - e. Copiare la seguente policy e incollarla nel campo di testo della policy, sostituendo la policy esistente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
    "Sid": "AllowListBucketIfSpecificPrefixIsIncludedInRequest",
    "Action": ["s3:ListBucket"],
    "Effect": "Allow",
    "Resource": ["arn:aws:s3:::companybucket"],
    "Condition": {
      "StringLike": {"s3:prefix": ["Development/*"]}
    }
  },
  {
    "Sid": "AllowUserToReadWriteObjectDataInDevelopmentFolder",
    "Action": ["s3:GetObject", "s3:PutObject"],
    "Effect": "Allow",
    "Resource": ["arn:aws:s3:::companybucket/Development/*"]
  }
]
```

3. Test della policy aggiornata:

- a. Mediante il link di accesso dell'utente IAM (consulta [Per fornire un collegamento di accesso agli utenti IAM](#)), accedere alla Console di gestione AWS.
- b. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
- c. Nella console di Amazon S3 verificare che Alice possa aggiungere e scaricare un oggetto nella cartella Development.

Fase 5.3: rifiuto esplicito delle autorizzazioni relative a qualsiasi altra cartella del bucket per l'utente IAM Alice

L'utente Alice ora può elencare il contenuto del bucket companybucket a livello root. Inoltre, ora può prendere e mettere oggetti nella cartella Development. Se si vuole effettivamente limitare le autorizzazioni di accesso, è possibile rifiutare esplicitamente ad Alice l'accesso a qualsiasi altra cartella del bucket. Se esiste qualsiasi altra policy (policy di bucket o ACL) che assegna ad Alice l'accesso a eventuali altre cartelle del bucket, questo rifiuto esplicito sovrascrive tali autorizzazioni.

È possibile aggiungere la seguente istruzione alla policy utente di Alice, che prevede che tutte le richieste inviate da Alice ad Amazon S3 includano il parametro prefix, il cui valore può essere Development/* oppure una stringa vuota.

```
{
```

```
"Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
"Action": ["s3:ListBucket"],
"Effect": "Deny",
"Resource": ["arn:aws:s3:::companybucket"],
"Condition":{
  "StringNotLike": {"s3:prefix":["Development/*",""] },
  "Null"           : {"s3:prefix":false }
}
}
```

Esistono due espressioni condizionali nel blocco `Condition`. Il risultato di queste espressioni condizionali viene combinato utilizzando l'AND logico. Se entrambe le condizioni sono vere, il risultato della condizione combinata è vero. Poiché `Effect` in questa policy è `Deny`, quando `Condition` viene valutata `true`, gli utenti non saranno in grado di eseguire la `Action` specificata.

- L'espressione condizionale `Null` assicura che le richieste provenienti da Alice includano il parametro `prefix`.

Il parametro `prefix` richiede l'accesso di tipo cartella. Se viene inviata una richiesta senza il parametro `prefix`, Amazon S3 restituisce tutte le chiavi degli oggetti.

Se la richiesta include il parametro `prefix` con un valore `null`, l'espressione restituisce il valore `True`, quindi tutta la `Condition` restituisce il valore `True`. È necessario consentire una stringa vuota come valore del parametro `prefix`. Da quanto detto in precedenza, ricordare che permettere una stringa nulla significa consentire ad Alice di recuperare le voci del bucket a livello root come fa la console nella precedente discussione. Per ulteriori informazioni, consulta [Fase 4.2: abilitazione degli utenti a elencare il contenuto di un bucket a livello root](#).

- L'espressione condizionale `StringNotLike` assicura che se il valore del parametro `prefix` viene specificato e non è `Development/*`, la richiesta ha esito negativo.

Seguire le fasi della sezione precedente e aggiornare nuovamente la policy inline creata per l'utente Alice.

Copiare la seguente policy e incollarla nel campo di testo della policy, sostituendo la policy esistente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

    {
      "Sid": "AllowListBucketIfSpecificPrefixIsIncludedInRequest",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition": {
        "StringLike": {"s3:prefix": ["Development/*"]}
      }
    },
    {
      "Sid": "AllowUserToReadWriteObjectDataInDevelopmentFolder",
      "Action": ["s3:GetObject", "s3:PutObject"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket/Development/*"]
    },
    {
      "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition": {
        "StringNotLike": {"s3:prefix": ["Development/*", "" ]},
        "Null"           : {"s3:prefix": false }
      }
    }
  ]
}

```

Fase 6: concessione di autorizzazioni specifiche all'utente IAM Bob

È necessario ora assegnare a Bob l'autorizzazione per la cartella Finance. Seguire le fasi utilizzate precedentemente per assegnare le autorizzazioni ad Alice ma sostituire la cartella Development con la cartella Finance. Per istruzioni dettagliate, consulta [Fase 5: concessione di autorizzazioni specifiche all'utente IAM Alice](#).

Fase 7: protezione della cartella Private (Privato)

In questo esempio, vi sono soltanto due utenti. Sono state concesse le autorizzazioni minime a livello di gruppo e quelle a livello di utente unicamente quando erano veramente necessarie delle autorizzazioni a livello di singolo utente. Questo approccio contribuisce ad alleggerire l'impegno necessario per gestire le autorizzazioni. Con l'aumento del numero degli utenti, la gestione delle autorizzazioni può diventare gravosa. Ad esempio, non vogliamo che alcun utente di questo esempio

acceda al contenuto della cartella `Private`. Come ci si assicura di non concedere accidentalmente a un utente i permessi per la cartella `Private`? È necessario aggiungere una policy che rifiuti esplicitamente l'accesso alla cartella. Un rifiuto esplicito sovrascrive qualsiasi altra autorizzazione.

Per essere certi che la cartella `Private` resti privata, è possibile aggiungere le seguenti due dichiarazioni di rifiuto alla policy di gruppo:

- Aggiungere la seguente dichiarazione per rifiutare esplicitamente qualsiasi operazione sulle risorse della cartella `Private` (`companybucket/Private/*`).

```
{
  "Sid": "ExplicitDenyAccessToPrivateFolderToEveryoneInTheGroup",
  "Action": ["s3:*"],
  "Effect": "Deny",
  "Resource": ["arn:aws:s3:::companybucket/Private/*"]
}
```

- Viene inoltre rifiutata l'autorizzazione a eseguire l'operazione di elenco degli oggetti quando la richiesta specifica il prefisso `Private/`. Nella console, se Bob o Alice apre la cartella `Private`, questa policy fa in modo che Amazon S3 restituisca una risposta di errore.

```
{
  "Sid": "DenyListBucketOnPrivateFolder",
  "Action": ["s3:ListBucket"],
  "Effect": "Deny",
  "Resource": ["arn:aws:s3::*"],
  "Condition": {
    "StringLike": {"s3:prefix": ["Private/"]}
  }
}
```

Sostituire la policy del gruppo `Consultants` con una policy aggiornata che includa le precedenti dichiarazioni di rifiuto. Una volta applicata la policy aggiornata, nessuno degli utenti del gruppo può accedere alla cartella `Private` nel bucket.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

Usa Account AWS le tue credenziali, non le credenziali di un utente IAM, per accedere alla console.

2. Sostituire la policy gestita AllowGroupToSeeBucketListInTheConsole esistente che è collegata al gruppo Consultants con la seguente policy. Ricordarsi di sostituire *companybucket* nella policy con il nome del bucket.

Per istruzioni, consulta [Modifica delle policy gestite dai clienti](#) nella Guida all'utente IAM. Quando si seguono le istruzioni, osservare le indicazioni per l'applicazione delle modifiche a tutte le entità principali a cui è collegata la policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
"AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
      "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    },
    {
      "Sid": "AllowRootLevelListingOfCompanyBucket",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition": {
        "StringEquals": {"s3:prefix": [""]}
      }
    },
    {
      "Sid": "RequireFolderStyleList",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition": {
        "StringNotEquals": {"s3:delimiter": ["/"]}
      }
    },
    {
      "Sid": "ExplicitDenyAccessToPrivateFolderToEveryoneInTheGroup",
      "Action": ["s3:*"],
      "Effect": "Deny",
```

```
    "Resource": ["arn:aws:s3:::companybucket/Private/*"]
  },
  {
    "Sid": "DenyListBucketOnPrivateFolder",
    "Action": ["s3:ListBucket"],
    "Effect": "Deny",
    "Resource": ["arn:aws:s3::*"],
    "Condition": {
      "StringLike": {"s3:prefix": ["Private/"]}
    }
  }
]
```

Fase 8: Pulizia

Per la pulizia, apri la [Console IAM](#) e rimuovi gli utenti Alice e Bob. Per istruzioni dettagliate, consulta [Eliminazione di un utente IAM](#) nella Guida all'utente IAM.

Per essere certi che non vengano addebitati costi aggiuntivi per lo storage, è necessario eliminare anche gli oggetti e il bucket che è stato creato per questo esercizio.

Risorse correlate

- [Gestione di policy IAM](#) nella Guida per l'utente IAM

Identity-based esempi di policy per Amazon S3

Questa sezione mostra diversi esempi di policy basate sull'identità AWS Identity and Access Management (IAM) per il controllo dell'accesso ad Amazon S3. Per le policy dei bucket (policy basate sulle risorse), consulta [Policy dei bucket per Amazon S3](#). Per informazioni sul linguaggio delle policy IAM, consulta [Policy e autorizzazioni in Amazon S3](#).

Le policy di esempio seguenti funzionano se vengono testate a livello di programma. Per utilizzarle con la console di Amazon S3 occorre tuttavia concedere autorizzazioni aggiuntive che sono richieste dalla console. Per ulteriori informazioni sull'utilizzo di policy come queste con la console di Amazon S3, consulta [Procedura guidata: controllo dell'accesso a un bucket con policy utente](#).

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Argomenti

- [Concessione a un utente IAM dell'accesso a uno dei bucket](#)
- [Concessione a ogni utente IAM dell'accesso a una cartella in un bucket](#)
- [Concessione a un gruppo dell'accesso a una cartella condivisa in Amazon S3](#)
- [Permesso a tutti gli utenti di leggere gli oggetti in una parte del bucket](#)
- [Permesso a un partner di rilasciare i file in una parte specifica del bucket](#)
- [Limitare l'accesso ai bucket Amazon S3 all'interno di uno specifico Account AWS](#)
- [Limitare l'accesso ai bucket Amazon S3 all'interno della propria unità organizzativa](#)
- [Limitazione dell'accesso ai bucket Amazon S3 all'interno dell'organizzazione](#)
- [Concessione dell'autorizzazione per recuperare il PublicAccessBlock configurazione per un Account AWS](#)
- [Limitare la creazione di bucket a una sola Regione](#)

Concessione a un utente IAM dell'accesso a uno dei bucket

In questo esempio, vuoi concedere a un utente IAM l' Account AWS accesso a uno dei tuoi bucket e consentirgli di aggiungere *amzn-s3-demo-bucket1*, aggiornare ed eliminare oggetti.

Oltre ad assegnare le autorizzazioni `s3:PutObject`, `s3:GetObject` e `s3:DeleteObject` all'utente, la policy assegna anche le autorizzazioni `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Queste sono le autorizzazioni aggiuntive richieste dalla console. Inoltre, le operazioni `s3:PutObjectAcl` e `s3:GetObjectAcl` sono necessarie per essere in grado di copiare, tagliare e incollare gli oggetti nella console. Per una procedura guidata di esempio che concede autorizzazioni a utenti e le testa utilizzando la console, consulta [Procedura guidata: controllo dell'accesso a un bucket con policy utente](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
  ],
}
```



```

    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketLocation"],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
  ]
}

```

Concessione a ogni utente IAM dell'accesso a una cartella in un bucket

In questo esempio, si vuole che due utenti IAM, Mary e Carlos, abbiano accesso al bucket, *amzn-s3-demo-bucket1*, in modo che possano aggiungere, aggiornare e cancellare oggetti. Tuttavia, si vuole limitare l'accesso di ciascun utente a un unico prefisso (cartella) nel bucket. Si possono creare cartelle con nomi che corrispondono ai loro nomi utente.

```

amzn-s3-demo-bucket1
  Mary/
  Carlos/

```

Per assegnare a ciascun utente unicamente l'accesso alla cartella, è possibile scrivere una policy per ogni utente e collegarla singolarmente. È ad esempio possibile collegare la seguente policy all'utente Mary per concederle autorizzazioni Amazon S3 specifiche sulla cartella *amzn-s3-demo-bucket1/Mary*.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```
{
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/Mary/*"
}
```

Successivamente, è possibile collegare una policy simile all'utente Carlos, specificando la cartella *Carlos* nel valore Resource.

Invece di collegare le policy ai singoli utenti, è possibile scrivere un'unica policy che utilizzi una variabile di policy, collegandola poi a un gruppo. In primo luogo, occorre creare un gruppo e aggiungervi Mary e Carlos. La seguente policy di esempio concede un set di autorizzazioni Amazon S3 nella cartella *amzn-s3-demo-bucket1/\${aws:username}*. Quando la policy viene valutata, la variabile della policy *\${aws:username}* viene sostituita dal nome utente del richiedente. Ad esempio, se Mary invia una richiesta di inserimento di un oggetto, l'operazione è consentita solo se l'oggetto viene caricato nella cartella *amzn-s3-demo-bucket1/Mary*.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
    }
  ]
}
```

```
}  
]  
}
```

Note

Quando si utilizzano le variabili di policy, è necessario specificare esplicitamente la versione 2012-10-17 nella policy. La versione di default del linguaggio della policy IAM, 2008-10-17, non supporta le variabili di policy.

Se si vuole testare la policy precedente nella console di Amazon S3, la console deve avere l'autorizzazione per ottenere autorizzazioni aggiuntive, come illustrato nella policy seguente. Per ulteriori informazioni su come la console utilizza queste autorizzazioni, consulta [Procedura guidata: controllo dell'accesso a un bucket con policy utente](#).

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowGroupToSeeBucketListInTheConsole",  
      "Action": [  
        "s3:ListAllMyBuckets",  
        "s3:GetBucketLocation"  
      ],  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3:::"  
    },  
    {  
      "Sid": "AllowRootLevelListingOfTheBucket",  
      "Action": "s3:ListBucket",  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",  
      "Condition": {  
        "StringEquals": {  
          "s3:prefix": [""], "s3:delimiter": ["/"]  
        }  
      }  
    }  
  ]  
}
```

```

    },
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition": { "StringLike": {"s3:prefix": ["${aws:username}/*"] }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
    }
  ]
}

```

Note

Nella versione 2012-10-17 della policy, le variabili di policy iniziano con \$. Questa modifica nella sintassi potenzialmente può creare un conflitto se la chiave dell'oggetto (nome dell'oggetto) include un \$.

Per evitare questo conflitto, specificare il carattere \$ usando \${\$}. Ad esempio, per includere una chiave dell'oggetto my\$file in una policy, si specifica il carattere con my\${\$}file.

Sebbene i nomi utente IAM siano identificatori semplici, in formato leggibile, non sono necessariamente univoci a livello globale. Ad esempio, se l'utente Carlos lascia l'organizzazione ed entra un altro utente Carlos, il Carlos nuovo potrebbe accedere alle informazioni del precedente Carlos.

Invece di usare i nomi utente, si possono creare cartelle basate sugli ID utente IAM. Ogni ID utente IAM è univoco. In questo caso, si deve modificare la policy precedente per utilizzare la variabile di

policy `${aws:userid}`. Per ulteriori informazioni sugli identificatori utente, consulta [Identificatori IAM](#) nella Guida per l'utente di IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/home/${aws:userid}/*"
    }
  ]
}
```

Concessione a utenti non IAM (utenti dell'app per dispositivi mobili) dell'accesso alle cartelle in un bucket

Si supponga che si vuole sviluppare un'app mobile, un gioco che archivia i dati degli utenti in un bucket S3. Per ogni utente dell'app, si vuole creare una cartella nel bucket. Si vuole anche limitare l'accesso di ogni utente alla propria cartella. Ma non è possibile creare cartelle prima che qualcuno scarichi l'applicazione e inizi a giocare, perché non si dispone del suo ID utente.

In questo caso, è possibile richiedere agli utenti di accedere all'app mediante provider di identità pubblici quali Login with Amazon, Facebook o Google. Una volta che gli utenti hanno effettuato l'accesso all'app mediante uno di questi provider, dispongono di un ID utente che può essere utilizzato per creare cartelle specifiche di un determinato utente al runtime.

Puoi quindi utilizzare la federazione delle identità web Servizio di token di sicurezza AWS per integrare le informazioni del provider di identità con la tua app e ottenere credenziali di sicurezza temporanee per ogni utente. Successivamente è possibile creare policy IAM che permettono all'app di accedere al bucket ed eseguire operazioni come la creazione di cartelle specifiche dell'utente

e il caricamento dei dati. Per ulteriori informazioni sulla federazione delle identità Web, consulta [Informazioni sulla federazione delle identità Web](#) nella Guida per l'utente di IAM.

Concessione a un gruppo dell'accesso a una cartella condivisa in Amazon S3

Collegando la policy seguente al gruppo viene concesso a tutti i membri del gruppo l'accesso alla seguente cartella in Amazon S3: *amzn-s3-demo-bucket1*/share/marketing. I membri del gruppo possono accedere solo alle autorizzazioni Amazon S3 specifiche illustrate nella policy e unicamente per gli oggetti nella cartella specificata.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/share/marketing/*"
    }
  ]
}
```

Permesso a tutti gli utenti di leggere gli oggetti in una parte del bucket

In questo esempio viene creato un gruppo denominato *AllUsers*, che contiene tutti gli utenti IAM che appartengono all' Account AWS. Viene collegata quindi una policy che consente al gruppo di accedere a `GetObject` e `GetObjectVersion`, ma solo per gli oggetti nella cartella *amzn-s3-demo-bucket1/readonly*.

JSON

```
{
```

```
"Version":"2012-10-17",
"Statement":[
  {
    "Effect":"Allow",
    "Action":[
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/readonly/*"
  }
]
```

Permesso a un partner di rilasciare i file in una parte specifica del bucket

In questo esempio, viene creato un gruppo denominato *AnyCompany* che rappresenta un'azienda partner. Viene creato un utente IAM per la persona o l'applicazione specifica presso l'azienda partner che ha necessità di effettuare l'accesso, quindi l'utente viene inserito nel gruppo.

Viene collegata quindi una policy che consente al gruppo di accedere alla cartella seguente in un bucket aziendale:

amzn-s3-demo-bucket1/uploads/anycompany

Desideri inoltre impedire al gruppo *AnyCompany* di eseguire qualsiasi altra operazione con il bucket, quindi aggiungi un'istruzione che rifiuta esplicitamente l'autorizzazione per qualsiasi azione Amazon S3 ad eccezione di PutObject su qualsiasi risorsa Amazon S3 nell'account Account AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":["s3:PutObject"],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
    },
    {
      "Effect":"Deny",
      "Action":["s3:*"],
```

```

    "NotResource": "arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
  }
]
}

```

Limitare l'accesso ai bucket Amazon S3 all'interno di uno specifico Account AWS

Se vuoi assicurarti che i tuoi principali Amazon S3 accedano solo alle risorse che si trovano all'interno di un account affidabile Account AWS, puoi limitare l'accesso. Ad esempio, questa [Policy IAM basata sull'identità](#) utilizza un effetto Deny per bloccare l'accesso alle azioni Amazon S3, a meno che la risorsa Amazon S3 a cui si accede non sia presente nell'account **222222222222**. Per impedire a un responsabile IAM di accedere a oggetti Amazon S3 esterni all'account, allega la seguente policy IAM: Account AWS

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyS3AccessOutsideMyBoundary",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": [
            "222222222222"
          ]
        }
      }
    }
  ]
}

```


 Note

Questa policy non sostituisce i controlli di accesso IAM esistenti, perché non concede alcun accesso. Invece, questa policy funge da guardrail aggiuntivo per le altre autorizzazioni IAM, indipendentemente dalle autorizzazioni concesse tramite altre policy IAM.

Assicurati di sostituire l'ID account **222222222222** nella policy con il tuo Account AWS. Per applicare una policy a più account pur mantenendo questa restrizione, sostituire l'ID account con la chiave di condizione `aws:PrincipalAccount`. Questa condizione richiede che il principale e la risorsa devono trovarsi nello stesso account.

Limitare l'accesso ai bucket Amazon S3 all'interno della propria unità organizzativa

Se hai un'unità [organizzativa \(OU\)](#) configurata AWS Organizations, potresti voler limitare l'accesso al bucket Amazon S3 a una parte specifica della tua organizzazione. In questo esempio, utilizziamo la chiave `aws:ResourceOrgPaths` per limitare l'accesso del bucket Amazon S3 a un'unità organizzativa della tua organizzazione. In questo esempio, l'[ID dell'unità organizzativa](#) è ***ou-acroot-exampleou***. Assicurati di sostituire questo valore nella tua policy con i tuoi ID dell'unità organizzativa.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3AccessOutsideMyBoundary",
      "Effect": "Allow",
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringLike": {
          "aws:ResourceOrgPaths": [
            "o-acorg/r-acroot/ou-acroot-exampleou/"
          ]
        }
      }
    }
  ]
}
```

```

    }
  ]
}
```

Note

Questa policy non garantisce alcun accesso. Questa policy funge invece da backstop per le altre autorizzazioni IAM, impedendo ai responsabili di accedere agli oggetti Amazon S3 al di fuori di un limite. OU-defined

La policy nega l'accesso alle azioni di Amazon S3 a meno che l'oggetto Amazon S3 a cui si accede non si trovi nell'OU *ou-acroot-example* nella tua organizzazione. La [Condizione di policy IAM](#) richiede `aws:ResourceOrgPaths`, una chiave di condizione multivalore, per contenere uno qualsiasi dei percorsi dell'unità organizzativa elencati. La politica utilizza l'operatore `ForAllValues:StringNotLike` per confrontare i valori di `aws:ResourceOrgPaths` alle OU elencate senza corrispondenza in base a maiuscole e minuscole.

Limitazione dell'accesso ai bucket Amazon S3 all'interno dell'organizzazione

Per limitare l'accesso agli oggetti Amazon S3 all'interno dell'organizzazione, allega una policy IAM alla radice dell'organizzazione, applicandola a tutti gli account dell'organizzazione. Per richiedere ai tuoi principale IAM di seguire questa regola, usa una [policy di controllo dei servizi \(SCP\)](#). Se scegli di utilizzare una SCP, assicurati di [testare l'SCP](#) prima di allegare la policy alla radice dell'organizzazione.

Nella seguente policy di esempio, l'accesso viene negato alle azioni di Amazon S3 a meno che l'oggetto Amazon S3 a cui si accede non si trovi nella stessa organizzazione del principale IAM che vi sta accedendo:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyS3AccessOutsideMyBoundary",
      "Effect": "Deny",
```

```

    "Action": [
      "s3:*"
    ],
    "Resource": "arn:aws:s3:::*/**",
    "Condition": {
      "StringNotEquals": {
        "aws:ResourceOrgID": "${aws:PrincipalOrgID}"
      }
    }
  }
]
}

```

Note

Questa policy non garantisce alcun accesso. Invece, questa policy funge da backstop per le altre autorizzazioni IAM, impedendo ai tuoi principali di accedere a qualsiasi oggetto Amazon S3 al di fuori della tua organizzazione. Questa policy si applica anche alle risorse Amazon S3 create dopo l'entrata in vigore della policy.

La [Condizione di policy IAM](#) in questo esempio richiede che `aws:ResourceOrgID` e `aws:PrincipalOrgID` siano uguali l'uno all'altro. Con questo requisito, il principale che effettua la richiesta e la risorsa a cui si accede devono trovarsi nella stessa organizzazione.

Concessione dell'autorizzazione per recuperare il `PublicAccessBlock` configurazione per un Account AWS

Il seguente esempio di policy basata sull'identità concede l'autorizzazione `s3:GetAccountPublicAccessBlock` a un utente. Per queste autorizzazioni, è necessario impostare il valore `Resource` su `"*"`. Per informazioni sugli ARN delle risorse, consulta [Risorse di policy per Amazon S3](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```
    "Sid": "statement1",
    "Effect": "Allow",
    "Action": [
        "s3:GetAccountPublicAccessBlock"
    ],
    "Resource": [
        "*"
    ]
  }
}
```

Limitare la creazione di bucket a una sola Regione

Supponiamo che un Account AWS amministratore voglia concedere al proprio utente (Dave) il permesso di creare un bucket solo nella regione del Sud America (San Paolo). L'amministratore dell'account può collegare la seguente policy utente assegnando l'autorizzazione `s3:CreateBucket` con una condizione, come mostrato. La coppia chiave-valore nel blocco `Condition` specifica la chiave `s3:LocationConstraint` e la regione `sa-east-1` come valore corrispondente.

Note

In questo esempio, il proprietario di bucket sta assegnando un'autorizzazione a uno dei suoi utenti, in modo da poter utilizzare una policy di bucket o una policy utente. Questo esempio mostra una policy utente.

Per un elenco delle regioni di Amazon S3, consultare la sezione relativa a [regioni ed endpoint](#) nella Riferimenti generali di AWS.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Action": "s3:CreateBucket",
      "Resource": "arn:aws:s3:::",

```

```

    "Condition": {
      "StringLike": {
        "s3:LocationConstraint": "sa-east-1"
      }
    }
  ]
}

```

Aggiunta del rifiuto esplicito

La policy precedente limita l'utente impedendogli di creare un bucket in qualsiasi altra regione al di fuori di sa-east-1. Tuttavia, qualche altra policy potrebbe assegnare a questo utente l'autorizzazione a creare bucket in un'altra regione. Ad esempio, se l'utente appartiene a un gruppo, è possibile che questo gruppo abbia una policy collegata che assegna a tutti gli utenti del gruppo stesso l'autorizzazione a creare bucket in un'altra regione. Per assicurarsi che l'utente non ottenga il permesso di creare bucket in qualsiasi altra Regione, è possibile aggiungere un'istruzione esplicita di rifiuto nella policy di cui sopra.

L'istruzione Deny utilizza la condizione StringNotLike. Cioè, la richiesta di creazione del bucket viene rifiutata se il vincolo di posizione non è sa-east-1. La negazione esplicita non consente all'utente di creare un bucket in nessun'altra Regione, indipendentemente dalle altre autorizzazioni ottenute dall'utente. La seguente policy include un'istruzione esplicita di rifiuto.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Action": "s3:CreateBucket",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringLike": {
          "s3:LocationConstraint": "sa-east-1"
        }
      }
    }
  ],
}

```

```
{
  "Sid": "statement2",
  "Effect": "Deny",
  "Action": "s3:CreateBucket",
  "Resource": "arn:aws:s3:::*",
  "Condition": {
    "StringNotLike": {
      "s3:LocationConstraint": "sa-east-1"
    }
  }
}
```

Verifica la politica con AWS CLI

È possibile testare la politica utilizzando il seguente `create-bucket` AWS CLI comando. Questo esempio utilizza il file `bucketconfig.txt` per specificare il vincolo di posizione. Si noti il percorso del file Windows. È necessario aggiornare il nome del bucket e il percorso come opportuno. È necessario fornire le credenziali utente utilizzando il parametro `--profile`. Per ulteriori informazioni sulla configurazione e l'utilizzo di AWS CLI, consulta [Developing with Amazon S3 using the AWS CLI](#) in [Amazon S3 API Reference](#).

```
aws s3api create-bucket --bucket examplebucket --profile AccountADave --create-bucket-configuration file://c:/Users/someUser/bucketconfig.txt
```

Il file `bucketconfig.txt` specifica la configurazione come segue:

```
{"LocationConstraint": "sa-east-1"}
```

Passaggi che utilizzano le policy per gestire l'accesso alle risorse Amazon S3

Questo argomento contiene i seguenti esempi di procedure guidate introduttive per concedere l'accesso alle risorse di Amazon S3. Questi esempi utilizzano il Console di gestione AWS per creare risorse (bucket, oggetti, utenti) e concedere loro autorizzazioni. Gli esempi mostrano quindi come verificare le autorizzazioni utilizzando gli strumenti a riga di comando per evitare di scrivere il codice. Forniamo comandi utilizzando sia AWS Command Line Interface (AWS CLI) che AWS Tools for Windows PowerShell.

- [Esempio 1: il proprietario del bucket concede agli utenti le autorizzazioni per il bucket](#)

Per default, gli utenti IAM creati nell'account non dispongono delle autorizzazioni. In questo esercizio agli utenti verrà concessa un'autorizzazione per eseguire le operazioni sui bucket e sugli oggetti.

- [Esempio 2: il proprietario del bucket concede autorizzazioni per il bucket multiaccount](#)

In questo esercizio un proprietario del bucket, Account A, concede le autorizzazioni multiaccount a un altro Account AWS, Account B, che delega quindi queste autorizzazioni agli utenti nel suo account.

- Gestione delle autorizzazioni per l'oggetto quando il proprietario dell'oggetto non corrisponde al proprietario del bucket

Gli scenari di esempio in questo caso riguardano un proprietario del bucket che concede ad altri le autorizzazioni per l'oggetto, sebbene non tutti gli oggetti nel bucket siano di sua proprietà. Di quali autorizzazioni ha bisogno il proprietario del bucket e come può delegare tali autorizzazioni?

Chi Account AWS crea un bucket si chiama proprietario del bucket. Il proprietario può concedere altre Account AWS autorizzazioni per caricare oggetti e chi crea oggetti Account AWS ne è il proprietario. Il proprietario del bucket non dispone delle autorizzazioni per gli oggetti creati dagli altri Account AWS. Se il proprietario del bucket scrive una policy del bucket che concede l'accesso agli oggetti, la policy non si applica agli oggetti di proprietà di altri account.

In questo caso il proprietario dell'oggetto deve in primo luogo concedere le autorizzazioni al proprietario del bucket utilizzando un'ACL dell'oggetto. Il proprietario del bucket può quindi delegare tali autorizzazioni per gli oggetti ad altri, agli utenti del proprio account o a un altro Account AWS, come illustrato negli esempi seguenti.

- [Esempio 3: il proprietario del bucket concede autorizzazioni per gli oggetti che non sono di sua proprietà](#)

In questo esercizio il proprietario del bucket ottiene prima le autorizzazioni dal proprietario dell'oggetto, il proprietario del bucket quindi delega queste autorizzazioni agli utenti nel suo account.

- [Esempio 4 - Proprietario di un bucket che concede un'autorizzazione multi-account agli oggetti di cui non è proprietario](#)

Dopo aver ricevuto le autorizzazioni dal proprietario dell'oggetto, il proprietario del bucket non può delegare l'autorizzazione ad altri Account AWS perché la delega tra account non è supportata (vedi). [Delega delle autorizzazioni](#) Invece, il proprietario del bucket può creare un ruolo IAM con le autorizzazioni per eseguire operazioni specifiche (come get object) e consentire a un altro di assumere quel ruolo. Account AWS Chiunque assuma il ruolo potrà quindi accedere agli oggetti. Questo esempio mostra in che modo un proprietario del bucket può utilizzare un ruolo IAM per abilitare questa delega multiaccount.

Prima di provare le procedure guidate di esempio

Questi esempi utilizzano il Console di gestione AWS per creare risorse e concedere autorizzazioni. Per testare le autorizzazioni, gli esempi utilizzano gli strumenti della riga di comando e AWS CLI AWS Tools for Windows PowerShell, quindi non è necessario scrivere alcun codice. Per testare le autorizzazioni, è necessario configurare uno di questi strumenti. Per ulteriori informazioni, consulta [Impostazione degli strumenti per le visite guidate](#).

Inoltre, quando si creano le risorse, questi esempi non utilizzano le credenziali dell'utente root di Account AWS. ma viene creato un utente amministratore in questi account per eseguire queste attività.

Informazioni sull'uso di un utente amministratore per creare risorse e concedere autorizzazioni

AWS Identity and Access Management (IAM) sconsiglia di utilizzare le credenziali dell'utente root dell'Account AWS per effettuare richieste. Invece, crea un utente o un ruolo IAM, concedi a tale utente o ruolo l'accesso completo, quindi utilizza le relative credenziali per fare richieste. Questo utente viene definito utente o ruolo amministratore. Per ulteriori informazioni, consultare la sezione relativa a [credenziali Utente root dell'account AWS e identità IAM](#) nella Riferimenti generali di AWS e [Best practice di IAM](#) nella Guida per l'utente di IAM.

In tutte le procedure guidate di esempio riportate in questa sezione vengono utilizzate le credenziali dell'utente amministratore. Se non hai creato un utente amministratore per il tuo Account AWS, negli argomenti viene illustrato come fare.

Per accedere Console di gestione AWS utilizzando le credenziali utente, è necessario utilizzare l'URL di accesso utente IAM. La [console IAM](#) fornisce questo URL per l' Account AWS. Negli argomenti di questa sezione viene illustrato come ottenere l'URL.

Impostazione degli strumenti per le visite guidate

Gli esempi introduttivi (vedi [Passaggi che utilizzano le policy per gestire l'accesso alle risorse Amazon S3](#)) utilizzano il Console di gestione AWS per creare risorse e concedere autorizzazioni. Per testare le autorizzazioni, gli esempi utilizzano gli strumenti da riga di comando, AWS Command Line Interface (AWS CLI) e AWS Tools for Windows PowerShell, quindi non è necessario scrivere alcun codice. Per testare le autorizzazioni, è necessario configurare uno di questi strumenti.

Per configurare AWS CLI

1. Scarica e configura la AWS CLI. Per le istruzioni, consulta i seguenti argomenti nella Guida per l'utente dell'AWS Command Line Interface :

[Installare o aggiornare alla versione più recente del programma AWS Command Line Interface](#)

[Nozioni di base su AWS Command Line Interface](#)

2. Impostare il profilo di default.

Le credenziali utente vengono memorizzate nel file di AWS CLI configurazione. Crea un profilo predefinito nel file di configurazione utilizzando le tue credenziali. Account AWS Per istruzioni su come trovare e modificare il file di AWS CLI configurazione, consulta Impostazioni dei file di [configurazione e credenziali](#).

```
[default]
aws_access_key_id = access key ID
aws_secret_access_key = secret access key
region = us-west-2
```

3. Verificare la configurazione digitando i comandi riportati di seguito al prompt dei comandi. Poiché entrambi questi comandi non forniscono credenziali in modo esplicito, vengono utilizzate le credenziali del profilo di default.

- Prova il comando `help`.

```
aws help
```

- Per ottenere un elenco dei bucket sull'account configurato, utilizza il comando `aws s3 ls`.

```
aws s3 ls
```

Man mano che si procede, si creano utenti e si salvano le credenziali degli utenti nei file di configurazione creando profili, come mostra l'esempio seguente. Questi profili hanno i nomi di `AccountAadmin` e `AccountBadmin`.

```
[profile AccountAadmin]
aws_access_key_id = User AccountAadmin access key ID
aws_secret_access_key = User AccountAadmin secret access key
region = us-west-2

[profile AccountBadmin]
aws_access_key_id = Account B access key ID
aws_secret_access_key = Account B secret access key
region = us-east-1
```

Per eseguire un comando utilizzando queste credenziali utente, aggiungere il parametro `--profile` specificando il nome del profilo. Il AWS CLI comando seguente recupera un elenco di oggetti in *examplebucket* e specifica il profilo. `AccountBadmin`

```
aws s3 ls s3://examplebucket --profile AccountBadmin
```

In alternativa, è possibile configurare un set di credenziali utente come profilo di default modificando la variabile di ambiente `AWS_DEFAULT_PROFILE` dal prompt dei comandi. Dopo averlo fatto, ogni volta che AWS CLI esegui comandi senza il `--profile` parametro, AWS CLI utilizza il profilo impostato nella variabile di ambiente come profilo predefinito.

```
$ export AWS_DEFAULT_PROFILE=AccountAadmin
```

Per configurare AWS Tools for Windows PowerShell

1. Scarica e configura la AWS Tools for Windows PowerShell. Per le istruzioni, consulta la sezione [Installazione di AWS Tools for Windows PowerShell](#) nella Guida all'utente AWS Strumenti per PowerShell .

Note

Per caricare il AWS Tools for Windows PowerShell modulo, è necessario abilitare l'esecuzione PowerShell dello script. Per ulteriori informazioni, consulta [Abilita l'esecuzione di script](#) nella Guida all'utente AWS Strumenti per PowerShell .

2. Per queste procedure dettagliate, si specificano AWS le credenziali per sessione utilizzando il comando. Set-AWSCredentials Il comando salva le credenziali in uno store permanente (parametro -StoreAs).

```
Set-AWSCredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -  
storeas string
```

3. Verificare la configurazione.

- Per ottenere un elenco dei comandi disponibili che si possono utilizzare per le operazioni su Amazon S3, esegui il comando Get-Command.

```
Get-Command -module awspowershell -noun s3* -StoredCredentials string
```

- Per recuperare un elenco di oggetti in un bucket, esegui il comando Get-S3Object.

```
Get-S3Object -BucketName bucketname -StoredCredentials string
```

Per un elenco dei comandi, vedere [AWS Tools for PowerShell Cmdlet Reference](#).

Ora sei pronto a provare le guide. Segui i link forniti all'inizio di ogni sezione.

Esempio 1: il proprietario del bucket concede agli utenti le autorizzazioni per il bucket

⚠ Important

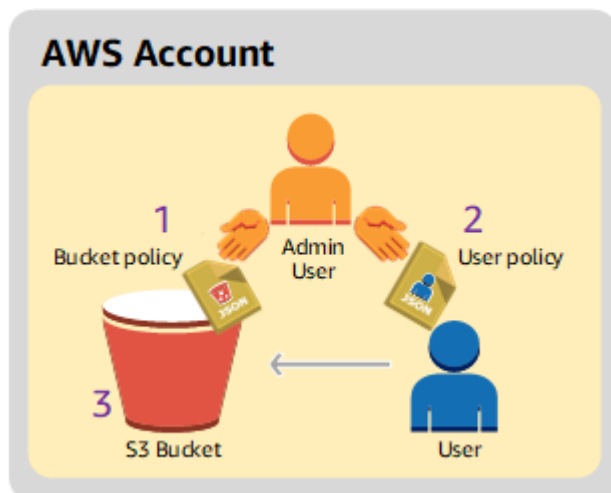
La concessione di autorizzazioni ai ruoli IAM è una pratica migliore rispetto alla concessione di autorizzazioni ai singoli utenti. Per ulteriori informazioni su come concedere autorizzazioni ai ruoli IAM, consulta [Comprendere le autorizzazioni multi-account e utilizzare i ruoli IAM](#).

Argomenti

- [Preparazione della spiegazione passo per passo](#)
- [Fase 1: Creare risorse nell'account A e concedere le autorizzazioni](#)
- [Fase 2: testare le autorizzazioni](#)

In questa procedura dettagliata, un Account AWS possiede un bucket e l'account include un utente IAM. Per impostazione predefinita, l'utente non dispone di autorizzazioni. Per eseguire qualsiasi attività, l'account padre deve concedere le autorizzazioni all'utente. Il proprietario del bucket e l'account padre sono uguali. Pertanto, per concedere all'utente le autorizzazioni sul bucket, Account AWS può utilizzare una bucket policy, una user policy o entrambe. Il proprietario dell'account concederà alcune autorizzazioni con una policy del bucket e altre con una policy utente.

La seguenti fasi riepilogano la procedura guidata:



1. L'amministratore dell'account crea una policy bucket per concedere un set di autorizzazioni all'utente.

2. L'amministratore dell'account collega una policy utente all'utente per concedere ulteriori autorizzazioni.
3. L'utente prova quindi le autorizzazioni concesse tramite la politica del bucket e la politica utente.

Per questo esempio, avrai bisogno di un Account AWS. Aniché utilizzare le credenziali dell'utente root dell'account, sarà necessario creare un utente amministratore (consultare [Informazioni sull'uso di un utente amministratore per creare risorse e concedere autorizzazioni](#)). Ci riferiamo all'utente Account AWS e all'amministratore come illustrato nella tabella seguente.

ID account	Account denominato	Utente amministratore nell'account
1111-1111-1111	Account A	AccountAdmin

 Note

L'utente amministratore in questo esempio è AccountAdmin, che si riferisce all'Account A, e non AccountAdmin.

Tutte le attività di creazione degli utenti e assegnazione delle autorizzazioni vengono effettuate nella Console di gestione AWS. Per verificare le autorizzazioni, la procedura dettagliata utilizza gli strumenti della riga di comando, AWS Command Line Interface (AWS CLI) e AWS Tools for Windows PowerShell, quindi non è necessario scrivere alcun codice.

Preparazione della spiegazione passo per passo

1. Assicurati di avere un Account AWS e che abbia un utente con privilegi di amministratore.
 - a. Registrati per un Account AWS, se necessario. Si fa riferimento a questo account come Account A.
 - i. Vai a <https://aws.amazon.com/s3> e scegli Crea un AWS account.
 - ii. Seguire le istruzioni su schermo.

AWS ti avviserà via e-mail quando il tuo account sarà attivo e disponibile per l'uso.

- b. Nell'account A, crea un utente amministratore **AccountAdmin**. Utilizzando le credenziali dell'Account A, accedere alla [console IAM](#) ed effettuare quanto segue:

- i. Crea l'utente **AccountAdmin** e annota le credenziali di sicurezza dell'utente.

Per istruzioni, consulta [Creazione di un utente IAM in Account AWS](#) nella Guida all'utente IAM.

- ii. Concedi i privilegi di amministratore **AccountAdmin** allegando una politica utente che consente l'accesso completo.

Per istruzioni, consulta [Gestione delle policy IAM](#) nella Guida all'utente IAM.

- iii. Nota l' Sign-In URL utente IAM per **AccountAdmin** che dovrà essere utilizzato per accedere alla Console di gestione AWS. Per ulteriori informazioni su dove trovare l'URL di accesso, consulta [Accedi Console di gestione AWS come utente IAM nella IAM User Guide](#). Annota l'URL di ciascun account.

2. Configura il AWS CLI o il AWS Tools for Windows PowerShell Assicurati di salvare le credenziali dell'utente amministratore come segue:

- Se si utilizza il AWS CLI, crea un profilo **AccountAdmin**, nel file di configurazione.
- Se usi il AWS Tools for Windows PowerShell, assicurati di memorizzare le credenziali per la sessione come **AccountAdmin**

Per istruzioni, consulta l'argomento [Impostazione degli strumenti per le visite guidate](#).

Fase 1: Creare risorse nell'account A e concedere le autorizzazioni

Utilizzando le credenziali dell'utente **AccountAdmin** nell'Account A e lo speciale URL di accesso dell'utente IAM, accedi a Console di gestione AWS ed esegui quanto segue:

1. Creare risorse di un bucket e di un utente IAM

- a. Nella console di Amazon S3 creare un bucket. Annota il codice Regione AWS in cui hai creato il bucket. Per istruzioni, consulta l'argomento [Creazione di un bucket per uso generico](#).
 - b. Nella [Console IAM](#), procedi come segue:
 - i. Crea un utente di nome Dave.

Per istruzioni dettagliate, consulta [Creazione di utenti IAM \(console\)](#) nella Guida all'utente IAM.

- ii. Annota le credenziali UserDave.
- iii. Annota il nome della risorsa Amazon (ARN) per l'utente Dave. Nella [Console IAM](#), seleziona l'utente e la scheda Riepilogo fornisce l'ARN dell'utente.

2. Concedi i permessi.

Poiché il proprietario del bucket e l'account principale a cui appartiene l'utente sono gli stessi, Account AWS può concedere le autorizzazioni utente utilizzando una policy del bucket, una policy utente o entrambe, come in questo esempio. Se l'oggetto è anche di proprietà dello stesso account, il proprietario del bucket può concedere le autorizzazioni per l'oggetto nella policy bucket (o una policy IAM).

- a. Nella console Amazon S3, allega la seguente policy del bucket a *awsexamplebucket1*

La policy include due dichiarazioni.

- La prima istruzione concede a Dave le autorizzazioni per le operazioni sul bucket `s3:GetBucketLocation` e `s3:ListBucket`.
- La seconda istruzione concede l'autorizzazione `s3:GetObject`. Poiché l'Account A è anche proprietario dell'oggetto, l'amministratore dell'account può concedere l'autorizzazione `s3:GetObject`.

Nell'istruzione `Principal` Dave è identificato dall'ARN utente. Per ulteriori informazioni sugli elementi delle policy, consultare [Policy e autorizzazioni in Amazon S3](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Dave"
      },
    },
  ],
}
```

```

        "Action": [
            "s3:GetBucketLocation",
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::awsexamplebucket1"
        ]
    },
    {
        "Sid": "statement2",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:user/Dave"
        },
        "Action": [
            "s3:GetObject"
        ],
        "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*"
        ]
    }
]
}

```

- b. Creare una policy inline per l'utente Dave mediante la policy che segue. La policy concede a Dave l'autorizzazione `s3:PutObject`. È necessario aggiornare la policy specificando il nome del bucket.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PermissionForObjectOperations",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::awsexamplebucket1/*"
      ]
    }
  ]
}

```



```
}  
]  
}
```

Per istruzioni, consulta [Gestione delle policy IAM](#) nella Guida all'utente IAM. Tenere presente che è necessario accedere alla console tramite le credenziali dell'Account A.

Fase 2: testare le autorizzazioni

Utilizzando le credenziali di Dave, verificare che le autorizzazioni funzionino correttamente. È possibile utilizzare una delle due procedure di seguito.

Verifica le autorizzazioni utilizzando il AWS CLI

1. Aggiorna il file di AWS CLI configurazione aggiungendo il seguente UserDaveAccountA profilo. Per ulteriori informazioni, consulta [Impostazione degli strumenti per le visite guidate](#).

```
[profile UserDaveAccountA]  
aws_access_key_id = access-key  
aws_secret_access_key = secret-access-key  
region = us-east-1
```

2. Verificare che Dave possa eseguire le operazioni autorizzate nella policy utente. Carica un oggetto di esempio utilizzando il seguente AWS CLI put-object comando.

Il parametro `--body` nel comando identifica il file di origine da caricare. Ad esempio, se il file si trova nella radice dell'unità C: su un computer Windows, si specifica `c:\HappyFace.jpg`. Il parametro `--key` fornisce il nome della chiave dell'oggetto.

```
aws s3api put-object --bucket awsexamplebucket1 --key HappyFace.jpg --  
body HappyFace.jpg --profile UserDaveAccountA
```

Eseguite il AWS CLI comando seguente per ottenere l'oggetto.

```
aws s3api get-object --bucket awsexamplebucket1 --key HappyFace.jpg OutputFile.jpg  
--profile UserDaveAccountA
```

Verifica le autorizzazioni utilizzando il AWS Tools for Windows PowerShell

1. Memorizza le credenziali di Dave come AccountADave. Si utilizzano quindi queste credenziali per PUT e GET un oggetto.

```
set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas AccountADave
```

2. Carica un oggetto di esempio utilizzando il AWS Tools for Windows PowerShell Write-S3Object comando utilizzando le credenziali archiviate dell'utente Dave.

```
Write-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file HappyFace.jpg -StoredCredentials AccountADave
```

Scaricare l'oggetto caricato in precedenza.

```
Read-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file Output.jpg -StoredCredentials AccountADave
```

Esempio 2: il proprietario del bucket concede autorizzazioni per il bucket multiaccount

Important

Concedere le autorizzazioni ai ruoli IAM è una pratica migliore rispetto alla concessione delle autorizzazioni ai singoli utenti. Per informazioni su come effettuare questa operazione, consulta [Comprendere le autorizzazioni multi-account e utilizzare i ruoli IAM](#).

Argomenti

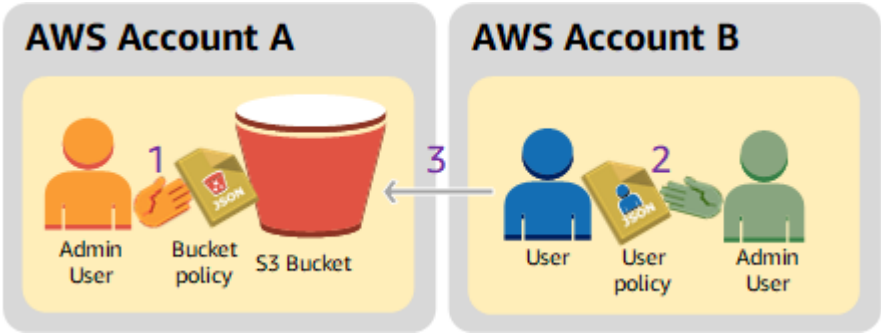
- [Preparazione della spiegazione passo per passo](#)
- [Fase 1: esecuzione delle attività per l'Account A](#)
- [Fase 2: esecuzione delle attività per l'Account B](#)
- [Fase 3: \(facoltativo\) provare un rifiuto esplicito](#)
- [Fase 4: pulizia](#)

Un account, ad Account AWS esempio, può concedere a un altro Account AWS, account B, il permesso di accedere alle sue risorse come bucket e oggetti. L'Account B può quindi delegare queste autorizzazioni agli utenti nel proprio account. In questo scenario di esempio, il proprietario del bucket concede a un altro account le autorizzazioni multiaccount per eseguire specifiche operazioni nel bucket.

Note

L'account A può inoltre concedere le autorizzazioni a un utente dell'Account B mediante una policy di bucket. Tuttavia, l'utente avrà comunque bisogno dell'autorizzazione dell'account padre, l'account B, a cui appartiene, anche se l'account B non ha le autorizzazioni dell'account A. Finché l'utente ha l'autorizzazione sia del proprietario della risorsa che dell'account padre, potrà accedere alla risorsa.

Di seguito è riportato un riepilogo delle fasi della procedura:



1. L'amministratore dell'Account A collega una policy di bucket che concede all'Account B autorizzazioni multiaccount per l'esecuzione di specifiche operazioni nel bucket.

L'utente amministratore dell'Account B erediterà automaticamente le autorizzazioni.

2. L'utente amministratore dell'account B collega una policy utente all'utente per delegare le autorizzazioni ricevute dall'Account A.

3. L'utente dell'Account B fa quindi una verifica delle autorizzazioni accedendo a un oggetto nel bucket di proprietà dell'Account A.

Per questo utente, sono necessari due account. La tabella seguente mostra come viene fatto riferimento a questi account e ai relativi utenti amministratori. In conformità alle linee guida IAM (consulta [Informazioni sull'uso di un utente amministratore per creare risorse e concedere autorizzazioni](#)), in questa guida non utilizzeremo le credenziali dell'utente root. Viene invece creato un utente amministratore in ciascun account e le credenziali vengono utilizzate per la creazione di risorse e per concedere autorizzazioni a tali risorse.

Account AWS ID	Account denominato	Utente amministratore nell'account
1111-1111-1111	Account A	AccountAdmin
2222-2222-2222	Account B	AccountBAdmin

Tutte le attività di creazione degli utenti e assegnazione delle autorizzazioni vengono effettuate nella Console di gestione AWS. Per verificare le autorizzazioni, la procedura dettagliata utilizza gli strumenti a riga di comando AWS Command Line Interface (CLI) e AWS Tools for Windows PowerShell, quindi, non è necessario scrivere alcun codice.

Preparazione della spiegazione passo per passo

1. Assicurati di averne due Account AWS e che ogni account abbia un utente amministratore, come mostrato nella tabella nella sezione precedente.
 - a. Registrati per un Account AWS, se necessario.
 - b. Utilizzando le credenziali dell'Account A, accedere alla [console IAM](#) per creare l'utente amministratore:
 - i. Crea l'utente **AccountAdmin** e annota le credenziali di sicurezza. Per istruzioni, consulta [Creazione di un utente IAM nell' Account AWS](#) nella Guida per l'utente di IAM.
 - ii. Concedi i privilegi di amministratore a **AccountAdmin** allegando una politica utente che consente l'accesso completo. Per istruzioni, consulta [Gestione di policy IAM](#) nella Guida per l'utente di IAM.
 - c. Mentre sei nella console IAM, annota l'Sign-In URL dell'utente IAM nella dashboard. Tutti gli utenti dell'account devono utilizzare questo URL per accedere alla Console di gestione AWS.

Per ulteriori informazioni, consulta [In che modo gli utenti effettuano l'accesso al tuo account](#) nella Guida per l'utente IAM.

- d. Ripeti il passaggio precedente utilizzando le credenziali dell'account B e creare l'utente amministratore **AccountBadmin**.
2. Configura AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell. Assicurati di salvare le credenziali dell'utente amministratore come segue:
 - Se si utilizza il AWS CLI, crea due profili **AccountAdmin** e **AccountBadmin**, nel file di configurazione.
 - Se usi il AWS Tools for Windows PowerShell, assicurati di memorizzare le credenziali per la sessione come **eAccountAdmin**. **AccountBadmin**

Per istruzioni, consulta l'argomento [Impostazione degli strumenti per le visite guidate](#).

3. Salvare le credenziali dell'utente amministratore, chiamate anche profili. È possibile utilizzare il nome del profilo anziché specificare le credenziali per ciascun comando immesso. Per ulteriori informazioni, consulta [Impostazione degli strumenti per le visite guidate](#).
 - a. Aggiungi i profili nel file delle AWS CLI credenziali per ciascuno degli utenti amministratori **AccountAdmin** e **AccountBadmin** nei due account.

```
[AccountAadmin]
aws_access_key_id = access-key-ID
aws_secret_access_key = secret-access-key
region = us-east-1

[AccountBadmin]
aws_access_key_id = access-key-ID
aws_secret_access_key = secret-access-key
region = us-east-1
```

- b. Se si utilizza AWS Tools for Windows PowerShell, esegui il seguente comando.

```
set-awscredentials -AccessKey AcctA-access-key-ID -SecretKey AcctA-secret-access-key -storeas AccountAadmin
set-awscredentials -AccessKey AcctB-access-key-ID -SecretKey AcctB-secret-access-key -storeas AccountBadmin
```

Fase 1: esecuzione delle attività per l'Account A

Passaggio 1.1: Accedi a Console di gestione AWS

Utilizzando l'URL di accesso dell'utente IAM per l'account A, accedi prima all'AccountAadminutente Console di gestione AWS come utente. Questo utente creerà un bucket e vi allegnerà una policy.

Fase 1.2: creazione di un bucket

1. Nella console di Amazon S3 creare un bucket. Questo esercizio presuppone che il bucket sia stato creato negli Stati Uniti orientali (Virginia settentrionale) Regione AWS e abbia un nome. *amzn-s3-demo-bucket*

Per istruzioni, consulta l'argomento [Creazione di un bucket per uso generico](#).

2. Caricare un oggetto campione nel bucket.

Per istruzioni, vai su [Fase 2: Carica un oggetto nel tuo bucket](#).

Fase 1.3: collegare una policy del bucket per concedere autorizzazioni tra account all'Account B

La policy del bucket concede le `s3:ListBucket` autorizzazioni `s3:GetLifecycleConfiguration` and all'Account B. Si presume che tu abbia ancora effettuato l'accesso alla console utilizzando le credenziali utente. AccountAdmin

1. Collegare la seguente policy di bucket a *amzn-s3-demo-bucket*. La policy concede all'Account B autorizzazioni per le operazioni `s3:GetLifecycleConfiguration` e `s3:ListBucket`.

Per istruzioni, consulta l'argomento [Aggiunta di una policy di bucket utilizzando la console di Amazon S3](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Example permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}
```

2. Verifica che l'account B (e quindi il suo utente amministratore) possa eseguire le operazioni.
 - Verifica utilizzando il AWS CLI

```
aws s3 ls s3://amzn-s3-demo-bucket --profile AccountAdmin
aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --
profile AccountAdmin
```

- Verifica utilizzando il AWS Tools for Windows PowerShell

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBadmin  
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -  
StoredCredentials AccountBadmin
```

Fase 2: esecuzione delle attività per l'Account B

A questo punto l'amministratore dell'Account B crea un utente, Dave, al quale delega le autorizzazioni ricevute dall'Account A.

Passaggio 2.1: Accedi a Console di gestione AWS

Utilizzando l'URL di accesso dell'utente IAM per l'account B, accedi prima a Console di gestione AWS come AccountBadmin utente.

Fase 2.2: creazione dell'utente Dave nell'Account B

Nella [console IAM](#), crea un utente, **Dave**.

Per le istruzioni, consulta [Creazione di utenti IAM \(console\)](#) nella Guida per l'utente di IAM.

Fase 2.3: delega delle autorizzazioni all'utente Dave

Creare una policy inline per l'utente Dave mediante la policy che segue. Sarà necessario aggiornare la policy specificando il nome del bucket.

Si presume che tu abbia effettuato l'accesso alla console utilizzando le credenziali AccountBadmin utente.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "Example",  
      "Effect": "Allow",  
      "Action": [  

```



```
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}
```

Per istruzioni, consulta [Gestione delle policy IAM](#) nella Guida all'utente IAM.

Fase 2.4: testare le autorizzazioni

Ora l'utente Dave dell'Account B può elencare il contenuto di *amzn-s3-demo-bucket* di proprietà dell'Account A. È possibile verificare le autorizzazioni mediante una delle procedure descritte di seguito.

Verifica le autorizzazioni utilizzando il AWS CLI

1. Aggiungi il UserDave profilo al file di AWS CLI configurazione. Per ulteriori informazioni sul file di configurazione, consulta [Impostazione degli strumenti per le visite guidate](#).

```
[profile UserDave]
aws_access_key_id = access-key
aws_secret_access_key = secret-access-key
region = us-east-1
```

2. Al prompt dei comandi, immetti il seguente AWS CLI comando per verificare che Dave possa ora ottenere un elenco di oggetti dall'*amzn-s3-demo-bucket* account A. Nota che il comando specifica il profilo. UserDave

```
aws s3 ls s3://amzn-s3-demo-bucket --profile UserDave
```

Dave non ha altri permessi. Quindi, se si tenta qualsiasi altra operazione, ad esempio la seguente configurazione `get-bucket-lifecycle`, Amazon S3 restituisce l'autorizzazione negata.

```
aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --profile UserDave
```

Verifica le autorizzazioni utilizzando AWS Tools for Windows PowerShell

1. Memorizza le credenziali di Dave come AccountBDave.

```
set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas AccountBDave
```

2. Provare a utilizzare il comando List Bucket.

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
```

Dave non ha altri permessi. Quindi, se si tenta un'altra operazione, ad esempio la seguente `get-s3bucketlifecycleconfiguration`-Amazon S3 restituisce Autorizzazione negata.

```
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -  
StoredCredentials AccountBDave
```

Fase 3: (facoltativo) provare un rifiuto esplicito

Le autorizzazioni possono essere concesse utilizzando una lista di controllo degli accessi (ACL), una policy di bucket o una policy utente. Tuttavia, se c'è un rifiuto esplicito impostato da una policy del bucket o da una policy dell'utente, il rifiuto esplicito ha la precedenza su qualsiasi altra autorizzazione. Per i test, aggiornare la policy del bucket e negare esplicitamente all'account B l'autorizzazione `s3:ListBucket`. La policy concede anche il permesso di `s3:ListBucket`. Tuttavia, il rifiuto esplicito ha la precedenza e l'account B o gli utenti dell'account B non potranno elencare gli oggetti in *amzn-s3-demo-bucket*.

1. Utilizzando le credenziali dell'utente AccountAadmin nell'account A, sostituisci la policy del bucket con il seguente.
2. Ora, se si cerca di ottenere un elenco di bucket utilizzando le credenziali di AccountBadmin, l'accesso viene negato.
 - Usando AWS CLI, esegui il seguente comando:

```
aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
```

- Usando AWS Tools for Windows PowerShell, esegui il seguente comando:

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
```

Fase 4: pulizia

1. Una volta terminato il test, è possibile eseguire le seguenti operazioni di pulizia:
 - Accedi a Console di gestione AWS ([Console di gestione AWS](#)) utilizzando le credenziali dell'Account A ed esegui le seguenti operazioni:
 - Nella console di Amazon S3 rimuovere la policy del bucket collegata a *amzn-s3-demo-bucket*. Nelle Proprietà del bucket, elimina la policy nella sezione Autorizzazioni.
 - Se il bucket è stato creato per questo esercizio, nella console di Amazon S3 eliminare gli oggetti e quindi il bucket.
 - Nella [Console IAM](#), rimuovi l'utente AccountAdmin.
2. Accedi alla [Console IAM](#) utilizzando le credenziali dell'Account B. Cancella l'utente AccountBadmin. Per istruzioni dettagliate, consulta [Eliminazione di un utente IAM](#) nella Guida all'utente IAM.

Esempio 3: il proprietario del bucket concede autorizzazioni per gli oggetti che non sono di sua proprietà

Important

Concedere le autorizzazioni ai ruoli IAM è una pratica migliore rispetto alla concessione delle autorizzazioni ai singoli utenti. Per informazioni su come effettuare questa operazione, consulta [Comprendere le autorizzazioni multi-account e utilizzare i ruoli IAM](#).

Argomenti

- [Fase 0: preparazione della procedura guidata](#)
- [Fase 1: esecuzione delle attività per l'Account A](#)
- [Fase 2: esecuzione delle attività per l'Account B](#)
- [Fase 3: testare le autorizzazioni](#)
- [Fase 4: pulizia](#)

Lo scenario di questo esempio è che il proprietario di un bucket voglia concedere il permesso di accedere agli oggetti, ma il proprietario del bucket non possiede tutti gli oggetti del bucket. In questo esempio, il proprietario del bucket tenta di concedere autorizzazioni agli utenti nel proprio account.

Il proprietario di un bucket può consentire ad altri Account AWS di caricare oggetti. Per impostazione predefinita, il proprietario del bucket non possiede oggetti scritti su un bucket da un altro Account AWS. Gli oggetti sono di proprietà degli account che li scrivono in un bucket S3. Se il proprietario del bucket non possiede oggetti nel bucket, il proprietario dell'oggetto deve prima concedere l'autorizzazione al proprietario del bucket utilizzando una lista di controllo degli accessi (ACL) dell'oggetto. Quindi, il proprietario del bucket può concedere i permessi a un oggetto di cui non è proprietario. Per ulteriori informazioni, consulta [Proprietà di bucket e oggetti di Amazon S3](#).

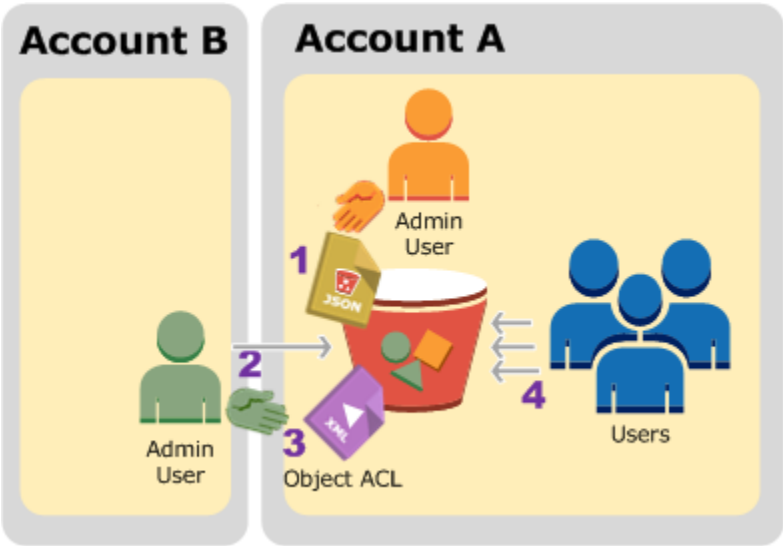
Se il proprietario del bucket esegue l'impostazione proprietario del bucket applicato per S3 Object Ownership per il bucket, il proprietario del bucket possiederà tutti gli oggetti nel bucket, inclusi gli oggetti scritti da un altro Account AWS. Questo approccio risolve il problema degli oggetti che non sono di proprietà del proprietario del bucket. Quindi, puoi delegare le autorizzazioni agli utenti nel tuo account o ad altri Account AWS.

Note

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le liste di controllo degli accessi (ACL) sono disabilite. Quando le ACL sono disabilite, il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ad essi in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilite, tranne nelle circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Con le ACL disabilite, puoi utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

In questo esempio supponiamo che il proprietario del bucket non abbia applicato l'impostazione proprietario del bucket applicato per Object Ownership. Il proprietario del bucket delega queste autorizzazioni agli utenti nel suo account. Di seguito è riportato un riepilogo delle fasi della procedura:



1. L'utente amministratore dell'Account A collega una policy di bucket con due istruzioni.
- Concedere all'Account B autorizzazioni multiaccount per caricare oggetti.
 - Consentire a un utente nel proprio account di accedere agli oggetti nel bucket.
2. L'utente amministratore dell'account B carica gli oggetti nel bucket di proprietà dell'Account A.
3. L'amministratore dell'Account B aggiorna l'ACL dell'oggetto e concede al proprietario del bucket l'autorizzazione al controllo completo sull'oggetto.
4. L'utente dell'Account A fa una verifica accedendo agli oggetti nel bucket, indipendentemente da chi ne ha la proprietà.

Per questo utente, sono necessari due account. La tabella seguente mostra come viene fatto riferimento a questi account e agli utenti amministratori degli account: In questa spiegazione passo per passo, non si utilizzano le credenziali dell'utente root dell'account, in base a quanto riportato nelle linee guida IAM consigliate. Per ulteriori informazioni, consulta [Informazioni sull'uso di un utente amministratore per creare risorse e concedere autorizzazioni](#). Viene invece creato un utente amministratore in ciascun account e le credenziali vengono utilizzate per la creazione di risorse e per concedere autorizzazioni a tali risorse

Account AWS ID	Account denominato	Amministratore nell'account
1111-1111-1111	Account A	AccountAdmin
2222-2222-2222	Account B	AccountBadmin

Tutte le attività di creazione degli utenti e assegnazione delle autorizzazioni vengono effettuate nella Console di gestione AWS. Per verificare le autorizzazioni, la procedura dettagliata utilizza gli strumenti della riga di comando, AWS Command Line Interface (AWS CLI) e AWS Tools for Windows PowerShell, quindi non è necessario scrivere alcun codice.

Fase 0: preparazione della procedura guidata

1. Assicurati di averne due Account AWS e che ogni account abbia un amministratore, come mostrato nella tabella nella sezione precedente.
 - a. Registrati per un Account AWS, se necessario.
 - b. Utilizzando le credenziali dell'account A, accedi alla [Console IAM](#) e procedere come segue per creare un utente amministratore:
 - Crea l'utente **AccountAdmin** e annota le credenziali di sicurezza dell'utente. Per ulteriori informazioni sull'aggiunta di utenti, consulta [Creazione di un utente IAM nell'Account AWS](#) nella Guida per l'utente di IAM.
 - Concedi le autorizzazioni di amministratore AccountAdmin allegando una politica utente che dia accesso completo. Per istruzioni, consulta [Gestione delle policy IAM](#) nella Guida all'utente IAM.
 - Nella [dashboard della console IAM](#), annota l'URL utente Sign-In IAM. Gli utenti di questo account devono utilizzare questo URL per accedere alla Console di gestione AWS. Per ulteriori informazioni, consulta [In che modo gli utenti effettuano l'accesso al tuo account](#) nella Guida per l'utente IAM.
 - c. Ripeti il passaggio precedente utilizzando le credenziali dell'account B e creare l'utente amministratore **AccountBadmin**.
2. Configura AWS CLI o gli Strumenti per Windows PowerShell. Assicurati di salvare le credenziali di amministratore nel modo seguente:
 - Se si utilizza il AWS CLI, crea due profili AccountAdmin e AccountBadmin, nel file di configurazione.
 - Se utilizzi gli Strumenti per Windows PowerShell, assicurati di archiviare le credenziali per la sessione come AccountAdmin e AccountBadmin

Per istruzioni, consulta l'argomento [Impostazione degli strumenti per le visite guidate](#).

Fase 1: esecuzione delle attività per l'Account A

Esegui le operazioni riportate di seguito per l'Account A:

Fase 1.1: Accesso alla console

Utilizzando l'URL di accesso utente IAM per l'account A, accedi Console di gestione AWS come **AccountAdmin** utente. Questo utente creerà un bucket e vi alleggerà una policy.

Fase 1.2: Creazione di un bucket e di un utente e aggiunta di una policy di bucket che concede le autorizzazioni utente

1. Nella console di Amazon S3 creare un bucket. Questo esercizio presuppone che il bucket sia stato creato negli Stati Uniti orientali (Virginia settentrionale) Regione AWS e che il nome sia. *amzn-s3-demo-bucket1*

Per istruzioni, consulta l'argomento [Creazione di un bucket per uso generico](#).

2. Nella [console IAM](#), crea un utente **Dave**.

Per istruzioni dettagliate, consulta [Creazione di utenti IAM \(console\)](#) nella Guida all'utente IAM.

3. Osserva le credenziali dell'utente Dave.
4. Nella console di Amazon S3 collegare la seguente policy del bucket a *amzn-s3-demo-bucket1*. Per istruzioni, consulta l'argomento [Aggiunta di una policy di bucket utilizzando la console di Amazon S3](#). Seguire le fasi per l'aggiunta di una policy di bucket. Per informazioni su come trovare gli ID degli account, vedi [Trovare il tuo ID. Account AWS](#)

La policy concede all'Account B le autorizzazioni `s3:PutObject` e `s3:ListBucket`. La policy concede inoltre all'utente Dave l'autorizzazione `s3:GetObject`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
    },
  ],
}
```

```

        "Action": [
            "s3:PutObject",
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "arn:aws:s3:::amzn-s3-demo-bucket1"
        ]
    },
    {
        "Sid": "Statement3",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:user/Dave"
        },
        "Action": [
            "s3:GetObject"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        ]
    }
]
}

```

Fase 2: esecuzione delle attività per l'Account B

Ora che l'account B ha le autorizzazioni per eseguire operazioni sul bucket dell'account A, l'amministratore dell'account B esegue le seguenti operazioni:

- Carica un oggetto nel bucket dell'account A
- Aggiunge una concessione nella ACL dell'oggetto per consentire all'account A, proprietario del bucket, il pieno controllo

Utilizzo di AWS CLI

1. Con il comando `put-object` AWS CLI, carica un oggetto. Il parametro `--body` nel comando identifica il file di origine da caricare. Ad esempio, se il file si trova sull'unità C: di una macchina Windows, specifica `c:\HappyFace.jpg`. Il parametro `--key` fornisce il nome della chiave dell'oggetto.


```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --body  
HappyFace.jpg --profile AccountBadmin
```

2. Aggiungere un'autorizzazione nell'ACL dell'oggetto per concedere controllo completo dell'oggetto al proprietario del bucket. Per informazioni su come trovare un ID utente canonico, consulta la sezione [Trovare l'ID utente canonico per Account AWS](#) nella AWS Guida di riferimento per la gestione degli account.

```
aws s3api put-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --grant-  
full-control id="AccountA-CanonicalUserID" --profile AccountBadmin
```

Utilizzo degli strumenti per Windows PowerShell

1. Con il comando Write-S3Object, carica un oggetto.

```
Write-S3Object -BucketName amzn-s3-demo-bucket1 -key HappyFace.jpg -file  
HappyFace.jpg -StoredCredentials AccountBadmin
```

2. Aggiungere un'autorizzazione nell'ACL dell'oggetto per concedere controllo completo dell'oggetto al proprietario del bucket.

```
Set-S3ACL -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -CannedACLName  
"bucket-owner-full-control" -StoredCreden
```

Fase 3: testare le autorizzazioni

A questo punto, verifica se l'utente Dave nell'Account A ha accesso all'oggetto di proprietà dell'Account B.

Utilizzo di AWS CLI

1. Aggiungi le credenziali dell'utente Dave al file di AWS CLI configurazione e crea un nuovo profilo, UserDaveAccountA. Per ulteriori informazioni, consulta [Impostazione degli strumenti per le visite guidate](#).

```
[profile UserDaveAccountA]  
aws_access_key_id = access-key  
aws_secret_access_key = secret-access-key
```

```
region = us-east-1
```

2. Esegui il comando della CLI di `get-object` per scaricare `HappyFace.jpg` e salvarlo in locale. Le credenziali dell'utente Dave vengono fornite aggiungendo il parametro `--profile`.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key  
HappyFace.jpg Outputfile.jpg --profile UserDaveAccountA
```

Utilizzo degli strumenti per Windows PowerShell

1. Memorizza AWS le credenziali dell'utente Dave, come `UserDaveAccountA`, in un archivio permanente.

```
Set-AWSCredentials -AccessKey UserDave-AccessKey -SecretKey UserDave-  
SecretAccessKey -storeas UserDaveAccountA
```

2. Esegui il comando `Read-S3Object` per scaricare l'oggetto `HappyFace.jpg` e salvarlo in locale. Le credenziali dell'utente Dave vengono fornite aggiungendo il parametro `-StoredCredentials`.

```
Read-S3Object -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -file  
HappyFace.jpg -StoredCredentials UserDaveAccountA
```

Fase 4: pulizia

1. Una volta terminato il test, è possibile eseguire le seguenti operazioni di pulizia:
 - Accedi alla [Console di gestione AWS](#) utilizzando le credenziali dell'Account A e procedere come di seguito:
 - Nella console di Amazon S3 rimuovere la policy del bucket collegata a *amzn-s3-demo-bucket1*. Nelle Proprietà del bucket, elimina la policy nella sezione Autorizzazioni.
 - Se il bucket è stato creato per questo esercizio, nella console di Amazon S3 eliminare gli oggetti e quindi il bucket.
 - Nella [Console IAM](#), rimuovi l'utente `AccountAdmin`. Per istruzioni dettagliate, consulta [Eliminazione di un utente IAM](#) nella Guida all'utente IAM.

2. Accedere alla [Console di gestione AWS](#) tramite le credenziali dell'Account B. Nella console [IAM](#), elimina l'utente. AccountAdmin

Esempio 4 - Proprietario di un bucket che concede un'autorizzazione multi-account agli oggetti di cui non è proprietario

Argomenti

- [Comprendere le autorizzazioni multi-account e utilizzare i ruoli IAM](#)
- [Fase 0: preparazione della procedura guidata](#)
- [Fase 1: eseguire le attività per l'Account A](#)
- [Fase 2: esecuzione delle attività per l'Account B](#)
- [Fase 3: Eseguire le attività dell'Account C](#)
- [Fase 4: pulizia](#)
- [Risorse correlate](#)

In questo scenario di esempio, possiedi un bucket e hai consentito ad altri Account AWS di caricare oggetti. Se è stata applicata l'impostazione proprietario del bucket applicato per S3 Object Ownership per il bucket, si avrà proprietà di tutti gli oggetti nel bucket, inclusi gli oggetti scritti da un altro Account AWS. Questo approccio risolve il problema che gli oggetti non sono di proprietà dell'utente, il proprietario del bucket. Quindi, puoi delegare le autorizzazioni agli utenti nel tuo account o ad altri Account AWS. Supponiamo che l'impostazione proprietario del bucket applicato per S3 Object Ownership non sia abilitata. In altre parole, il bucket può avere oggetti di proprietà di altri Account AWS .

Ora, si supponga che, in qualità di proprietario del bucket, si debbano concedere autorizzazioni multiaccount per gli oggetti a un utente di un altro account, indipendentemente dall'utente a cui appartengono. Ad esempio, l'utente potrebbe essere un'applicazione per la fatturazione che deve accedere ai metadata dell'oggetto. Esistono due problemi principali:

- Il proprietario del bucket non dispone delle autorizzazioni per gli oggetti creati dagli altri Account AWS. Affinché il proprietario del bucket possa concedere autorizzazioni su oggetti che non possiede, il proprietario dell'oggetto deve prima concedere l'autorizzazione al proprietario del bucket. Il proprietario dell'oggetto è Account AWS che ha creato gli oggetti. Il proprietario del bucket può quindi delegare tali autorizzazioni.

- L'account proprietario del bucket può delegare le autorizzazioni agli utenti del proprio account (consulta [Esempio 3: il proprietario del bucket concede autorizzazioni per gli oggetti che non sono di sua proprietà](#)). Tuttavia, l'account proprietario del bucket non può delegare le autorizzazioni ad altri Account AWS perché la delega tra account non è supportata.

In questo scenario, il proprietario del bucket può creare un ruolo AWS Identity and Access Management (IAM) con il permesso di accedere agli oggetti. Quindi, il proprietario del bucket può concedere un'altra Account AWS autorizzazione per assumere il ruolo, abilitandolo temporaneamente ad accedere agli oggetti nel bucket.

Note

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le liste di controllo degli accessi (ACL) sono disabilitate. Quando le ACL sono disabilitate, il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ad essi in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne nelle circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Con le ACL disabilitate, puoi utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Comprendere le autorizzazioni multi-account e utilizzare i ruoli IAM

I ruoli IAM consentono diversi scenari per la delega dell'accesso alle risorse. Uno degli scenari principali è l'accesso multiaccount. In questo esempio, il proprietario del bucket, l'Account A, utilizza un ruolo IAM per delegare temporaneamente l'accesso agli oggetti tra più account agli utenti di un altro Account AWS account C. A ciascun ruolo IAM creato sono associate le due politiche seguenti:

- Una politica di fiducia che ne identifica un'altra Account AWS che può assumere il ruolo.

- Una policy di accesso per la definizione delle autorizzazioni consentite quando qualcuno assume il ruolo, ad esempio `s3:GetObject`. Per un elenco delle autorizzazioni che è possibile specificare in una policy, consulta [Azioni di policy per Amazon S3](#).

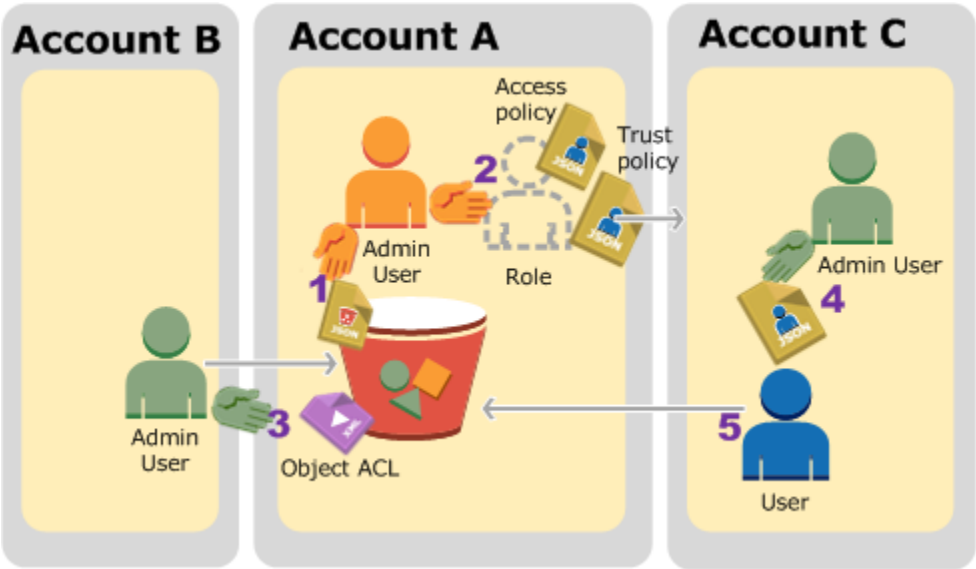
La politica Account AWS identificata nella politica di fiducia concede quindi all'utente l'autorizzazione ad assumere il ruolo. L'utente può quindi accedere agli oggetti nel modo seguente:

- Assumere il ruolo e, in risposta, ottenere le credenziali di sicurezza temporanee.
- Accedere agli oggetti nel bucket utilizzando le credenziali di sicurezza temporanee.

Per ulteriori informazioni sui ruoli IAM, consulta [Ruoli IAM](#) nella Guida per l'utente di IAM.

1. L'utente amministratore dell'account A collega una policy di bucket che concede all'Account B un'autorizzazione condizionale per caricare gli oggetti.
2. L'amministratore dell'Account A crea un ruolo IAM per stabilire l'attendibilità con l'Account C, pertanto gli utenti in quell'account possono accedere all'Account A. La policy di accesso collegata al ruolo limita le operazioni consentite all'utente nell'Account C quando accede all'Account A.
3. L'amministratore dell'Account B carica un oggetto nel bucket di proprietà dell'Account A, concedendo al proprietario del bucket un'autorizzazione al controllo completo.
4. L'amministratore dell'account C crea un utente e collega una policy utente che gli consente di assumere il ruolo.
5. L'utente nell'Account C per prima cosa assume il ruolo, che restituisce all'utente credenziali di sicurezza temporanee. Mediante tali credenziali temporanee, l'utente accede quindi agli oggetti nel bucket.

Di seguito è riportato un riepilogo delle fasi della procedura:



Per questo esempio sono necessari tre account. La tabella seguente mostra come viene fatto riferimento a questi account e agli utenti amministratori degli account: In conformità con le linee guida IAM (consulta [Informazioni sull'uso di un utente amministratore per creare risorse e concedere autorizzazioni](#)), in questa guida non utilizzeremo le credenziali Utente root dell'account AWS . Viene invece creato un utente amministratore in ciascun account e le credenziali vengono utilizzate per la creazione di risorse e per concedere autorizzazioni a tali risorse.

Account AWS ID	Account denominato	Utente amministratore nell'account
1111-1111-1111	Account A	AccountAadmin
2222-2222-2222	Account B	AccountBadmin
3333-3333-3333	Account C	AccountCadmin

Fase 0: preparazione della procedura guidata

Note

Si consiglia di aprire un editor di testo e di annotare alcune informazioni man mano che si procede. In particolare, avrai bisogno di ID account, ID utente canonici, Sign-in URL utente

IAM per ogni account da connettere alla console e Amazon Resource Names (ARN) degli utenti e dei ruoli IAM.

1. Assicurati di averne tre Account AWS e ogni account abbia un utente amministratore, come mostrato nella tabella nella sezione precedente.
 - a. Iscriviti a Account AWS, se necessario. Si fa riferimento a questi account come Account A, Account B e Account C.
 - b. Utilizzando le credenziali dell'Account A, accedere alla [console IAM](#) ed effettuare quanto segue per creare un utente amministratore:
 - Crea l'utente **AccountAdmin** e prendi nota delle sue credenziali di sicurezza. Per ulteriori informazioni sull'aggiunta di utenti, consulta [Creazione di un utente IAM nell'Account AWS](#) nella Guida per l'utente di IAM.
 - Concedi i privilegi di amministratore AccountAdmin allegando una politica utente che dà accesso completo. Per istruzioni, consulta [Gestione delle policy IAM](#) nella Guida all'utente IAM.
 - Nella dashboard della console IAM, annota l'URL utente Sign-In IAM. Gli utenti di questo account devono utilizzare questo URL per accedere alla Console di gestione AWS. Per maggiori informazioni, consulta [Accedi Console di gestione AWS come utente IAM](#) nella IAM User Guide.
 - c. Ripetere la fase precedente per creare utenti amministratore nell'Account B e nell'Account C.
2. Per l'account C, annota l'ID utente canonico.

Quando si crea un ruolo IAM nell'Account A, la policy di attendibilità concede all'Account C l'autorizzazione per assumere il ruolo mediante la specifica dell'ID account. È possibile trovare informazioni sull'account come indicato di seguito:

- a. Usa il tuo Account AWS ID o alias dell'account, il tuo nome utente IAM e la tua password per accedere alla console [Amazon S3](#).
- b. Scegliere il nome di un bucket Amazon S3 per visualizzare i relativi dettagli.
- c. Selezionare la scheda Permissions (Autorizzazioni) e selezionare Access Control List (Lista di controllo accessi).

- d. Nella sezione Accesso per il tuo Account AWS, nella colonna Account è presente un identificatore lungo, come
c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6.
Questo è il tuo ID utente canonico.
3. Quando si crea una policy di bucket, è necessario disporre delle informazioni seguenti. Osserva questi valori:
 - ID utente canonico dell'Account A – Quando l'amministratore dell'Account A concede all'amministratore dell'Account B l'autorizzazione condizionale per il caricamento degli oggetti, la condizione specifica l'ID utente canonico dell'utente dell'Account A che deve ottenere controllo completo degli oggetti.

 Note

L'ID utente canonico è un concetto esclusivo di Amazon S3. Si tratta di una versione offuscata dell'ID account, composta da 64 caratteri.

- ARN dell'utente per l'amministratore dell'account B - È possibile trovare l'ARN dell'utente nella [Console IAM](#). È necessario selezionare l'utente e trovare l'ARN dell'utente nella scheda Riepilogo.

Nella policy del bucket, si concede a AccountAdmin l'autorizzazione a caricare oggetti e si specifica l'utente utilizzando l'ARN. Ecco un esempio di valore ARN:

```
arn:aws:iam::AccountB-ID:user/AccountAdmin
```

4. Configura AWS Command Line Interface (CLI) o. AWS Tools for Windows PowerShell Assicurati di salvare le credenziali dell'utente amministratore come segue:
 - Se si utilizza il AWS CLI, crea profili AccountAdmin eAccountAdmin, nel file di configurazione.
 - Se utilizzi il AWS Tools for Windows PowerShell, assicurati di archiviare le credenziali per la sessione come eAccountAdmin. AccountAdmin

Per istruzioni, consulta l'argomento [Impostazione degli strumenti per le visite guidate](#).

Fase 1: eseguire le attività per l'Account A

In questo esempio, l'Account A è il proprietario del bucket. Quindi l'utente AccountAdmin nell'Account A farà quanto segue:

- Creare un bucket.
- Allega una policy del bucket che conceda all'amministratore dell'account B l'autorizzazione a caricare oggetti.
- Crea un ruolo IAM che conceda all'account C l'autorizzazione ad assumere il ruolo in modo da poter accedere agli oggetti del bucket.

Passaggio 1.1: Accedi al Console di gestione AWS

Utilizzando l' Sign-in URL utente IAM per l'account A, accedi prima a Console di gestione AWS come **AccountAdmin** utente. Questo utente creerà un bucket e vi alleggerà una policy.

Fase 1.2: creare un bucket e allegarlo alla policy di bucket

Nella console di Amazon S3 effettuare quanto segue:

1. Creare un bucket. In questo esercizio si presume che il nome del bucket sia *amzn-s3-demo-bucket1*.

Per istruzioni, consulta l'argomento [Creazione di un bucket per uso generico](#).

2. Allega la seguente policy del bucket. La policy concede all'amministratore dell'account B l'autorizzazione condizionata a caricare gli oggetti.

Aggiorna la policy fornendo valori personalizzati per *amzn-s3-demo-bucket1*, *AccountB-ID*, e *CanonicalUserId-of-AWSaccountA-BucketOwner*.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "111",
      "Effect": "Allow",
      "Principal": {
```

```

        "AWS": "arn:aws:iam::111122223333:user/AccountBadmin"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
  },
  {
    "Sid": "112",
    "Effect": "Deny",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:user/AccountBadmin"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-grant-full-control": "id=CanonicalUserId-of-
AWSaccountA-BucketOwner"
      }
    }
  }
]
}

```

Fase 1.3: Creare un ruolo IAM per consentire all'account C l'accesso multi-account all'account A

Nella [Console IAM](#), crea un ruolo IAM (**examplerole**) che conceda all'account C l'autorizzazione ad assumere il ruolo. Assicurati di aver effettuato l'accesso come amministratore dell'account A, poiché il ruolo deve essere creato nell'account A.

1. Prima di creare il ruolo, preparare la policy gestita che definisce le autorizzazioni richieste dal ruolo. La policy verrà collegata al ruolo in una fase successiva.
 - a. Nel riquadro di navigazione a sinistra, seleziona Policy e poi Crea policy.
 - b. Accanto a Create Your Own Policy (Crea la tua policy) scegli Select (Seleziona).
 - c. Immettere **access-accountA-bucket** nel campo Policy Name (Nome policy).
 - d. Copiare la seguente policy di accesso e incollarla nel campo Policy Document (Documento policy). La policy di accesso concede l'autorizzazione al ruolo s3:GetObject, quindi, quando l'utente Account C assume il ruolo, può eseguire solo l'operazione s3:GetObject.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
  ]
}
```

- e. Scegli Crea policy.

La nuova policy viene inserita nell'elenco delle policy gestite.

2. Nel riquadro di navigazione a sinistra, scegli Ruoli e quindi Crea nuovo ruolo.
3. In Seleziona tipo di ruolo, seleziona Ruolo per Cross-Account l'accesso, quindi scegli il pulsante Seleziona accanto a Fornisci l'accesso tra i Account AWS tuoi.
4. Immettere l'ID account dell'Account C.

Per questa guida, non è necessario richiedere agli utenti l'autenticazione a più fattori (MFA) per assumere il ruolo, quindi lasciare l'opzione deselezionata.

5. Scegli Fase successiva per impostare le autorizzazioni associate al ruolo.
6. Seleziona la casella di controllo accanto alla A-bucket politica dell'account di accesso che hai creato, quindi scegli Passaggio successivo.

Viene visualizzata la pagina Review (Revisione) che consente di confermare le impostazioni per il ruolo prima che venga creato. Questa pagina contiene una voce molto importante, ossia il collegamento che è possibile inviare agli utenti che hanno necessità di utilizzare questo ruolo. Gli utenti che utilizzano il link accedono direttamente alla pagina Cambia ruolo con i campi ID account e Nome ruolo già compilati. Questo link è visibile anche in seguito nella pagina di riepilogo dei ruoli per qualsiasi multi-account.

7. Immetti `examplerole` per il nome del ruolo, quindi scegli Fase successiva.
8. Dopo aver esaminato il ruolo, scegli Crea ruolo.

Il ruolo `examplerole` viene visualizzato nell'elenco dei ruoli.

9. Scegli il nome del ruolo `examplerole`.
10. Selezionare la scheda Trust Relationships (Relazioni di trust).
11. Scegli Mostra documento della policy e verifica che la policy di attendibilità mostrata corrisponda alla policy seguente.

Le seguente policy di attendibilità stabilisce l'attendibilità con l'Account C, consentendogli di eseguire l'operazione `sts:AssumeRole`. Per ulteriori informazioni, consulta [AssumeRole](#) nella documentazione di riferimento dell'API Servizio di token di sicurezza AWS .

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

12. Osserva il nome della risorsa Amazon (ARN) del ruolo `examplerole` creato.

Nelle fasi successive verrà illustrato come allegare una policy utente per consentire all'utente IAM di assumere questo ruolo e come identificare il ruolo mediante il valore ARN.

Fase 2: esecuzione delle attività per l'Account B

Il bucket di esempio di proprietà dell'Account A necessita di oggetti di proprietà di altri account. In questa fase, l'amministratore dell'Account B carica un oggetto mediante gli strumenti a riga di comando.

- Utilizzando il `put-object` AWS CLI comando, carica un oggetto su. ***amzn-s3-demo-bucket1***

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --  
body HappyFace.jpg --grant-full-control id="canonicalUserId-ofTheBucketOwner" --  
profile AccountBadmin
```

Tenere presente quanto segue:

- Il parametro `--Profile` specifica il profilo `AccountBadmin`, quindi l'oggetto è di proprietà dell'account B.
- Il parametro `grant-full-control` concede al proprietario del bucket l'autorizzazione al controllo completo sull'oggetto, come richiesto dalla policy di bucket.
- Il parametro `--body` identifica il file di origine da caricare. Ad esempio, se il file si trova nell'unità C: di un computer Windows, si specifica `c:\HappyFace.jpg`.

Fase 3: Eseguire le attività dell'Account C

Nei passaggi precedenti, l'account A ha già creato un ruolo, `examplerole`, che stabilisce un rapporto di attendibilità con l'account C. Questo ruolo consente agli utenti dell'account C di accedere all'account A. In questo passaggio, l'amministratore dell'account C crea un utente (Dave) e gli delega il permesso `sts:AssumeRole` ricevuto dall'account A. Questo approccio consente a Dave di assumere il ruolo `examplerole` e di ottenere temporaneamente l'accesso all'account A. La policy di accesso che l'account A ha collegato al ruolo limita ciò che Dave può fare quando accede all'account A, in particolare ottenere oggetti in *amzn-s3-demo-bucket1*.

Passaggio 3.1: Creare un utente nell'Account C e delegare l'autorizzazione ad assumere ruolo di esempio

1. Utilizzando l'URL di accesso dell'utente IAM per l'account C, accedi prima all'utente `as`. Console di gestione AWS **AccountAdmin**
2. Nella [console IAM](#), crea un utente, Dave.

Per istruzioni dettagliate, consulta [Creazione di utenti IAM \(Console di gestione AWS\)](#) nella Guida all'utente IAM.

3. Annota le credenziali di Dave. Dave dovrà utilizzare queste credenziali per assumere il ruolo `examplerole`.
4. Crea una policy in linea per l'utente IAM Dave per delegare a Dave l'autorizzazione `sts:AssumeRole` sul ruolo `examplerole` nell'account A.

- a. Nel riquadro di navigazione sinistro, scegli Utenti.
- b. Scegli il nome utente Dave.
- c. Nella pagina dei dettagli dell'utente, selezionare la scheda Permissions (Autorizzazioni), quindi espandere la sezione Inline Policies (Policy inline).
- d. Scegliere click here (fai clic qui) oppure Create User Policy (Crea policy di utente).
- e. Scegliere Custom Policy (Policy personalizzata) quindi Select (Seleziona).
- f. Immettere un nome per la policy nel campo Policy Name (Nome policy).
- g. Copiare la seguente policy nel campo Policy Document (Documento policy).

È necessario aggiornare la policy fornendo *AccountA-ID*.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/examplerole"
    }
  ]
}
```

- h. Scegli Apply Policy (Applica policy).
5. Salva le credenziali di Dave nel file di configurazione di AWS CLI aggiungendo un altro profilo, AccountCDave

```
[profile AccountCDave]
aws_access_key_id = UserDaveAccessKeyID
aws_secret_access_key = UserDaveSecretAccessKey
region = us-west-2
```

Passaggio 3.2: Assumi il ruolo (ruolo di esempio) e accedi agli oggetti

Ora Dave può accedere agli oggetti nel bucket di proprietà dell'Account A nel modo seguente:

- Per prima cosa, Dave assume il ruolo `examplerole` utilizzando le sue credenziali personali. Questa operazione restituirà le credenziali temporanee.
 - Dave utilizzerà le credenziali temporanee per accedere agli oggetti nel bucket dell'Account A.
1. Al prompt dei comandi, esegui il AWS CLI `assume-role` comando seguente utilizzando il `AccountCDave` profilo.

È necessario aggiornare il valore ARN nel comando fornendo l'*AccountA-ID* dove è definito `examplerole`.

```
aws sts assume-role --role-arn arn:aws:iam::AccountA-ID:role/examplerole --profile
AccountCDave --role-session-name test
```

In risposta, Servizio di token di sicurezza AWS (AWS STS) restituisce le credenziali di sicurezza temporanee (ID della chiave di accesso, chiave di accesso segreta e un token di sessione).

2. Salva le credenziali di sicurezza temporanee nel file di AWS CLI configurazione sotto il profilo. `TempCred`

```
[profile TempCred]
aws_access_key_id = temp-access-key-ID
aws_secret_access_key = temp-secret-access-key
aws_session_token = session-token
region = us-west-2
```

3. Al prompt dei comandi, esegui il AWS CLI comando seguente per accedere agli oggetti utilizzando le credenziali temporanee. Ad esempio, il comando specifica l'API `head-object` per recuperare i metadata dell'oggetto per l'oggetto `HappyFace.jpg`.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --
key HappyFace.jpg SaveFileAs.jpg --profile TempCred
```

Dal momento che la policy di accesso collegata a `examplerole` consente l'esecuzione delle operazioni, Amazon S3 elabora la richiesta. È possibile provare ad eseguire un'altra operazione su qualsiasi altro oggetto nel bucket.

Se si tenta un'altra azione, ad esempio `get-object-acl`, l'autorizzazione sarà negata perché il ruolo non è autorizzato a eseguire tale azione.

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --  
profile TempCred
```

È stato utilizzato l'utente Dave per assumere il ruolo e accedere all'oggetto mediante le credenziali temporanee. L'accesso agli oggetti in *amzn-s3-demo-bucket1* può essere effettuato anche da un'applicazione nell'Account C. L'applicazione può ottenere credenziali di sicurezza temporanee e l'Account C può delegare all'applicazione le autorizzazioni per assumere `examplerole`.

Fase 4: pulizia

1. Una volta terminato il test, è possibile eseguire le seguenti operazioni di pulizia:
 - Accedi alla [Console di gestione AWS](#) utilizzando le credenziali dell'Account A e procedere come di seguito:
 - Nella console di Amazon S3 rimuovere la policy del bucket collegata a *amzn-s3-demo-bucket1*. Nelle Proprietà del bucket, elimina la policy nella sezione Autorizzazioni.
 - Se il bucket è stato creato per questo esercizio, nella console di Amazon S3 eliminare gli oggetti e quindi il bucket.
 - Nella [Console IAM](#), rimuovi l'indirizzo `examplerole` creato nell'account A. Per istruzioni dettagliate, consulta [Eliminazione di un utente IAM](#) nella Guida all'utente IAM.
 - Nella [Console IAM](#), rimuovi l'utente `AccountAdmin`.
2. Accedi alla [Console IAM](#) utilizzando le credenziali dell'account B. Eliminare l'utente `AccountAdmin`.
3. Accedi alla [Console IAM](#) utilizzando le credenziali dell'Account C. Elimina `AccountAdmin` e l'utente Dave.

Risorse correlate

Per ulteriori informazioni relative a questa guida, consulta le seguenti risorse nella Guida all'utente IAM:

- [Creazione di un ruolo per delegare le autorizzazioni a un utente IAM](#)
- [Tutorial: Delega l'accesso Account AWS tramite i ruoli IAM](#)
- [Gestione delle policy IAM](#)

Utilizzo dei ruoli collegati ai servizi per Amazon S3 Storage Lens

Per utilizzare Amazon S3 Storage Lens per raccogliere e aggregare i parametri su tutti i tuoi account AWS Organizations, devi innanzitutto assicurarti che per S3 Storage Lens sia abilitato l'accesso attendibile all'account di gestione della tua organizzazione. S3 Storage Lens crea un ruolo collegato ai servizi (SLR) per consentirgli di ottenere l'elenco di appartenenza all'organizzazione. Account AWS Questo elenco di account viene utilizzato da S3 Storage Lens per raccogliere i parametri delle risorse S3 in tutti gli account membri quando il pannello di controllo o le configurazioni dello Storage Lens S3 vengono create o aggiornate.

Amazon S3 Storage Lens utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html#iam-term-service-linked-role Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a S3 Storage Lens. Service-linked i ruoli sono predefiniti da S3 Storage Lens e includono tutte le autorizzazioni richieste dal servizio per chiamare altri per conto dell'utente. Servizi AWS

Un ruolo collegato ai servizi semplifica la configurazione di S3 Storage Lens perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. S3 Storage Lens definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo S3 Storage Lens potrà assumere i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare il ruolo collegato ai servizi solo dopo avere eliminato le risorse correlate. Questa procedura protegge le risorse di S3 Storage Lens perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta [AWS i servizi che funzionano con IAM](#) e cerca i servizi che hanno Sì nella colonna Ruolo. Service-Linked Scegliere Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Service-linked autorizzazioni di ruolo per Amazon S3 Storage Lens

S3 Storage Lens utilizza il ruolo collegato al servizio denominato

`AWSServiceRoleForS3StorageLens`: Ciò consente l'accesso ai AWS servizi e alle risorse utilizzati o gestiti da S3 Storage Lens. Ciò consente a S3 Storage Lens di accedere alle risorse per tuo conto AWS Organizations .

Il ruolo collegato ai servizi S3 Storage Lens considera attendibile il seguente servizio nello storage dell'organizzazione:

- `storage-lens.s3.amazonaws.com`

La policy delle autorizzazioni del ruolo consente a S3 Storage Lens di eseguire le seguenti operazioni:

- `organizations:DescribeOrganization`

`organizations:ListAccounts`

`organizations:ListAWSServiceAccessForOrganization`

`organizations:ListDelegatedAdministrators`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta le autorizzazioni dei [Service-linked ruoli](#) nella IAM User Guide.

Creazione di un ruolo collegato ai servizi per S3 Storage Lens

Non devi creare manualmente un ruolo collegato ai servizi. Quando completi una delle seguenti attività mentre sei connesso agli account di AWS Organizations gestione o di amministratore delegato, S3 Storage Lens crea automaticamente il ruolo collegato al servizio:

- Crea una configurazione del pannello di controllo S3 Storage Lens per la tua organizzazione nella console di Amazon S3.
- PUT una configurazione S3 Storage Lens per la tua organizzazione utilizzando l'API REST e gli SDK. AWS CLI

 Note

S3 Storage Lens supporterà un massimo di cinque amministratori delegati per organizzazione.

Se si elimina questo ruolo collegato ai servizi, le azioni precedenti lo ricreeranno all'occorrenza.

Esempio di policy per il ruolo collegato ai servizi S3 Storage Lens

Example Policy di autorizzazione per il ruolo collegato ai servizi S3 Storage Lens

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AwsOrgsAccess",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Modifica di un ruolo collegato ai servizi per Amazon S3 Storage Lens

S3 Storage Lens non consente di modificare il ruolo collegato al servizio `AWSServiceRoleForS3StorageLens`. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Amazon S3 Storage Lens

Se non devi più utilizzare il ruolo collegato ai servizi, è consigliabile eliminarlo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Note

Se il servizio Amazon S3 Storage Lens utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminarla `AWSServiceRoleForS3StorageLens` è necessario eliminare tutte le configurazioni S3 Storage Lens a livello di organizzazione presenti in tutte Regioni AWS utilizzando gli account di AWS Organizations gestione o di amministratore delegato.

Le risorse sono configurazioni S3 Storage Lens a livello di organizzazione. Usa S3 Storage Lens per ripulire le risorse e poi usa la console [IAM, la CLI](#), l'API REST o l' AWS SDK per eliminare il ruolo.

Nell'API REST e negli SDK AWS CLI, le configurazioni di S3 Storage Lens possono essere scoperte utilizzando tutte le regioni `ListStorageLensConfigurations` in cui l'organizzazione ha creato configurazioni S3 Storage Lens. Utilizza l'azione `DeleteStorageLensConfiguration` per eliminare queste configurazioni in modo che sia possibile eliminare il ruolo.

Note

Per eliminare il ruolo collegato ai servizi, è necessario eliminare tutte le configurazioni S3 Storage Lens a livello di organizzazione in tutte le regioni in cui esistono.

Per eliminare le risorse di Amazon S3 Storage Lens utilizzate da `AWSServiceRoleForS3StorageLens` SLR

1. Per ottenere un elenco delle configurazioni a livello di organizzazione, è necessario utilizzare `ListStorageLensConfigurations` in ogni Regione in cui sono presenti configurazioni di S3 Storage Lens. Questo elenco può essere ottenuto anche dalla console Amazon S3.

2. Eliminare queste configurazioni dagli endpoint regionali appropriati invocando la chiamata API `DeleteStorageLensConfiguration` o utilizzando la console Amazon S3.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Dopo aver eliminato le configurazioni, elimina la `AWSServiceRoleForS3StorageLens` SLR dalla console [IAM](#) o richiamando l'API IAM o utilizzando l'or `DeleteServiceLinkedRole` SDK. AWS CLI AWS Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi S3 Storage Lens

S3 Storage Lens supporta l'utilizzo di ruoli collegati ai servizi in tutti i luoghi in cui il servizio è disponibile. Regioni AWS Per ulteriori informazioni, consulta la sezione [Regioni ed endpoint di Amazon S3](#).

Risoluzione dei problemi di identità e accesso ad Amazon S3

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi comuni che potresti incontrare quando lavori con Amazon S3 e IAM.

Argomenti

- [Errore di accesso negato ricevuto](#)
- [Non sono autorizzato a eseguire un'azione in Amazon S3](#)
- [Non sono autorizzato a svolgere attività come: PassRole](#)
- [Voglio consentire l'accesso a persone esterne alla mia Account AWS per accedere alle mie risorse Amazon S3](#)
- [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#)

Errore di accesso negato ricevuto

Verifica che non ci sia un'istruzione esplicita Deny contro il richiedente a cui si sta cercando di concedere le autorizzazioni nella policy di bucket o nella policy basata sull'identità.

Per informazioni dettagliate sulla risoluzione dei problemi relativi agli errori di accesso negato, consulta [Risolvi i problemi relativi all'accesso negato \(403 Non consentito\) errori in Amazon S3](#).

Non sono autorizzato a eseguire un'azione in Amazon S3

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa `my-example-widget` fittizia ma non dispone di autorizzazioni `s3:GetWidget` fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
s3:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa `my-example-widget` utilizzando l'azione `s3:GetWidget`.

Se hai bisogno di aiuto, contatta il tuo amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a svolgere attività come: PassRole

Se si riceve un errore che indica che non si è autorizzati a eseguire l'azione `iam:PassRole`, è necessario aggiornare le policy per consentire di passare un ruolo ad Amazon S3.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente esempio di errore si verifica quando un utente IAM di nome `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon S3. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire l'accesso a persone esterne alla mia Account AWS per accedere alle mie risorse Amazon S3

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizzare tali policy per concedere alle persone l'accesso alle proprie risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon S3 supporta queste funzioni, consulta [Come funziona Amazon S3 con IAM](#).
- Per sapere come fornire l'accesso alle tue risorse su Account AWS quello che possiedi, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà](#) nella IAM User Guide.
- Per sapere come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a risorse Account AWS di proprietà di terzi](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente di IAM.

Risolvi i problemi relativi all'accesso negato (403 Non consentito) errori in Amazon S3

Gli errori di accesso negato (HTTP403 Forbidden) compaiono quando si nega AWS esplicitamente o implicitamente una richiesta di autorizzazione.

- Un rifiuto esplicito si verifica quando una policy contiene una Deny dichiarazione per l'azione specifica. AWS
- Un diniego implicito si verifica quando non è presente un'istruzione Deny applicabile e non è presente neppure un'istruzione Allow applicabile.

Poiché una policy AWS Identity and Access Management (IAM) nega implicitamente un principale IAM per impostazione predefinita, la policy deve consentire esplicitamente al principale di eseguire un'azione. In caso contrario, la policy nega implicitamente l'accesso. Per ulteriori informazioni, consulta la sezione [Differenza tra rifiuti espliciti e impliciti](#) nella Guida all'utente IAM. Per informazioni sulla logica di valutazione delle policy che determina se una richiesta di accesso è consentita o negata, consulta [Logica di valutazione delle policy](#) nella Guida all'utente IAM.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

I seguenti argomenti trattano le cause più comuni degli errori di accesso negato in Amazon S3.

Note

Per gli errori di accesso negato (HTTP403 Forbidden), Amazon S3 non addebita alcun costo al proprietario del bucket quando la richiesta viene avviata al di fuori dell' AWS account individuale del proprietario del bucket o dell'organizzazione del proprietario del bucket. AWS

Argomenti

- [Esempi di messaggi di accesso negato e di risoluzione dei problemi](#)
- [Accesso negato a causa delle impostazioni Pagamento a carico del richiedente](#)
- [Policy di bucket e policy IAM](#)
- [Impostazioni ACL di Amazon S3](#)
- [Impostazioni dell'opzione S3 Blocco dell'accesso pubblico](#)
- [Impostazioni della crittografia Amazon S3](#)
- [Impostazioni dell'opzione S3 Blocco oggetti](#)
- [Policy di endpoint VPC](#)
- [AWS Organizations policies](#)
- [CloudFront accesso alla distribuzione](#)
- [Impostazioni del punto di accesso](#)
- [Risorse aggiuntive](#)

Note

Se si sta cercando di risolvere un problema di permessi, inizia dalla sezione [the section called “Esempi di messaggi di accesso negato e di risoluzione dei problemi”](#), quindi passa alla sezione [???](#). Assicurati inoltre di seguire le indicazioni contenute in [the section called “Suggerimenti per la verifica delle autorizzazioni”](#).

Esempi di messaggi di accesso negato e di risoluzione dei problemi

Amazon S3 ora include un contesto aggiuntivo negli errori di accesso negato (HTTP403 Forbidden) per le richieste effettuate a risorse all'interno della stessa o della stessa organizzazione in. Account AWS AWS Organizations Questo contesto include il tipo di policy che ha negato l'accesso, il motivo del rifiuto e le informazioni sull'utente o sul ruolo IAM che ha richiesto l'accesso alla risorsa.

Con questo contesto aggiuntivo, puoi risolvere i problemi di accesso, identificare la causa principale degli errori di accesso negato e correggere i controlli di accesso errati aggiornando le politiche pertinenti. Questo contesto aggiuntivo è disponibile anche nei AWS CloudTrail log. I messaggi di errore di accesso negato avanzati per le richieste relative allo stesso account o alla stessa organizzazione sono disponibili in tutti Regioni AWS, comprese le regioni cinesi AWS GovCloud (US) Regions e cinesi.

Per i casi di rifiuto esplicito, il messaggio di errore include anche l'Amazon Resource Name (ARN) della politica specifica che ha rifiutato la richiesta. Con questa policy ARN, puoi identificare rapidamente la policy esatta responsabile del rifiuto e accedervi direttamente per apportare le modifiche necessarie. Il messaggio di errore include la politica ARN per le politiche di controllo dei servizi (SCP), le politiche di controllo delle risorse (RCP), le politiche basate sull'identità, le politiche di sessione e i limiti delle autorizzazioni.

Per la maggior parte, i messaggi di errore di accesso negato sono visualizzati nel formato `User user-arn is not authorized to perform action on "resource-arn" because context`. In questo esempio, *user-arn* è il [nome della risorsa Amazon \(ARN\)](#) dell'utente che non riceve l'accesso, *action* è l'azione del servizio che la policy nega e *resource-arn* è l'ARN della risorsa su cui agisce la policy. Il campo *context* rappresenta un contesto aggiuntivo sul tipo di policy che spiega perché la policy ha negato l'accesso.

Quando una policy nega esplicitamente l'accesso perché contiene una Deny dichiarazione, il messaggio di errore di accesso negato include la frase `with an explicit deny in a type policy`, insieme all'ARN della politica specifica che ha rifiutato la richiesta. Quando la policy nega implicitamente l'accesso, il messaggio di errore di accesso negato include la frase `because no type policy allows the action action`.

Important

- I messaggi di accesso negato avanzato vengono restituiti solo per le richieste relative allo stesso account o per le richieste all'interno della stessa organizzazione in. AWS

Organizations Cross-account le richieste esterne alla stessa organizzazione restituiscono un messaggio generico `Access Denied`.

Per informazioni sulla logica di valutazione delle policy che determina se una richiesta di accesso tra account è consentita o negata, consulta la logica di valutazione delle [Cross-account policy](#) nella IAM User Guide. Per una guida che mostra come concedere l'accesso multi-account, consulta [the section called "Concessione di autorizzazioni multiaccount"](#).

- Per le richieste all'interno della stessa organizzazione in AWS Organizations:
 - I messaggi di accesso negato avanzati non vengono restituiti se la negazione si verifica a causa di una policy dell'endpoint del cloud privato virtuale (VPC).
 - I messaggi di accesso negato avanzati vengono forniti ogni volta che sia il proprietario del bucket sia l'account chiamante appartengono alla stessa organizzazione in AWS Organizations. Sebbene i bucket configurati con le impostazioni Proprietario del bucket preferito o Autore dell'oggetto di Proprietà dell'oggetto S3 possano contenere oggetti di proprietà di account diversi, la proprietà degli oggetti non influisce sui messaggi di accesso negato avanzati. I messaggi di accesso negato avanzati vengono restituiti per tutte le richieste di oggetti purché il proprietario del bucket e il chiamante si trovino nella stessa organizzazione, indipendentemente dal proprietario dell'oggetto specifico. Per informazioni sulle impostazioni e le configurazioni di Proprietà dell'oggetto, consulta [the section called "Controllo della proprietà degli oggetti"](#).
- I messaggi di errore di accesso negato non vengono restituiti per le richieste effettuate ai bucket di directory. Le richieste di directory bucket restituiscono un messaggio generico `Access Denied`.
- Se più policy dello stesso tipo negano una richiesta di autorizzazione, il messaggio di errore Accesso negato non specifica il numero di policy.
- Per i casi di rifiuto esplicito, il messaggio di errore include l'ARN della politica specifica che ha rifiutato la richiesta. Ciò si applica alle politiche di controllo dei servizi (SCP), alle politiche di controllo delle risorse (RCP), alle politiche basate sull'identità, alle politiche di sessione e ai limiti delle autorizzazioni.
- Se più tipi di policy negano una richiesta di autorizzazione, il messaggio di errore include solo uno di questi tipi di policy.
- Se una richiesta di accesso viene rifiutata per più motivi, il messaggio di errore include solo uno dei motivi del rifiuto.

Gli esempi seguenti mostrano il formato dei diversi tipi di messaggi di errore di accesso negato e come risolvere i problemi di ciascun tipo di messaggio.

Accesso negato a causa del tipo di crittografia bloccato

Per limitare i tipi di crittografia lato server che puoi utilizzare nei tuoi bucket generici, puoi scegliere di bloccare le richieste di SSE-C scrittura aggiornando la configurazione di crittografia predefinita per i tuoi bucket. Questa configurazione a livello di bucket blocca le richieste di caricamento di oggetti che specificano SSE-C. Quando SSE-C è bloccata per un bucket `PutObject`, `CopyObject`, `PostObject`, qualsiasi richiesta di caricamento o replica in più parti che specifichi la SSE-C crittografia verrà rifiutata con un errore HTTP 403. `AccessDenied`

Questa impostazione è un parametro dell'`PutBucketEncryptionAPI` e può essere aggiornata anche utilizzando la console S3, la AWS CLI e gli AWS SDK, se si dispone dell'autorizzazione. `s3:PutEncryptionConfiguration` I valori validi sono `SSE-C`, che blocca la SSE-C crittografia per il bucket generico `eNONE`, che consente l'uso SSE-C per le scritture nel bucket.

Ad esempio, quando l'accesso a una `PutObject` richiesta viene negato perché l'`BlockedEncryptionTypes` impostazione blocca le richieste di scrittura specificando SSE-C, viene visualizzato il seguente messaggio:

```
An error occurred (AccessDenied) when calling the PutObject operation:
User: arn:aws:iam::123456789012:user/MaryMajor is not
authorized to perform: s3:PutObject on resource:
"arn:aws:s3:::amzn-s3-demo-bucket1/object-name" because this
bucket has blocked upload requests that specify
Server Side Encryption with Customer provided keys (SSE-C).
Please specify a different server-side encryption type
```

Per ulteriori informazioni su questa impostazione, consulta [the section called “Blocco o sblocco SSE-C”](#).

Accesso negato a causa di una policy di controllo delle risorse - rifiuto esplicito

1. Verifica la presenza di una Deny dichiarazione esplicita per l'azione nelle tue politiche di controllo delle risorse (RCP). Il messaggio di errore include la policy ARN, che puoi utilizzare per identificare e accedere direttamente alla policy che ha rifiutato la richiesta. Per l'esempio seguente, l'operazione è `s3:GetObject`.

2. Aggiorna la tua RCP rimuovendo l'istruzione Deny. Per ulteriori informazioni, consulta [Aggiornamento di una policy di controllo delle risorse \(RCP\)](#) nella Guida all'utente AWS Organizations .

```
An error occurred (AccessDenied) when calling the GetObject operation:
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
with an explicit deny in a resource control policy, with policy ARN:
arn:aws:organizations::777788889999:policy/o-exampleorgid/resource_control_policy/p-
examplepolicyid
```

Accesso negato a causa di una policy di controllo dei servizi: diniego implicito

1. Verifica un'istruzione Allow mancante relativa all'operazione nelle tue policy di controllo dei servizi. Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiorna la tua SCP aggiungendo l'istruzione Allow. Per ulteriori informazioni, consulta [Aggiornamento di una SCP](#) nella Guida per l'utente di AWS Organizations .

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject because no service control policy allows the s3:GetObject action
```

Accesso negato a causa di una policy di controllo dei servizi: diniego esplicito

1. Verifica la presenza di un'istruzione Deny esplicita relativa all'azione nelle tue policy di controllo dei servizi (SCP). Il messaggio di errore include il criterio ARN, che è possibile utilizzare per identificare e accedere direttamente al criterio che ha rifiutato la richiesta. Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiorna la tua SCP modificando l'istruzione Deny per consentire all'utente l'accesso necessario. Per un esempio di come eseguire questa operazione, consulta Esempi di policy [di controllo del servizio](#) su GitHub. Per ulteriori informazioni sull'aggiornamento dell'SCP, consulta [Aggiornamento di un SCP](#) nella Guida all'utente di AWS Organizations .

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a service control policy, with policy ARN:
arn:aws:organizations::777788889999:policy/o-exampleorgid/service_control_policy/p-
examplepolicyid
```

Accesso negato a causa di una policy dell'endpoint VPC: diniego implicito

1. Verificare la mancanza di un'istruzione Allow per l'azione nelle policy degli endpoint del cloud privato virtuale (VPC). Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiorna la tua policy sugli endpoint VPC aggiungendo l'istruzione Allow. Per ulteriori informazioni, consulta [Aggiornamento di una policy dell'endpoint VPC](#) nella AWS PrivateLink Guida.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no VPC endpoint policy allows the s3:GetObject action
```

Accesso negato a causa di una policy dell'endpoint VPC: diniego esplicito

1. Verifica la presenza di un'istruzione esplicita Deny per l'azione nelle policy dell'endpoint del cloud privato virtuale (VPC). Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiornare la policy dell'endpoint VPC modificando l'istruzione Deny per consentire all'utente l'accesso necessario. Ad esempio, è possibile aggiornare l'istruzione Deny per utilizzare la chiave di condizione `aws:PrincipalAccount` con l'operatore di condizione `StringNotEquals` per consentire l'accesso al principale specifico, come mostrato in [the section called "Esempio 7: Esclusione dei principali dalle istruzioni Deny"](#). Per ulteriori informazioni sull'aggiornamento delle policy degli endpoint VPC, consulta [Aggiornamento di una policy degli endpoint VPC](#) nella Guida a AWS PrivateLink .

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a VPC endpoint policy
```

Accesso negato a causa di limiti delle autorizzazioni: diniego implicito

1. Verifica la presenza di un'istruzione Allow mancante relativa all'azione nel limite delle autorizzazioni. Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiorna il limite delle autorizzazioni aggiungendo l'istruzione Allow relativa alla tua policy IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) e [Modifica delle policy IAM](#) nella Guida dell'utente IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:  
s3:GetObject on resource: "arn:aws:s3::amzn-s3-demo-bucket1/object-name"  
because no permissions boundary allows the s3:GetObject action
```

Accesso negato a causa di un limite delle autorizzazioni: diniego esplicito

1. Verifica la presenza di un'istruzione Deny esplicita relativa all'azione nel limite delle autorizzazioni. Il messaggio di errore include la policy ARN, che è possibile utilizzare per identificare e accedere direttamente alla policy che ha rifiutato la richiesta. Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiornare il limite delle autorizzazioni modificando l'istruzione Deny nella policy IAM per consentire all'utente l'accesso necessario. Ad esempio, è possibile aggiornare l'istruzione Deny per utilizzare la chiave di condizione `aws:PrincipalAccount` con l'operatore di condizione `StringNotEquals` per consentire l'accesso al principale specifico, come mostrato in [aws:PrincipalAccount](#) nella Guida all'utente IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) e [Modifica delle policy IAM](#) nella Guida dell'utente IAM.

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:  
s3:GetObject with an explicit deny in a permissions boundary, with policy ARN:  
arn:aws:iam::777788889999:policy/ExamplePermissionsBoundaryPolicy
```

Accesso negato a causa di policy di sessione: diniego implicito

1. Verifica la presenza di un'istruzione Allow mancante relativa all'azione nelle tue policy di sessione. Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiorna la tua policy di sessione aggiungendo l'istruzione Allow. Per ulteriori informazioni, consulta [Policy di sessione](#) e [Modifica delle policy IAM](#) nella Guida all'utente IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:  
s3:GetObject because no session policy allows the s3:GetObject action
```

Accesso negato a causa di policy di sessione: diniego esplicito

1. Verifica la presenza di un'istruzione Deny esplicita relativa all'azione nelle tue policy di sessione. Il messaggio di errore include il criterio ARN, che è possibile utilizzare per identificare e accedere

direttamente al criterio che ha rifiutato la richiesta. Per l'esempio seguente, l'operazione è `s3:GetObject`.

2. Aggiornare la policy di sessione modificando l'istruzione Deny per consentire all'utente l'accesso necessario. Ad esempio, è possibile aggiornare l'istruzione Deny per utilizzare la chiave di condizione `aws:PrincipalAccount` con l'operatore di condizione `StringNotEquals` per consentire l'accesso al principale specifico, come mostrato in [the section called “Esempio 7: Esclusione dei principali dalle istruzioni Deny”](#). Per ulteriori informazioni sull'aggiornamento delle policy di sessione, consulta [Policy di sessione](#) e [Modifica delle policy IAM](#) nella Guida all'utente IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a session policy, with policy ARN:
arn:aws:iam::123456789012:policy/ExampleSessionPolicy
```

Accesso negato a causa di policy basate sulle risorse: diniego implicito

Note

Resource-based per policy si intendono politiche come le politiche bucket e le policy dei punti di accesso.

1. Verifica la presenza di un'istruzione Allow mancante relativa all'azione nella tua policy basata sulle risorse. Controlla anche se l'impostazione `IgnorePublicAcls` di Blocco dell'accesso pubblico S3 è applicata a livello di bucket, punto di accesso o account. Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiorna la tua policy aggiungendo l'istruzione Allow. Per ulteriori informazioni, consulta [Resource-based le policy](#) e la [modifica delle policy IAM](#) nella IAM User Guide.

Potrebbe anche essere necessario modificare l'impostazione `IgnorePublicAcls` di Blocco dell'accesso pubblico per il bucket, il punto di accesso o l'account. Per ulteriori informazioni, consulta [the section called “Accesso negato a causa delle impostazioni di Blocco accesso pubblico”](#) e [the section called “Configurazione delle impostazioni del bucket e dei punti di accesso”](#).

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
```

```
s3:GetObject
```

 because no resource-based policy allows the `s3:GetObject` action

Accesso negato a causa di policy basate sulle risorse: diniego esplicito

Note

Resource-based per policy si intendono politiche come le politiche bucket e le policy dei punti di accesso.

1. Verifica la presenza di un'istruzione Deny esplicita relativa all'azione nella tua policy basata sulle risorse. Controlla anche se l'impostazione `RestrictPublicBuckets` di Blocco dell'accesso pubblico S3 è applicata a livello di bucket, punto di accesso o account. Per l'esempio seguente, l'operazione è `s3:GetObject`.
2. Aggiorna la policy modificando l'istruzione Deny per consentire all'utente l'accesso necessario. Ad esempio, è possibile aggiornare l'istruzione Deny per utilizzare la chiave di condizione `aws:PrincipalAccount` con l'operatore di condizione `StringNotEquals` per consentire l'accesso al principale specifico, come mostrato in [the section called “Esempio 7: Esclusione dei principali dalle istruzioni Deny”](#). Per ulteriori informazioni sull'aggiornamento della policy basata sulle risorse, consulta [Resource-based le policy](#) e la [modifica delle policy IAM](#) nella IAM User Guide.

Potrebbe anche essere necessario modificare l'impostazione `RestrictPublicBuckets` di Blocco dell'accesso pubblico per il bucket, il punto di accesso o l'account. Per ulteriori informazioni, consulta [the section called “Accesso negato a causa delle impostazioni di Blocco accesso pubblico”](#) e [the section called “Configurazione delle impostazioni del bucket e dei punti di accesso”](#).

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

Accesso negato a causa di policy basate sull'identità: diniego implicito

1. Verifica l'eventuale mancanza di un'istruzione Allow per l'azione nelle policy basate sull'identità collegate all'identità. Per l'esempio seguente, l'azione è `s3:GetObject` e l'identità è l'utente IAM. `MaryMajor`

2. Aggiorna la tua policy aggiungendo l'istruzione Allow. Per ulteriori informazioni, consulta [Identity-based le policy](#) e la [modifica delle policy IAM](#) nella IAM User Guide.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no identity-based policy allows the s3:GetObject action
```

Accesso negato a causa di policy basate sull'identità: diniego esplicito

1. Verifica la presenza di un'istruzione Deny esplicita per l'azione nelle policy basate sull'identità collegate all'identità. Il messaggio di errore include la policy ARN, che puoi utilizzare per identificare e accedere direttamente alla policy che ha rifiutato la richiesta. Nel seguente esempio, l'azione è `s3:GetObject` e l'identità è l'utente `MaryMajor` IAM.
2. Aggiorna la policy modificando l'istruzione Deny per consentire all'utente l'accesso necessario. Ad esempio, è possibile aggiornare l'istruzione Deny per utilizzare la chiave di condizione `aws:PrincipalAccount` con l'operatore di condizione `StringNotEquals` per consentire l'accesso al principale specifico, come mostrato in [aws:PrincipalAccount](#) nella Guida all'utente IAM. Per ulteriori informazioni, consulta [Identity-based le policy](#) e la [modifica delle policy IAM](#) nella IAM User Guide.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3::amzn-s3-demo-bucket1/object-name" with
an explicit deny in an identity-based policy, with policy ARN:
arn:aws:iam::123456789012:policy/ExampleIdentityBasedPolicy
```

Accesso negato a causa delle impostazioni di Blocco accesso pubblico

La funzione Blocco dell'accesso pubblico Amazon S3 fornisce le impostazioni per i punti di accesso, i bucket e gli account per aiutare a gestire l'accesso pubblico alle risorse Amazon S3. Per ulteriori informazioni su cosa si intende con il termine "pubblico" in Amazon S3, consulta [Significato di "pubblico"](#).

Per impostazione predefinita, i nuovi bucket, punti di accesso e oggetti non consentono l'accesso pubblico. Tuttavia, gli utenti possono modificare le policy di bucket, le policy di punto di accesso, le policy utente IAM, le autorizzazioni degli oggetti o le liste di controllo degli accessi (ACL) per consentire l'accesso pubblico. Le impostazioni di Blocco dell'accesso pubblico S3 annullano queste policy, autorizzazioni e ACL. Da aprile 2023, tutte le impostazioni di Blocco dell'accesso pubblico sono attivate per impostazione predefinita per i nuovi bucket.

Quando Amazon S3 riceve una richiesta di accesso a un bucket o a un oggetto, determina se per il bucket o l'account del proprietario del bucket è applicata un'impostazione di blocco dell'accesso pubblico. Se la richiesta è stata effettuata tramite un punto di accesso, Amazon S3 controlla anche la presenza di impostazioni di blocco dell'accesso pubblico per il punto di accesso. Se è presente un'impostazione di blocco dell'accesso pubblico che vieta l'accesso richiesto, Amazon S3 rifiuta la richiesta.

Il blocco dell'accesso pubblico di Amazon S3 comprende quattro impostazioni. Queste impostazioni sono indipendenti e possono essere usate in qualunque combinazione. Ogni impostazione può essere applicata a un punto di accesso, un bucket o un intero AWS account. Se le impostazioni di blocco dell'accesso pubblico per il punto di accesso, il bucket o l'account differiscono, Amazon S3 applica la combinazione più restrittiva di punto di accesso, bucket e account.

Quando Amazon S3 valuta se un'operazione è vietata da un'impostazione di accesso pubblico al blocco, rifiuta qualsiasi richiesta che violi l'impostazione di un punto di accesso, un bucket o un account.

Le quattro impostazioni fornite da Blocco dell'accesso pubblico Amazon S3 sono le seguenti:

- **BlockPublicAcls** - Questa impostazione si applica alle richieste `PutBucketAcl`, `PutObjectAcl`, `PutObject`, `CreateBucket`, `CopyObject` e `POST Object`. L'impostazione `BlockPublicAcls` causa il seguente comportamento:
 - `PutBucketAcl` e `PutObjectAcl` falliscono se la lista di controllo degli accessi (ACL) specificata è pubblica.
 - `PutObject` fallisce se la richiesta include una ACL pubblica.
 - Se questa impostazione è applicata a un account, le chiamate `CreateBucket` hanno esito negativo con una risposta HTTP 400 (Bad Request) se la richiesta include un'ACL pubblica.

Ad esempio, quando l'accesso è negato per una richiesta `CopyObject` a causa dell'impostazione `BlockPublicAcls`, si riceve il seguente messaggio:

```
An error occurred (AccessDenied) when calling the CopyObject operation:
User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
perform: s3:CopyObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
because public ACLs are prevented by the BlockPublicAcls setting in S3 Block Public
Access.
```

- **IgnorePublicAcls** - L'impostazione `IgnorePublicAcls` fa sì che Amazon S3 ignori tutte le ACL pubbliche su un bucket e sugli oggetti in esso contenuti. Se l'autorizzazione della richiesta è

concessa solo da una ACL pubblica, l'impostazione `IgnorePublicAcls` comporta il rifiuto della richiesta.

Qualsiasi negazione derivante dall'impostazione di `IgnorePublicAcls` è implicita. Ad esempio, se `IgnorePublicAcls` nega una richiesta `GetObject` a causa di una ACL pubblica, si riceve il seguente messaggio:

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no resource-based policy allows the s3:GetObject action
```

- **BlockPublicPolicy** - Questa impostazione si applica alle richieste `PutBucketPolicy` e `PutAccessPointPolicy`.

L'impostazione di `BlockPublicPolicy` per un bucket fa sì che Amazon S3 rifiuti le chiamate a `PutBucketPolicy` se la policy del bucket specificata consente l'accesso pubblico. Questa impostazione fa sì che Amazon S3 rifiuti anche le chiamate a `PutAccessPointPolicy` per tutti i punti di accesso dello stesso account del bucket, se la policy specificata consente l'accesso pubblico.

Impostando `BlockPublicPolicy` per un punto di accesso, Amazon S3 rifiuta le chiamate a `PutAccessPointPolicy` e `PutBucketPolicy` effettuate attraverso il punto di accesso se la policy specificata (per il punto di accesso o il bucket sottostante) consente l'accesso pubblico.

Ad esempio, quando l'accesso viene negato a una richiesta di `PutBucketPolicy` a causa dell'impostazione `BlockPublicPolicy`, si riceve il seguente messaggio:

```
An error occurred (AccessDenied) when calling the PutBucketPolicy operation:
User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
perform: s3:PutBucketPolicy on resource: "arn:aws:s3::amzn-s3-demo-bucket1/object-
name"
because public policies are prevented by the BlockPublicPolicy setting in S3 Block
Public Access.
```

- **RestrictPublicBuckets**— L'impostazione `RestrictPublicBuckets` limita l'accesso a un access point o bucket con una policy pubblica solo ai Servizio AWS principali e agli utenti autorizzati all'interno dell'account del proprietario del bucket e dell'account del proprietario del punto di accesso. Questa impostazione blocca tutti gli accessi tra account all'access point o al bucket (ad eccezione Servizio AWS dei principali), pur consentendo agli utenti all'interno dell'account di gestire l'access point o il bucket. Questa impostazione rifiuta anche tutte le chiamate anonime (o non firmate).

Qualsiasi negazione derivante dall'impostazione di `RestrictPublicBuckets` è esplicita. Ad esempio, se `RestrictPublicBuckets` nega una richiesta di `GetObject` a causa di un bucket pubblico o di una policy del punto di accesso, si riceve il seguente messaggio:

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

Per ulteriori informazioni su queste impostazioni, consultare [the section called “Impostazioni di blocco dell'accesso pubblico”](#). Per rivedere e aggiornare queste impostazioni, consulta [the section called “Configurazione del blocco dell'accesso pubblico”](#).

Accesso negato a causa delle impostazioni Pagamento a carico del richiedente

Se il bucket Amazon S3 a cui si tenta di accedere ha la funzionalità Pagamento a carico del richiedente abilitata, è necessario passare i parametri di richiesta corretti quando si effettuano le richieste a quel bucket. La funzionalità Pagamento a carico del richiedente di Amazon S3 consente al richiedente, anziché al proprietario del bucket, di pagare i costi di trasferimento dei dati e di richiesta per l'accesso agli oggetti nel bucket. Quando `Requester Pays` è abilitato per un bucket, al proprietario del bucket non vengono addebitati costi per le richieste effettuate da altri account. AWS

Se effettui una richiesta a un `Pays-enabled` bucket `Requester` senza superare i parametri necessari, riceverai un errore `Access Denied (403 Forbidden)`. Per accedere agli oggetti in un `Pays-enabled` bucket `Requester`, devi fare quanto segue:

1. Quando si effettuano richieste utilizzando la AWS CLI, è necessario includere il parametro. `--request-payer requester` Ad esempio, per copiare un oggetto con la chiave `object.txt` contenuta nel bucket S3 `s3://amzn-s3-demo-bucket/` in una posizione sul computer locale, è necessario passare il parametro `--request-payer requester` se questo bucket ha il Pagamento a carico del richiedente abilitato.

```
aws s3 cp s3://amzn-s3-demo-bucket/object.txt /local/path \
--request-payer requester
```

2. Quando si effettuano richieste programmatiche utilizzando un AWS SDK, impostate l'`x-amz-request-payer` intestazione sul valore. `requester` Per un esempio, consulta [Download di oggetti dai bucket con pagamento a carico del richiedente](#).

3. È necessario che l'utente o il ruolo IAM che effettua la richiesta disponga delle autorizzazioni richieste per accedere al bucket con Pagamento a carico del richiedente, ad esempio le autorizzazioni `s3:GetObject` e `s3:ListBucket`.

Includendo il `--request-payer requester` parametro o impostando l'`x-amz-request-payer` intestazione, stai comunicando ad Amazon S3 che tu, il richiedente, pagherai i costi associati all'accesso agli oggetti nel bucket Requester Pays-enabled. Questo eviterà l'errore di accesso negato (403 Forbidden).

Policy di bucket e policy IAM

Bucket-level operazioni

Se non è in vigore una policy per i bucket, il bucket consente implicitamente le richieste provenienti da qualsiasi identità AWS Identity and Access Management (IAM) nell'account del proprietario del bucket. Inoltre, il bucket rifiuta implicitamente le richieste provenienti da qualsiasi altra identità IAM da qualsiasi altro account e le richieste anonime (non firmate). Tuttavia, se non esiste una policy per gli utenti IAM, al richiedente (a meno che non sia l'utente Account AWS root) viene implicitamente negato di effettuare richieste. Per ulteriori informazioni su questa logica di valutazione, consulta [Determinazione se una richiesta è consentita o rifiutata in un account](#) nella Guida per l'utente di IAM.

Object-level operazioni

Se l'oggetto è di proprietà dell'account proprietario del bucket, la policy di bucket e la policy degli utenti IAM funzioneranno allo stesso modo per le operazioni a livello di oggetto e per le operazioni a livello di bucket. Ad esempio, se non esiste una policy del bucket, il bucket consente implicitamente le richieste di oggetti da qualsiasi identità IAM nell'account del proprietario del bucket. Inoltre, il bucket rifiuta implicitamente le richieste di oggetti provenienti da qualsiasi altra identità IAM da qualsiasi altro account e le richieste anonime (non firmate). Tuttavia, se non esiste una policy per gli utenti IAM, al richiedente (a meno che non sia l'utente Account AWS root) viene implicitamente negato di effettuare richieste di oggetti.

Se l'oggetto è di proprietà di un account esterno, l'accesso all'oggetto può essere concesso solo tramite le relative liste di controllo degli accessi (ACL). La policy di bucket e la policy degli utenti IAM possono ancora essere utilizzate per rifiutare le richieste di oggetti.

Pertanto, per assicurarsi che la policy del bucket o dell'utente IAM non provochi un errore di Accesso negato (403 Forbidden), verificare che siano soddisfatti i seguenti requisiti:

- Per l'accesso con lo stesso account, non deve esserci un'istruzione Deny esplicita per il richiedente a cui stai cercando di concedere le autorizzazioni nella policy di bucket né nella politica degli utenti IAM. Se desideri concedere le autorizzazioni utilizzando solo la policy di bucket e la policy degli utenti IAM, deve esserci almeno un'istruzione Allow esplicita in una di queste policy.
- Per l'accesso multi-account, non deve essere presente un'istruzione esplicita Deny contro il richiedente a cui si sta cercando di concedere le autorizzazioni, né nella policy del bucket né in quella dell'utente IAM. Per concedere le autorizzazioni per più account utilizzando solo la policy di bucket e la policy utente IAM, assicurati che sia la policy di bucket sia la policy utente IAM del richiedente includano un'istruzione esplicita Allow.

Note

Le istruzioni Allow in una policy di bucket si applicano solo agli oggetti [di proprietà dello stesso account proprietario del bucket](#). Tuttavia, le istruzioni Deny in una policy di bucket si applicano a tutti gli oggetti indipendentemente dalla proprietà dell'oggetto.

Per rivedere o modificare la policy di bucket

Note

Per visualizzare una policy bucket, è necessario disporre dell'autorizzazione. `s3:GetBucketPolicy` Per modificare una policy bucket, è necessario disporre dell'`s3:PutBucketPolicy` autorizzazione.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il nome del bucket per il quale vuoi visualizzare o modificare una policy di bucket.
4. Scegli la scheda Autorizzazioni.
5. In Policy del bucket, scegli Modifica. Viene visualizzata la pagina Modifica la policy del bucket.

Per rivedere la tua policy sui bucket utilizzando AWS Command Line Interface (AWS CLI), usa il [get-bucket-policy](#) comando. Per modificare la tua policy sui bucket, usa il [put-bucket-policy](#) comando.

Note

Se vieni bloccato da un bucket a causa di una policy errata sul bucket, [accedi Console di gestione AWS utilizzando le tue credenziali di utente Account AWS root](#). Per riottenere l'accesso al tuo bucket, assicurati di eliminare la policy errata del bucket utilizzando le credenziali dell'utente Account AWS root.

Suggerimenti per la verifica delle autorizzazioni

Per verificare se il richiedente dispone delle autorizzazioni adeguate per eseguire un'operazione Amazon S3, prova quanto segue:

- Identifica il richiedente. Se si tratta di una richiesta non firmata, significa che è una richiesta anonima senza una policy utente IAM. Se si tratta di una richiesta che utilizza un URL prefirmato, la policy utente è la stessa dell'utente o del ruolo IAM che ha firmato la richiesta.
- Assicurati di utilizzare il ruolo o l'utente IAM corretto. Puoi verificare il tuo utente o ruolo IAM controllando la barra di navigazione della console o utilizzando il comando. [aws sts get-caller-identity](#)
- Controlla tutte le policy IAM collegate al ruolo o all'utente IAM. È possibile utilizzare uno dei seguenti metodi:
 - [Verifica le policy IAM con il simulatore di policy IAM](#).
 - Esamina i vari [tipi di policy IAM](#).
- Se necessario, [modifica la policy utente IAM](#).
- Consulta i seguenti esempi di policy che negano o consentono esplicitamente l'accesso:
 - Policy utente IAM di autorizzazione esplicita: [IAM: consente e rifiuta l'accesso a più servizi a livello di programmazione e nella console](#)
 - Policy di bucket di autorizzazione esplicita: [Concessione delle autorizzazioni a più account per caricare oggetti o impostare le ACL degli oggetti per l'accesso pubblico](#)
 - Politica di negazione esplicita degli utenti IAM [AWS: nega l'accesso a in AWS base alla richiesta Regione AWS](#)
 - Politica esplicita di negazione del bucket: [richiede SSE-KMS tutti gli oggetti scritti in un bucket](#)

Impostazioni ACL di Amazon S3

Quando controlli le impostazioni relative alle liste di controllo degli accessi, [controlla innanzitutto l'impostazione dell'opzione Proprietà dell'oggetto](#) per verificare se le liste di controllo degli accessi sono abilitate nel bucket. Considera che le autorizzazioni ACL possono essere usate solo per concedere autorizzazioni e non possono essere usate per rifiutare richieste. Inoltre, le ACL non possono essere utilizzate per concedere l'accesso a richiedenti che sono rifiutati da dinieghi espliciti nelle policy dei bucket o nelle policy utente IAM.

L'impostazione Proprietà dell'oggetto è impostata su Proprietario del bucket applicato

Se è abilitata l'impostazione Proprietario del bucket applicato, è improbabile che le impostazioni ACL causino un errore di accesso negato (403 Forbidden) perché questa impostazione disabilita tutte le ACL valide per il bucket e gli oggetti. Proprietario del bucket applicato è l'impostazione predefinita (e consigliata) per i bucket Amazon S3.

L'opzione Proprietà dell'oggetto è impostata su Proprietario del bucket preferito o Autore dell'oggetto

Le autorizzazioni ACL continuano a essere valide con l'impostazione Proprietario del bucket preferito o Autore dell'oggetto. Esistono due tipi di ACL: le ACL dei bucket e le ACL degli oggetti. Per informazioni sulle differenze tra questi due tipi di ACL, consulta [Mappatura delle autorizzazioni ACL e delle autorizzazioni della policy di accesso](#).

A seconda dell'azione della richiesta rifiutata, [controlla le autorizzazioni ACL per il bucket o l'oggetto](#):

- Se Amazon S3 ha rifiutato una richiesta LIST, PUT oggetto, GetBucketAcl o PutBucketAcl, [controlla le autorizzazioni ACL per il tuo bucket](#).

Note

Non è possibile concedere le autorizzazioni agli oggetti GET con le impostazioni ACL dei bucket.

- Se Amazon S3 ha rifiutato una richiesta GET per un oggetto S3 o una richiesta [PutObjectAcl](#), [controlla le autorizzazioni ACL per l'oggetto](#).

Important

Se l'account proprietario dell'oggetto è diverso dall'account proprietario del bucket, l'accesso all'oggetto non è controllato dalla policy di bucket.

Risoluzione di un errore di accesso negato (403 proibito) generato da una richiesta di oggetto **GET** durante la proprietà di un oggetto su più account

Esamina le [impostazioni dell'opzione Proprietà dell'oggetto](#) del bucket per determinare il proprietario dell'oggetto. Se hai accesso alle [ACL dell'oggetto](#), puoi anche controllare l'account del proprietario dell'oggetto. (Per visualizzare l'account del proprietario dell'oggetto, controlla l'impostazione ACL dell'oggetto nella console Amazon S3.) In alternativa, puoi anche eseguire una richiesta `GetObjectAcl` per trovare l'[ID canonico](#) del proprietario dell'oggetto per verificare l'account del proprietario. Per impostazione predefinita, le ACL concedono autorizzazioni di tipo autorizzazione esplicita per le richieste GET all'account del proprietario dell'oggetto.

Dopo aver verificato che il proprietario dell'oggetto sia diverso dal proprietario del bucket, a seconda del caso d'uso e del livello di accesso, scegli uno dei seguenti metodi per risolvere l'errore di accesso negato (403 Accesso negato):

- Disabilitare le ACL (consigliato): questo metodo è valido per tutti gli oggetti e può essere eseguito dal proprietario del bucket. Questo metodo assegna automaticamente il ruolo di proprietario del bucket e il controllo completo su ogni oggetto in esso contenuto. Prima di implementare questo metodo, verifica i [prerequisiti per la disabilitazione delle ACL](#). Per informazioni su come impostare il bucket su Proprietario del bucket applicato (scelta consigliata), consulta [Impostazione della proprietà dell'oggetto su un bucket esistente](#).

Important

Per evitare un errore di accesso negato (403 Accesso negato), assicurati di eseguire la migrazione delle autorizzazioni delle liste di controllo degli accessi a una policy di bucket prima di disabilitare le liste. Per ulteriori informazioni, consulta [Esempi di policy di bucket per la migrazione delle autorizzazioni delle ACL](#).

- Cambiare il proprietario dell'oggetto in proprietario del bucket: questo metodo può essere applicato a singoli oggetti, ma solo il proprietario dell'oggetto (o un utente con le autorizzazioni appropriate) può modificare la proprietà di un oggetto. Potrebbero essere applicati costi aggiuntivi a PUT. Per ulteriori informazioni, consulta la pagina [Prezzi di Amazon S3](#). Questo metodo garantisce al proprietario del bucket la piena proprietà dell'oggetto, consentendogli di controllare l'accesso all'oggetto tramite una policy di bucket.

Per modificare la proprietà dell'oggetto, procedi in uno dei seguenti modi:

- Tu (il proprietario del bucket) puoi [copiare nuovamente l'oggetto](#) nel bucket.

- È possibile modificare l'impostazione Proprietà dell'oggetto per il bucket impostandola su Proprietario del bucket preferito. Se il controllo delle versioni è disabilitato, gli oggetti nel bucket vengono sovrascritti. Se il controllo delle versioni è abilitato, nel bucket verranno visualizzate versioni duplicate dello stesso oggetto, per le quali il proprietario può [impostare una regola del ciclo di vita per la scadenza](#). Per istruzioni su come modificare le impostazioni dell'opzione Proprietà dell'oggetto, consulta [Impostazione di Object Ownership su un bucket esistente](#).

 Note

Quando si aggiorna l'impostazione Proprietà dell'oggetto impostandola su Proprietario del bucket preferito, l'impostazione viene applicata solo ai nuovi oggetti caricati nel bucket.

- È possibile fare in modo che il proprietario dell'oggetto carichi nuovamente l'oggetto con l'ACL bucket-owner-full-control predefinita dell'oggetto.

 Note

Per i caricamenti multi-account, nella tua policy di bucket dovrai disporre anche dell'ACL bucket-owner-full-control dell'oggetto predefinito. Per una policy di bucket di esempio, consulta [Concedere autorizzazioni multi-account per il caricamento di oggetti a garanzia del controllo completo da parte del proprietario del bucket](#).

- Mantenere l'autore dell'oggetto come proprietario dell'oggetto: questo metodo non modifica il proprietario dell'oggetto, ma consente di concedere l'accesso agli oggetti singolarmente. Per concedere l'accesso a un oggetto, devi disporre dell'autorizzazione PutObjectACL per l'oggetto. Quindi, per correggere l'errore di accesso negato (403 Accesso negato), aggiungi il richiedente come [utente autorizzato](#) per accedere all'oggetto nelle relative ACL. Per ulteriori informazioni, consulta [Configurazione delle ACL](#).

Impostazioni dell'opzione S3 Blocco dell'accesso pubblico

Se la richiesta fallita riguarda l'accesso pubblico o le policy pubbliche, controllare le impostazioni di Blocco dell'accesso pubblico S3 sull'account, sul bucket o sul punto di accesso. Per ulteriori informazioni sulla risoluzione dei problemi relativi agli errori di accesso negato relativi alle impostazioni di Blocco dell'accesso pubblico S3, consulta [the section called "Accesso negato a causa delle impostazioni di Blocco accesso pubblico"](#).

Impostazioni della crittografia Amazon S3

Amazon S3 supporta la crittografia lato server sul tuo bucket. Server-side la crittografia è la crittografia dei dati a destinazione da parte dell'applicazione o del servizio che li riceve. Amazon S3 crittografa i tuoi dati a livello di oggetto mentre li scrive sui dischi AWS dei data center e li decrittografa automaticamente quando accedi ad essi.

Per impostazione predefinita, Amazon S3 ora applica la crittografia lato server con le chiavi gestite da Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. Amazon S3 consente inoltre di specificare il metodo di crittografia lato server durante il caricamento degli oggetti.

Per esaminare lo stato della crittografia lato server e le impostazioni della crittografia del bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket, scegli il bucket per cui vuoi controllare le impostazioni della crittografia.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri verso il basso fino alla sezione Crittografia predefinita e visualizza le impostazioni dell'opzione Tipo di crittografia.

Per verificare le impostazioni di crittografia utilizzando il comando AWS CLI, usa il [get-bucket-encryption](#) comando.

Per controllare lo stato della crittografia dell'oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il nome del bucket contenente l'oggetto.
4. Nell'elenco Nome scegli il nome dell'oggetto per cui desideri aggiungere o modificare la crittografia.

Viene visualizzata la pagina dei dettagli dell'oggetto.

5. Scorri verso il basso fino alla sezione delle impostazioni di Server-side crittografia per visualizzare le impostazioni di crittografia lato server dell'oggetto.

Per verificare lo stato di crittografia dell'oggetto utilizzando il comando AWS CLI, usa il [head-object](#) comando.

Requisiti relativi a crittografia e autorizzazioni

Amazon S3 supporta tre tipi di crittografia lato server:

- Server-side crittografia con chiavi gestite da Amazon S3 () SSE-S3
- Server-side crittografia con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS)
- Server-side crittografia con chiavi fornite dal cliente () SSE-C

In base alle impostazioni di crittografia correnti, verifica che siano soddisfatti i seguenti requisiti relativi alle autorizzazioni:

- SSE-S3— Non sono richieste autorizzazioni aggiuntive.
- SSE-KMS (con una chiave gestita dal cliente): per caricare oggetti, AWS KMS key è richiesta l'`kms:GenerateDataKey` autorizzazione. Per scaricare oggetti ed eseguire caricamenti di oggetti in più parti, è necessaria l'autorizzazione `kms:Decrypt` per la chiave KMS.
- SSE-KMS (con un Chiave gestita da AWS) — Il richiedente deve provenire dallo stesso account che possiede la chiave `aws/s3` KMS. Il richiedente deve inoltre disporre delle autorizzazioni Amazon S3 corrette per accedere all'oggetto.
- SSE-C (con una chiave fornita dal cliente): non sono richieste autorizzazioni aggiuntive. Puoi configurare la policy di bucket per [richiedere e limitare la crittografia lato server con chiavi di crittografia fornite dal cliente](#) per gli oggetti nel bucket.

Se l'oggetto è crittografato con una chiave gestita dal cliente, assicurati che la policy della chiave KMS ti consenta di eseguire le operazioni `kms:GenerateDataKey` o `kms:Decrypt`. Per istruzioni su come verificare la policy della chiave KMS, consulta [Visualizzazione di una policy di chiave](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Impostazioni dell'opzione S3 Blocco oggetti

Se il bucket ha [S3 Object Lock](#) abilitato e l'oggetto è protetto da un [periodo di conservazione](#) o da un [blocco legale](#) e si tenta di eliminare un oggetto, Amazon S3 restituisce una delle seguenti risposte, a seconda di come si cerca di eliminare l'oggetto:

- Richiesta **DELETE** permanente: se viene inviata una richiesta DELETE permanente (una richiesta che specifica un ID di versione), Amazon S3 restituisce un errore di accesso negato (403 Forbidden) quando si tenta di eliminare l'oggetto.
- Richiesta **DELETE** semplice: se viene inviata una richiesta DELETE semplice (una richiesta che non specifica un ID di versione), Amazon S3 restituisce una risposta 200 OK e inserisce un [indicatore di eliminazione](#) nel bucket, che diventa la versione corrente dell'oggetto con un nuovo ID.

Per verificare se l'opzione Blocco oggetti è abilitata per il bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il nome del bucket da controllare.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri verso il basso fino alla sezione Blocco oggetti. Verifica se l'impostazione dell'opzione Blocco oggetti è abilitata o disabilitata.

Per determinare se l'oggetto è protetto da un periodo di conservazione o da un blocco a fini legali, [visualizza le informazioni relative al blocco](#) dell'oggetto.

Se l'oggetto è protetto da un periodo di conservazione o da un blocco a fini legali, verifica quanto segue:

- Se la versione dell'oggetto è protetta dalla modalità di conservazione della conformità, non è possibile eliminarla definitivamente. Una DELETE richiesta permanente da parte di qualsiasi richiedente, incluso l'utente Account AWS root, genererà un errore di accesso negato (403 Forbidden). Inoltre, considera che quando invii una richiesta DELETE per un oggetto protetto dalla modalità di conservazione della conformità, Amazon S3 crea un [contrassegno di eliminazione](#) per l'oggetto.
- Se la versione dell'oggetto è protetta con la modalità di conservazione della governance e disponi dell'autorizzazione `s3:BypassGovernanceRetention`, è possibile aggirare la protezione ed eliminare definitivamente la versione. Per ulteriori informazioni, consulta [Bypassare la modalità Governance](#).
- Se la versione dell'oggetto è protetta da un blocco a fini legali, una richiesta DELETE permanente può generare un errore di accesso negato (403 Accesso negato). Per eliminare

definitivamente la versione dell'oggetto, è necessario rimuovere il blocco a fini legali applicato alla versione dell'oggetto. Per rimuovere un blocco a fini legali, devi disporre dell'autorizzazione `s3:PutObjectLegalHold`. Per ulteriori informazioni sulla rimozione di un blocco a fini legali, consulta [Configurazione di S3 Object Lock](#).

Policy di endpoint VPC

Se si accede ad Amazon S3 utilizzando un endpoint di cloud privato virtuale (VPC), assicurarsi che la policy dell'endpoint VPC non blocchi l'accesso alle risorse di Amazon S3. Per impostazione predefinita, la policy degli endpoint VPC consente di eseguire tutte le richieste indirizzate ad Amazon S3. È inoltre possibile configurare la policy degli endpoint VPC per limitare determinate richieste. Per informazioni su come controllare le policy degli endpoint VPC, consulta le seguenti risorse:

- [the section called “Accesso negato a causa di una policy dell'endpoint VPC: diniego implicito”](#)
- [the section called “Accesso negato a causa di una policy dell'endpoint VPC: diniego esplicito”](#)
- [Controllo dell'accesso agli endpoint VPC utilizzando le policy degli endpoint](#) nella Guida a AWS PrivateLink

AWS Organizations policies

Se Account AWS appartieni a un'organizzazione, AWS Organizations le policy possono impedirti di accedere alle risorse di Amazon S3. Per impostazione predefinita, AWS Organizations le policy non bloccano alcuna richiesta ad Amazon S3. Tuttavia, assicurati che AWS Organizations le tue policy non siano state configurate per bloccare l'accesso ai bucket S3. Per istruzioni su come controllare le tue AWS Organizations policy, consulta le seguenti risorse:

- [the section called “Accesso negato a causa di una policy di controllo dei servizi: diniego implicito”](#)
- [the section called “Accesso negato a causa di una policy di controllo dei servizi: diniego esplicito”](#)
- [the section called “Accesso negato a causa di una policy di controllo delle risorse - rifiuto esplicito”](#)
- [Elenco di tutte le policy](#) nella Guida all'utente di AWS Organizations

Inoltre, se si è configurato in modo errato la policy del bucket per un account membro in modo da negare a tutti gli utenti l'accesso al bucket S3, è possibile sbloccare il bucket avviando una sessione privilegiata per l'account membro in IAM. Una volta avviata una sessione privilegiata, è possibile eliminare la policy di bucket configurata in modo errato per riottenere l'accesso al bucket. Per ulteriori

informazioni, consulta [Eseguire un'operazione privilegiata su un account AWS Organizations membro](#) nella Guida per l'AWS Identity and Access Management utente.

CloudFront accesso alla distribuzione

Se ricevi un errore di accesso negato (403 Forbidden) quando provi ad accedere al tuo sito web statico S3 tramite CloudFront, verifica questi problemi comuni:

- Il nome di dominio di origine è nel formato corretto?
 - Assicurati di utilizzare il formato dell'endpoint del sito web S3 (bucket-name.s3-website-region.amazonaws.com) anziché l'endpoint della REST API
 - Verifica che l'hosting di siti web statici sia abilitato nel bucket
- La tua policy sui bucket consente l'accesso? CloudFront
 - Assicurati che la tua policy bucket includa le autorizzazioni per Origin Access Identity (OAI) o Origin Access Control (OAC) della tua CloudFront distribuzione
 - Verifica che la policy includa le autorizzazioni s3: richieste GetObject

Per ulteriori passaggi e configurazioni di risoluzione dei problemi, tra cui le impostazioni della pagina di errore e le impostazioni del protocollo, vedi [Perché ricevo un errore «403 accesso negato» quando utilizzo un endpoint del sito Web Amazon S3 come origine della mia distribuzione? CloudFront](#) nel AWS re:Post Knowledge Center.

Note

Questo errore è diverso dagli errori 403 che potresti ricevere accedendo direttamente a S3. In caso di CloudFront-specific problemi, assicurati di controllare sia le impostazioni di CloudFront distribuzione che le configurazioni di S3.

Impostazioni del punto di accesso

Se ricevi un errore di accesso negato (403 Accesso negato) mentre effettui richieste tramite i punti di accesso Amazon S3, potresti dover controllare quanto segue:

- Le configurazioni per i punti di accesso
- La policy utente IAM utilizzata per i punti di accesso
- La policy di bucket utilizzata per gestire o configurare i punti di accesso multi-account

Configurazioni e policy dei punti di accesso

- Quando si crea un punto di accesso, è possibile scegliere di impostare Internet o VPC come origine della rete. Se l'origine della rete è impostata su "Solo VPC", Amazon S3 rifiuterà tutte le richieste effettuate al punto di accesso che non provengono dal VPC specificato. Per verificare l'origine della rete del punto di accesso, consulta [Creazione di access point limitati a un cloud privato virtuale](#).
- Con i punti di accesso, puoi anche configurare impostazioni personalizzate dell'opzione Blocco dell'accesso pubblico, che funzionano in modo simile alle impostazioni di Blocco dell'accesso pubblico a livello di bucket o account. Per verificare le impostazioni personalizzate dell'opzione Blocco dell'accesso pubblico, consulta [Gestione dell'accesso pubblico ai punti di accesso per bucket per uso generico](#).
- Per effettuare con successo richieste ad Amazon S3 utilizzando i punti di accesso, assicurati che il richiedente disponga delle autorizzazioni IAM necessarie. Per ulteriori informazioni, consulta [Configurazione delle policy IAM per l'utilizzo degli access point](#).
- Se la richiesta interessa punti di accesso multi-account, assicurati che il proprietario del bucket abbia aggiornato la policy di bucket per autorizzare le richieste provenienti dal punto di accesso. Per ulteriori informazioni, consulta [Concessione delle autorizzazioni per i punti di accesso multi-account](#).

Se l'errore Access Denied (403 Forbidden) persiste anche dopo aver controllato tutti gli elementi di questo argomento, [recupera l'ID](#) della tua richiesta Amazon S3 e contattaci per ulteriori indicazioni. Supporto

Risorse aggiuntive

Per ulteriori indicazioni sugli errori di accesso negato (403 Forbidden), consulta le seguenti risorse:

- [Come posso risolvere gli errori 403 Access Denied di Amazon S3?](#) nel Knowledge Center. AWS re:Post
- [Perché ricevo un "403 Forbidden" errore quando provo a caricare file in Amazon S3?](#) nel AWS re:Post Knowledge Center.
- [Perché ricevo un errore di accesso negato quando cerco di accedere a una risorsa Amazon S3 nella stessa Account AWS?](#) nel AWS re:Post Knowledge Center.
- [Perché ricevo un errore di accesso negato quando cerco di accedere a un bucket Amazon S3 con accesso pubblico in lettura?](#) nel AWS re:Post Knowledge Center.

- [Perché ricevo un errore di «mancata corrispondenza della firma» quando cerco di utilizzare un URL prefirmato per caricare un oggetto su Amazon S3?](#) nel Knowledge Center. AWS re:Post
- [Perché ricevo un errore di accesso negato per la versione ListObjects V2 quando eseguo il comando sync sul mio bucket Amazon S3?](#) nel Knowledge Center. AWS re:Post
- [Perché ricevo l'errore «403 access denied» quando utilizzo un endpoint del sito Web Amazon S3 come origine della mia distribuzione? CloudFront](#) nel Knowledge Center. AWS re:Post

AWS politiche gestite per Amazon S3

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. AWS le policy gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una policy AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui la policy è associata. AWS è più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AmazonS3FullAccess

È possibile allegare la policy AmazonS3FullAccess alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso completo ad Amazon S3.

Per visualizzare le autorizzazioni per questa policy, consulta [AmazonS3FullAccess](#) in Console di gestione AWS.

AWS politica gestita: AmazonS3ReadOnlyAccess

È possibile allegare la policy AmazonS3ReadOnlyAccess alle identità IAM. Questa policy concede le autorizzazioni che consentono l'accesso in sola lettura ad Amazon S3.

Per visualizzare le autorizzazioni per questa policy, consulta [AmazonS3ReadOnlyAccess](#) in Console di gestione AWS.

AWS politica gestita: AmazonS3ObjectLambdaExecutionRolePolicy

Fornisce AWS Lambda alle funzioni le autorizzazioni necessarie per inviare dati a S3 Object Lambda quando le richieste vengono effettuate a un punto di accesso S3 Object Lambda. Concede inoltre a Lambda le autorizzazioni per scrivere su Amazon logs. CloudWatch

Per visualizzare le autorizzazioni per questa policy, consulta [AmazonS3ObjectLambdaExecutionRolePolicy](#) in Console di gestione AWS.

AWS politica gestita: S3UnlockBucketPolicy

Se hai configurato erroneamente la policy del bucket per un account membro per negare a tutti gli utenti l'accesso al bucket S3, puoi utilizzare questa policy AWS gestita (S3UnlockBucketPolicy) per sbloccare il bucket. Per ulteriori informazioni su come rimuovere una policy bucket configurata in modo errato che impedisce a tutti i principali di accedere a un bucket Amazon S3, consulta [Eseguire un'attività privilegiata su un account membro nella Guida per l'utente. AWS Organizations](#) AWS Identity and Access Management

Amazon S3 si aggiorna a AWS policy gestite

Visualizza i dettagli sugli aggiornamenti delle policy AWS gestite per Amazon S3 da quando questo servizio ha iniziato a tracciare queste modifiche.

Modifica	Descrizione	Data
Amazon S3 ha aggiunto S3UnlockBucketPolicy	Amazon S3 ha aggiunto una nuova policy AWS gestita chiamata S3UnlockBucketPolicy per sbloccare un bucket e rimuovere una policy di bucket mal configurata che impedisce a tutti i principali di accedere a un bucket Amazon S3.	1 novembre 2024
Amazon S3 ha aggiunto le autorizzazioni Descrivi a	Amazon S3 ha aggiunto le autorizzazioni s3:Descr	11 agosto 2023

Modifica	Descrizione	Data
AmazonS3ReadOnlyAccess	be* a AmazonS3ReadOnlyAccess .	
Amazon S3 ha aggiunto le autorizzazioni per S3 Object Lambda AmazonS3FullAccess e AmazonS3ReadOnlyAccess	Amazon S3 ha aggiornato le policy AmazonS3FullAccess e AmazonS3ReadOnlyAccess in modo da includere le autorizzazioni per S3 Object Lambda.	27 settembre 2021
Amazon S3 ha aggiunto AmazonS3ObjectLambdaExecutionRolePolicy	Amazon S3 ha aggiunto una nuova policy AWS gestita denominata AmazonS3ObjectLambdaExecutionRolePolicy che fornisce alle funzioni Lambda le autorizzazioni per interagire con S3 Object Lambda e scrivere nei log. CloudWatch	18 agosto 2021
Amazon S3 ha iniziato a tenere traccia delle modifiche	Amazon S3 ha iniziato a tracciare le modifiche per le sue policy gestite. AWS	18 agosto 2021

Gestione dell'accesso a set di dati condivisi con punti di accesso

I punti di accesso Amazon S3 semplificano l'accesso ai dati per qualsiasi AWS servizio o applicazione per i clienti che archivia i dati in S3. I punti di accesso sono denominati endpoint di rete collegati a un'origine dati come un bucket, un volume Amazon FSx for NetApp ONTAP, un volume Amazon FSx per OpenZFS o un punto di ripristino Amazon S3 in. AWS Backup Per informazioni sull'utilizzo di bucket, consulta [Panoramica dei bucket per uso generico](#). Per informazioni su come lavorare con FSx for NetApp ONTAP, consulta [What is Amazon FSx for ONTAP nella FSx for ONTAP User Guide. NetApp](#). Per informazioni sull'utilizzo di FSx for OpenZFS, consulta [What is Amazon FSx for OpenZFS nella Guida per l'utente di FSx for OpenZFS](#). Un punto di ripristino (o backup) di Amazon S3 rappresenta il contenuto di un bucket S3 in un determinato momento,

creato da AWS Backup. Per informazioni sull'utilizzo dei backup di Amazon S3, consulta i backup di [Amazon S3 nella Developer Guide](#). AWS Backup

È possibile utilizzare i punti di accesso per eseguire operazioni sugli oggetti S3, ad esempio `GetObject` e `PutObject`. Ogni access point dispone di autorizzazioni e controlli di rete distinti che S3 applica per qualsiasi richiesta effettuata tramite l'access point in questione. Ogni endpoint applica una policy di punto di accesso personalizzata che consente di controllare l'utilizzo per risorsa, utente o altre condizioni. Se il punto di accesso è collegato a un bucket, la policy del punto di accesso funziona insieme alla policy di bucket sottostante. È possibile configurare qualsiasi punto di accesso in modo che accetti richieste solo da un cloud privato virtuale (VPC) per limitare l'accesso ai dati Amazon S3 a una rete privata. È inoltre possibile configurare le impostazioni di blocco dell'accesso pubblico personalizzate per ciascun access point.

Note

Puoi utilizzare gli access point solo per eseguire le operazioni sugli oggetti. Non è possibile utilizzare i punti di accesso per eseguire altre operazioni Amazon S3, come l'eliminazione di bucket o la creazione di configurazioni di replica S3. Per un elenco completo delle operazioni S3 che supportano i punti di accesso, consulta [Compatibilità dei punti di accesso](#).

Gli argomenti di questa sezione spiegano come utilizzare i punti di accesso Amazon S3. Per argomenti sull'uso dei punti di accesso con i bucket di directory, consulta [Gestione dell'accesso ai set di dati condivisi in bucket di directory con punti di accesso](#).

Argomenti

- [Regole di denominazione, restrizioni e limitazioni dei punti di accesso](#)
- [Riferimento ai punti di accesso con ARN, alias di punti di accesso o URI virtual-hosted-style](#)
- [Compatibilità dei punti di accesso](#)
- [Configurazione delle policy IAM per l'utilizzo degli access point](#)
- [Monitoraggio e registrazione degli access point](#)
- [Creazione di un access point](#)
- [Gestione dei punti di accesso Amazon S3 per bucket per uso generico](#)
- [Utilizzo dei punti di accesso Amazon S3 per bucket per uso generico](#)
- [Utilizzo di tag con punti di accesso S3 per bucket per uso generico](#)

Regole di denominazione, restrizioni e limitazioni dei punti di accesso

I punti di accesso sono denominati endpoint di rete collegati a un bucket, a un volume su un file system Amazon FSx o a un punto di ripristino Amazon S3 e semplificano la gestione dei dati. AWS Backup Quando crei un punto di accesso, scegli un nome e il nome in cui Regione AWS crearlo. I seguenti argomenti forniscono informazioni sulle regole di denominazione dei punti di accesso, restrizioni e limitazioni.

Argomenti

- [Regole di denominazione dei punti di accesso](#)
- [Restrizioni e limitazioni dei punti di accesso](#)
- [Restrizioni e limitazioni dei punti di accesso collegati a un volume su un file system Amazon FSx](#)
- [Restrizioni e limitazioni per i punti di accesso collegati a un punto di ripristino Amazon S3 in AWS Backup](#)

Regole di denominazione dei punti di accesso

Quando si crea un punto di accesso, si sceglie il nome e il nome in Regione AWS cui crearlo. A differenza dei bucket generici, i nomi dei punti di accesso non devono essere univoci tra Account AWS o Regioni AWS. Lo stesso Account AWS può creare punti di accesso con lo stesso nome in diversi Regioni AWS o due diversi Account AWS può utilizzare lo stesso nome del punto di accesso. Tuttavia, all'interno di Regione AWS un singolo uomo non Account AWS possono essere presenti due punti di accesso con lo stesso nome.

Note

Se scegli di pubblicizzare il nome del punto di accesso, è consigliabile evitare di includere informazioni sensibili nel nome del punto di accesso. I nomi dei punti di accesso vengono pubblicati in un database accessibile pubblicamente noto come sistema dei nomi di dominio (DNS).

I nomi dei punti di accesso devono DNS-compliant e devono soddisfare le seguenti condizioni:

- Devono essere univoci all'interno di un unico Account AWS e Regione AWS
- Devono iniziare con un numero o una lettera minuscola
- Devono contenere da 3 a 50 caratteri

- Non possono iniziare o terminare con un trattino (-).
- Non possono contenere caratteri di sottolineatura (_), lettere maiuscole, spazi o punti (.).
- Non possono terminare con il suffisso -s3alias o -ext-s3alias. Questi suffissi sono riservati ai nomi di alias dei punti di accesso. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

Restrizioni e limitazioni dei punti di accesso

Gli Punti di accesso Amazon S3 presentano le seguenti restrizioni e limitazioni:

- Ogni punto di accesso è associato esattamente a un solo bucket o volume FSx per OpenZFS. È necessario specificare questa associazione quando si crea il punto di accesso. Dopo aver creato un punto di accesso, non è possibile associarlo a un bucket o a un volume FSx per OpenZFS diverso. Tuttavia, è possibile eliminare il punto di accesso e quindi crearne un altro con lo stesso nome.
- Dopo aver creato un access point, non è possibile modificarne la configurazione del cloud privato virtuale (VPC).
- Le policy access point sono limitate a una dimensione di 20 KB.
- È possibile creare un massimo di 10.000 punti di accesso per Account AWS persona Regione AWS. Se hai bisogno di più di 10.000 punti di accesso per un singolo account in una singola Regione, puoi richiedere un aumento della quota di servizio. Per ulteriori informazioni su Service Quotas e la richiesta di un aumento, consultare [AWS Service Quotas](#) in Riferimenti generali di AWS.
- Non è possibile utilizzare un punto di accesso come destinazione della replica S3. Per ulteriori informazioni sulla replica, consulta [Replica di oggetti all'interno e tra le Regioni](#).
- Non è possibile utilizzare gli alias dei punti di accesso S3 come origine o destinazione per le operazioni di spostamento nella console Amazon S3.
- Puoi indirizzare i punti di accesso solo utilizzando URL in stile host virtuale. Per ulteriori informazioni sull'indirizzamento in stile hosting virtuale, consulta [Accesso a un bucket per uso generico Amazon S3](#).
- Le operazioni API che controllano la funzionalità dei punti di accesso (ad esempio, PutAccessPoint e GetAccessPointPolicy) non supportano le chiamate multi-account.
- È necessario utilizzare AWS la versione 4 di Signature quando si effettuano richieste a un punto di accesso utilizzando le API REST. Per ulteriori informazioni sull'autenticazione delle richieste, consulta [Authenticating Requests \(AWS Signature Version 4\)](#) nel Amazon Simple Storage Service API Reference.

- I punti di accesso supportano solo le richieste tramite HTTPS. Amazon S3 risponderà automaticamente con un reindirizzamento HTTP per qualsiasi richiesta effettuata tramite HTTP, per aggiornare la richiesta a HTTPS.
- Gli access point non supportano l'accesso anonimo.
- Dopo aver creato un punto di accesso, non è più possibile modificare le impostazioni di blocco dell'accesso pubblico.
- Cross-account i punti di accesso non ti concedono l'accesso ai dati finché non ti vengono concesse le autorizzazioni dal proprietario del bucket. Il proprietario del bucket mantiene sempre il massimo controllo sui dati e deve aggiornare la policy di bucket per autorizzare le richieste provenienti dal punto di accesso multi-account. Per un esempio di policy di bucket, consulta [Configurazione delle policy IAM per l'utilizzo degli access point](#).
- Regioni AWS Se hai più di 1.000 punti di accesso, non puoi cercare un punto di accesso per nome nella console Amazon S3.
- Quando visualizzi un punto di accesso multi-account nella console Amazon S3, la colonna Accesso mostra Sconosciuto. La console Amazon S3 non è in grado di determinare se l'accesso pubblico è concesso per il bucket e gli oggetti associati. A meno che non sia necessaria una configurazione pubblica per un caso d'uso specifico, si consiglia all'utente e al proprietario del bucket di bloccare tutti gli accessi pubblici al punto di accesso e al bucket. Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Restrizioni e limitazioni dei punti di accesso collegati a un volume su un file system Amazon FSx

Di seguito sono riportate le limitazioni specifiche relative all'utilizzo dei punti di accesso collegati a un volume su un file system Amazon FSx:

- Quando si creano punti di accesso, è possibile collegare il punto di accesso solo a un volume su un file system Amazon FSx di cui si è proprietari. Non puoi collegarti a un volume di proprietà di un altro Account AWS.
- Non è possibile utilizzare l'API `CreateAccessPoint` per creare e collegare un punto di accesso a un volume su un file system Amazon FSx. È necessario utilizzare l'API [CreateAndAttachS3AccessPoint](#).
- Non è possibile disattivare le impostazioni di blocco dell'accesso pubblico quando si crea o si utilizza un punto di accesso collegato a un volume su un file system Amazon FSx.

- Non è possibile elencare oggetti o utilizzare le operazioni Copia o Sposta nella console S3 con punti di accesso collegati a un volume su un file system Amazon FSx.
- CopyObject è supportato per i punti di accesso collegati a un volume FSx for NetApp ONTAP o FSx for OpenZFS solo se l'origine e la destinazione sono lo stesso punto di accesso. Per ulteriori informazioni sulla compatibilità dei punti di accesso, consulta [Compatibilità dei punti di accesso](#).
- I caricamenti multiparte sono limitati a 5 GB.
- Il supporto per il tipo di distribuzione e la classe di storage di FSx for OpenZFS varia in base. Regione AWS Per ulteriori informazioni, consulta [Disponibilità in base alla Regione AWS](#) nella Guida per l'utente di OpenZFS.

Restrizioni e limitazioni per i punti di accesso collegati a un punto di ripristino Amazon S3 in AWS Backup

Le seguenti sono limitazioni specifiche quando si utilizzano punti di accesso collegati a un punto di ripristino S3 in: AWS Backup

- I punti di accesso per i punti di ripristino S3 sono di sola lettura. Le operazioni di scrittura come PutObjectDeleteObject, CopyObject e i caricamenti in più parti non sono supportate.
- Usa l' AWS Backup CreateBackupAccessPointAPI o la AWS Backup console per creare punti di accesso. L>CreateAccessPointAPI S3 non è supportata.
- Per eliminare questi punti di accesso utilizza l' AWS Backup DeleteBackupAccessPointAPI o la AWS Backup console.
- Ogni account può avere fino a 5 punti di accesso per punto di ripristino, indipendentemente dallo stato.
- I nomi dei punti di accesso condividono lo spazio dei nomi dei punti di accesso S3. Un nome utilizzato da un punto di accesso di backup non può essere riutilizzato per un punto di accesso S3 standard nello stesso account e nella stessa regione.
- Per ulteriori informazioni, consulta i punti [di accesso di backup](#) nella Guida per gli AWS Backup sviluppatori.

Riferimento ai punti di accesso con ARN, alias di punti di accesso o URI virtual-hosted-style

Dopo aver creato un punto di accesso, è possibile utilizzare questi endpoint per eseguire una serie di operazioni. Quando si fa riferimento a un punto di accesso, è possibile utilizzare il nome della risorsa Amazon (ARN), l'alias del punto di accesso o l'URI virtual-hosted-style.

Argomenti

- [ARN del punto di accesso](#)
- [Alias del punto di accesso](#)
- [Virtual-hosted—style URI](#)

ARN del punto di accesso

I punti di accesso hanno il nome della risorsa Amazon (ARN). Gli ARN degli access point sono simili agli ARN bucket, ma sono digitati in modo esplicito e codificano gli access point Regione AWS e l'Account AWS ID del proprietario del punto di accesso. Per maggiori informazioni sugli ARN, consulta [Identificare le risorse AWS con nomi della risorsa Amazon \(ARN\)](#) nella Guida per l'utente IAM.

Gli ARN dei punti di accesso utilizzano il seguente formato:

```
arn:aws:s3:region:account-id:accesspoint/resource
```

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test` rappresenta il punto di accesso denominato *test*, di proprietà dell'account *123456789012* nella Regione *us-west-2*.
- `arn:aws:s3:us-west-2:123456789012:accesspoint/*` rappresenta tutti i punti di accesso nell'account *123456789012* nella Regione *us-west-2*.

Gli ARN per gli oggetti a cui si accede tramite un punto di accesso utilizzano il seguente formato:

```
arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource
```

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/unit-01` rappresenta l'oggetto *unit-01*, a cui si accede attraverso il punto di accesso denominato *test*, posseduto dall'account *123456789012* nella Regione *us-west-2*.

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/*` rappresenta tutti gli oggetti per il punto di accesso denominato `test` nell'account `123456789012` nella Regione `us-west-2`.
- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/unit-01/finance/*` rappresenta tutti gli oggetti sotto il prefisso `unit-01/finance/` per il punto di accesso denominato `test` nell'account `123456789012` nella Regione `us-west-2`.

Alias del punto di accesso

Quando crei un punto di accesso, Amazon S3 genera automaticamente un alias che puoi utilizzare al posto di un nome bucket Amazon S3 per l'accesso ai dati. Puoi utilizzare questo alias del punto di accesso al posto di un nome della risorsa Amazon (ARN) per qualsiasi operazione del piano dati del punto di accesso. Per un elenco di queste operazioni, consulta [Compatibilità dei punti di accesso](#).

Un nome alias punto di accesso viene creato nello stesso spazio dei nomi di un bucket Amazon S3. Questo nome alias viene generato automaticamente e non può essere modificato. Un nome alias del punto di accesso soddisfa tutti i requisiti di un nome bucket Amazon S3 valido e comprende le seguenti parti:

ACCESS POINT NAME-METADATA-s3alias (per punti di accesso collegati a un bucket Amazon S3)

ACCESS POINT NAME-METADATA-ext-s3alias (per punti di accesso collegati a un'origine dati bucket non S3)

Note

I suffissi `-s3alias` e `-ext-s3alias` sono riservati ai nomi alias dei punti di accesso e non possono essere utilizzati per i nomi dei bucket o dei punti di accesso. Per ulteriori informazioni sulle regole di denominazione dei bucket Amazon S3, consulta [Regole di denominazione dei bucket per uso generico](#).

Casi d'uso e limitazioni degli alias dei punti di accesso

Quando si adottano i punti di accesso, è possibile utilizzare nomi alias dei punti di accesso senza richiedere modifiche estese di codice.

Quando crei un punto di accesso, Amazon S3 genera automaticamente un nome alias del punto di accesso, come mostrato nell'esempio seguente. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control create-access-point --bucket amzn-s3-demo-bucket1 --name my-access-point
--account-id 111122223333
{
  "AccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-access-point",
  "Alias": "my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-s3alias"
}
```

Puoi utilizzare questo nome alias del punto di accesso invece di un nome bucket Amazon S3 in qualsiasi operazione del piano dati. Per un elenco di queste operazioni, consulta [Compatibilità dei punti di accesso](#).

L'AWS CLI esempio seguente del `get-object` comando utilizza l'alias del punto di accesso del bucket per restituire informazioni sull'oggetto specificato. Per eseguire questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api get-object --bucket my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-
s3alias --key dir/my_data.rtf my_data.rtf
{
  "AcceptRanges": "bytes",
  "LastModified": "2020-01-08T22:16:28+00:00",
  "ContentLength": 910,
  "ETag": "\"00751974dc146b76404bb7290f8f51bb\"",
  "VersionId": "null",
  "ContentType": "text/rtf",
  "Metadata": {}
}
```

Limitazioni degli alias del punto di accesso

- Gli alias non possono essere configurati dai clienti.
- Gli alias non possono essere eliminati, modificati o disabilitati in un punto di accesso.
- È possibile utilizzare questo nome di alias del punto di accesso al posto di un nome di bucket Amazon S3 in alcune operazioni del piano dati. Per un elenco di queste operazioni, consulta [Compatibilità dei punti di accesso con le operazioni S3](#).

- Non puoi utilizzare un nome alias del punto di accesso per le operazioni del piano di controllo Amazon S3. Per un elenco delle operazioni del piano di controllo Amazon S3, consulta [Controllo Amazon S3](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.
- Non è possibile utilizzare gli alias dei punti di accesso S3 come origine o destinazione per le operazioni di spostamento nella console Amazon S3.
- Gli alias non possono essere utilizzati nelle policy AWS Identity and Access Management (IAM).
- Gli alias non possono essere utilizzati come destinazione di registrazione per i log di accesso al server S3.
- Gli alias non possono essere utilizzati come destinazione di registrazione per i log AWS CloudTrail.
- Amazon SageMaker AI GroundTruth non supporta gli alias dei punti di accesso.

Virtual-hosted—style URI

Gli access point supportano solo l'indirizzamento in stile hosting virtuale. In un URI in stile ospitato virtualmente, il nome del punto di accesso e Regione AWS fa parte del nome di dominio nell'URL. Account AWS Per ulteriori informazioni sull'hosting virtuale consulta [Hosting virtuale di bucket per uso generico](#).

Virtual-hosted—style URI per i punti di accesso utilizza il seguente formato:

```
https://access-point-name-account-id.s3-accesspoint.region.amazonaws.com
```

Note

- Se il nome del punto di accesso include trattini (-), includere i trattini nell'URL e inserire un altro trattino prima dell'ID account. Ad esempio, per utilizzare un punto di accesso denominato *finance-docs* di proprietà dell'account *123456789012* nella Regione *us-west-2*, l'URL appropriato è `https://finance-docs-123456789012.s3-accesspoint.us-west-2.amazonaws.com`.
- I punti di accesso S3 non supportano l'accesso tramite HTTP. I punti di accesso supportano solo l'accesso sicuro tramite HTTPS.

Compatibilità dei punti di accesso

Puoi utilizzare i punti di accesso per accedere agli oggetti utilizzando il seguente sottoinsieme di API Amazon S3. Tutte le operazioni elencate di seguito possono accettare ARN o alias dei punti di accesso.

Per esempi di uso dei punti di accesso per eseguire le operazioni sugli oggetti, consulta [Utilizzo dei punti di accesso Amazon S3 per bucket per uso generico](#).

Compatibilità dei punti di accesso con le operazioni S3

La tabella seguente è un elenco parziale delle operazioni Amazon S3 e indica se sono compatibili con i punti di accesso. Tutte le operazioni seguenti sono supportate dai punti di accesso che utilizzano un bucket S3 come origine dati, mentre solo alcune operazioni sono supportate dai punti di accesso che utilizzano un volume FSx per ONTAP o FSx per OpenZFS o un punto di ripristino S3 come origine dati. AWS Backup

Per ulteriori informazioni, consulta la compatibilità degli access point nella Guida per l'utente di [FSx for ONTAP](#) o nella Guida per l'utente di [FSx for OpenZFS](#).

Operazioni S3	Punto di accesso collegato a un bucket S3	Punto di accesso collegato a un volume FSx per OpenZFS	Punto di accesso collegato a un punto di ripristino Amazon S3 in AWS Backup
AbortMultipartUpload	Supportata	Supportata	Non supportata
CompleteMultipartUpload	Supportato	Supportata	Non supportata
CopyObject (solo copie della stessa Regione)	Supportata	Supportato, se origine e destinazione sono lo stesso punto di accesso	Non supportata
CreateMultipartUpload	Supportato	Supportata	Non supportata

Operazioni S3	Punto di accesso collegato a un bucket S3	Punto di accesso collegato a un volume FSx per OpenZFS	Punto di accesso collegato a un punto di ripristino Amazon S3 in AWS Backup
DeleteObject	Supportato	Supportata	Non supportata
DeleteObjects	Supportato	Supportata	Non supportata
DeleteObjectTagging	Supportato	Supportata	Non supportata
GetBucketAcl	Supportata	Non supportata	Non supportato
GetBucketCors	Supportata	Non supportata	Non supportato
GetBucketLocation	Supportato	Supportato	Supportato
GetBucketNotificationConfiguration	Supportata	Non supportata	Non supportato
GetBucketPolicy	Supportata	Non supportata	Non supportato
GetObject	Supportato	Supportato	Supportato
GetObjectAcl	Supportata	Non supportata	Non supportato
GetObjectAttributes	Supportato	Supportato	Supportato
GetObjectLegalHold	Supportata	Non supportata	Non supportato
GetObjectRetention	Supportata	Non supportata	Non supportato

Operazioni S3	Punto di accesso collegato a un bucket S3	Punto di accesso collegato a un volume FSx per OpenZFS	Punto di accesso collegato a un punto di ripristino Amazon S3 in AWS Backup
GetObjectTagging	Supportato	Supportato	Supportato
HeadBucket	Supportato	Supportata	Non supportata
HeadObject	Supportato	Supportato	Supportato
ListMulti partUploads	Supportato	Supportata	Non supportata
ListObjects	Supportato	Supportato	Supportato
ListObjectsV2	Supportato	Supportato	Supportato
ListObject tVersions	Supportata	Non supportata	Supportato
ListParts	Supportato	Supportata	Non supportata
Presign	Supportato	Supportata	Non supportata
PutObject	Supportato	Supportata	Non supportata
PutObjectAc1	Supportata	Non supportata	Non supportato
PutObject LegalHold	Supportata	Non supportata	Non supportato
PutObject Retention	Supportata	Non supportata	Non supportato
PutObject Tagging	Supportato	Supportata	Non supportata
RestoreObject	Supportata	Non supportata	Non supportato

Operazioni S3	Punto di accesso collegato a un bucket S3	Punto di accesso collegato a un volume FSx per OpenZFS	Punto di accesso collegato a un punto di ripristino Amazon S3 in AWS Backup
UploadPart	Supportato	Supportata	Non supportata
UploadPartCopy (solo copie della stessa Regione)	Supportata	Supportato, se origine e destinazione sono lo stesso punto di accesso	Non supportata

Configurazione delle policy IAM per l'utilizzo degli access point

I punti di accesso Amazon S3 supportano politiche sulle risorse AWS Identity and Access Management (IAM) che consentono di controllare l'uso del punto di accesso per risorsa, utente o altre condizioni. Affinché un'applicazione o un utente possa accedere agli oggetti tramite un punto di accesso, sia il punto di accesso sia il bucket sottostante o il file system Amazon FSx devono consentire la richiesta.

Important

Le limitazioni incluse in una policy di access point si applicano solo alle richieste effettuate tramite quell'access point. Il collegamento di un punto di accesso a un bucket non modifica il comportamento della risorsa sottostante. Tutte le operazioni esistenti inerenti il bucket che non sono state effettuate tramite il punto di accesso continueranno a funzionare come prima.

Quando utilizzi le policy relative alle risorse IAM, assicurati di risolvere gli avvisi di sicurezza, gli errori, gli avvisi generali e i suggerimenti AWS Identity and Access Management Access Analyzer prima di salvare la policy. IAM Access Analyzer esegue controlli sulle policy per convalidare le policy rispetto alla [grammatica delle policy](#) IAM e alle [best practice](#). Questi controlli generano risultati e forniscono suggerimenti per aiutarti a creare policy funzionali e conformi alle best practice per la sicurezza.

Per ulteriori informazioni sulla convalida delle policy tramite IAM Access Analyzer, consulta [Convalida delle policy di IAM Access Analyzer](#) nella Guida per l'utente di IAM. Per visualizzare un elenco delle

avvertenze, degli errori e dei suggerimenti restituiti da IAM Access Analyzer, consulta il [Riferimento al controllo delle policy di IAM Access Analyzer](#).

Esempi di policy per i punti di accesso

Negli esempi seguenti viene illustrato come creare le policy IAM per controllare le richieste effettuate tramite un access point.

Note

Le autorizzazioni concesse in una policy del punto di accesso sono valide solo se anche il bucket sottostante consente lo stesso accesso. Puoi farlo in due modi:

1. (Consigliato) Delega il controllo degli accessi dal bucket al punto di accesso come descritto in [Delegazione del controllo di accesso agli access point](#).
2. Aggiungere le stesse autorizzazioni contenute nella policy del punto di accesso alla policy del bucket sottostante. Nel primo esempio di policy del punto di accesso viene illustrato come modificare la policy di bucket sottostante per consentire l'accesso necessario.

Example 1: Concessione della policy del punto di accesso

La policy del punto di accesso seguente concede all'utente IAM *Jane* dell'account *123456789012* le autorizzazioni per gli oggetti GET e PUT con il prefisso *Jane/* tramite il punto di accesso *my-access-point* nell'account *123456789012*.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Jane"
      },
      "Action": ["s3:GetObject", "s3:PutObject"],
      "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point/object/Jane/*"
    }
  ]
}
```

```
}
}]
```

Note

Affinché la policy del punto di accesso fornisca effettivamente l'accesso a *Jane*, anche il bucket sottostante deve consentire lo stesso accesso a *Jane*. È possibile delegare il controllo di accesso dal bucket all'access point come descritto in [Delegazione del controllo di accesso agli access point](#). In alternativa, è possibile aggiungere la policy seguente al bucket sottostante per concedere le autorizzazioni necessarie a Jane. Si noti che la voce Resource differisce tra le policy dell'access point e del bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Jane"
      },
      "Action": ["s3:GetObject", "s3:PutObject"],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/Jane/*"
    }
  ]
}
```

Example 2: Policy del punto di accesso con condizione di tag

La policy del punto di accesso riportata di seguito concede all'utente IAM *Mateo* dell'account *123456789012* le autorizzazioni per gli oggetti GET tramite il punto di accesso *my-access-point* nell'account *123456789012* con la chiave di tag *data* impostata su un valore pari a *finance*.

JSON

```
{
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "AWS": "arn:aws:iam::123456789012:user/Mateo"
        },
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-  
point/object/*",
        "Condition": {
          "StringEquals": {
            "s3:ExistingObjectTag/data": "finance"
          }
        }
      }
    ]
  }
}

```

Example 3: Policy del punto di accesso che consente l'elenco dei bucket

La policy del punto di accesso riportata di seguito consente all'utente IAM Arnav nell'account **123456789012** di visualizzare gli oggetti contenuti nel bucket sottostante il punto di accesso *my-access-point* nell'account **123456789012**.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Arnav"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-  
point"
    }
  ]
}

```

Example 4: Policy di controllo dei servizi

La seguente policy di controllo dei servizi richiede la creazione di tutti i nuovi punti di accesso con un'origine di rete di tipo cloud privato virtuale (VPC). Con questa policy, gli utenti dell'organizzazione non possono creare nuovi access point accessibili da Internet.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "s3:CreateAccessPoint",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:AccessPointNetworkOrigin": "VPC"
        }
      }
    }
  ]
}
```

Example 5: Policy di bucket per limitare le operazioni S3 alle origini di rete VPC

La policy di bucket seguente limita l'accesso a tutte le operazioni degli oggetti S3 per il bucket *amzn-s3-demo-bucket* ai punti di accesso con un'origine di rete VPC.

Important

Prima di utilizzare un'istruzione come quella mostrata in questo esempio, assicurati di non dover utilizzare funzionalità non supportate dai punti di accesso, come Cross-Region Replication.

JSON

```
{
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Effect": "Deny",
        "Principal": "*",
        "Action": [
          "s3:AbortMultipartUpload",
          "s3:BypassGovernanceRetention",
          "s3:DeleteObject",
          "s3:DeleteObjectTagging",
          "s3:DeleteObjectVersion",
          "s3:DeleteObjectVersionTagging",
          "s3:GetObject",
          "s3:GetObjectAcl",
          "s3:GetObjectLegalHold",
          "s3:GetObjectRetention",
          "s3:GetObjectTagging",
          "s3:GetObjectVersion",
          "s3:GetObjectVersionAcl",
          "s3:GetObjectVersionTagging",
          "s3:ListMultipartUploadParts",
          "s3:PutObject",
          "s3:PutObjectAcl",
          "s3:PutObjectLegalHold",
          "s3:PutObjectRetention",
          "s3:PutObjectTagging",
          "s3:PutObjectVersionAcl",
          "s3:PutObjectVersionTagging",
          "s3:RestoreObject"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
          "StringNotEquals": {
            "s3:AccessPointNetworkOrigin": "VPC"
          }
        }
      }
    ]
  }
}

```

Chiavi di condizione

I punti di accesso S3 utilizzano chiavi di condizione che possono essere utilizzate nelle policy IAM per controllare l'accesso alle risorse. Le seguenti chiavi di condizione rappresentano solo una parte di una policy IAM. Per esempi completi di policy, consulta [Esempi di policy per i punti di accesso](#), [the section called “Delegazione del controllo di accesso agli access point”](#) e [the section called “Concessione delle autorizzazioni per i punti di accesso multi-account”](#).

s3:DataAccessPointArn

Questo esempio mostra una stringa che è possibile utilizzare per la corrispondenza dell'ARN di un punto di accesso. L'esempio seguente corrisponde a tutti i punti di accesso per Account AWS **123456789012** in Region **us-west-2**:

```
"Condition" : {
  "StringLike": {
    "s3:DataAccessPointArn": "arn:aws:s3:us-west-2:123456789012:accesspoint/*"
  }
}
```

s3:DataAccessPointAccount

Questo esempio mostra un operatore stringa che è possibile utilizzare per la corrispondenza dell'ID account del proprietario di un punto di accesso. L'esempio seguente restituisce tutti i punti di accesso di proprietà dell' Account AWS **123456789012**.

```
"Condition" : {
  "StringEquals": {
    "s3:DataAccessPointAccount": "123456789012"
  }
}
```

s3:AccessPointNetworkOrigin

Questo esempio mostra un operatore stringa che è possibile utilizzare per la corrispondenza dell'origine di rete, Internet o VPC. L'esempio seguente esegue la corrispondenza solo degli access point con un'origine VPC.

```
"Condition" : {
  "StringEquals": {
```

```
    "s3:AccessPointNetworkOrigin": "VPC"
  }
}
```

Per ulteriori informazioni sull'uso delle chiavi di condizione con Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Delegazione del controllo di accesso agli access point

È possibile delegare il controllo degli accessi per un bucket agli access point del bucket. La policy di bucket di esempio seguente consente l'accesso completo a tutti i punti di accesso dell'account del proprietario del bucket. Pertanto, tutto l'accesso a questo bucket è controllato dalle policy associate agli access point. Si consiglia di configurare i bucket in questo modo per tutti i casi d'uso che non richiedono l'accesso diretto al bucket.

Example 6: Policy di bucket che delega il controllo degli accessi ai punti di accesso

JSON

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect": "Allow",
      "Principal" : { "AWS": "*" },
      "Action" : "*",
      "Resource" : [ "arn:aws:s3:::amzn-s3-demo-bucket", "arn:aws:s3:::amzn-s3-
demo-bucket/*" ],
      "Condition": {
        "StringEquals" : { "s3:DataAccessPointAccount" : "111122223333" }
      }
    }
  ]
}
```

Concessione delle autorizzazioni per i punti di accesso multi-account

Per creare un punto di accesso a un bucket di proprietà di un altro account, devi prima creare il punto di accesso specificando il nome del bucket e l'ID del proprietario dell'account. Il proprietario del bucket deve quindi aggiornare la policy di bucket per autorizzare le richieste dal punto di accesso. La creazione di un punto di accesso è simile alla creazione di un DNS CNAME in quanto il punto di accesso non fornisce l'accesso al contenuto del bucket. Tutti gli accessi ai bucket sono controllati dalla policy di bucket. La policy di bucket di esempio consente di eseguire richieste GET e LIST sul bucket da un punto di accesso di proprietà di un Account AWS attendibile.

Sostituisci *Bucket ARN* con l'ARN del bucket.

Example 7 — Politica del bucket che delega le autorizzazioni a un altro Account AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect": "Allow",
      "Principal" : { "AWS": "*" },
      "Action" : ["s3:GetObject", "s3:ListBucket"],
      "Resource" : ["arn:aws:s3:::amzn-s3-demo-bucket", "arn:aws:s3:::amzn-s3-
demo-bucket/*"],
      "Condition": {
        "StringEquals" : { "s3:DataAccessPointAccount" : "Access point
owner's account ID" }
      }
    }
  ]
}
```

Note

Cross-account i punti di accesso sono disponibili solo per i punti di accesso collegati ai bucket S3. Non è possibile collegare un punto di accesso a un volume su un file system Amazon FSx di proprietà di un altro Account AWS.

Monitoraggio e registrazione degli access point

Amazon S3 registra le richieste effettuate attraverso i punti di accesso e le richieste effettuate alle operazioni API che gestiscono i punti di accesso, come `CreateAccessPoint` e `GetAccessPointPolicy`. Per monitorare e gestire i modelli di utilizzo, puoi anche configurare le metriche di richiesta di Amazon CloudWatch Logs per i punti di accesso.

Argomenti

- [CloudWatch metriche di richiesta](#)
- [AWS CloudTrail registri delle richieste effettuate tramite punti di accesso](#)

CloudWatch metriche di richiesta

Per comprendere e migliorare le prestazioni delle applicazioni che utilizzano punti di accesso, puoi utilizzare CloudWatch le metriche delle richieste di Amazon S3. I parametri di richiesta ti aiutano a monitorare le richieste di Amazon S3 per identificare rapidamente i problemi operativi e intraprendere le operazioni appropriate.

Per impostazione predefinita, questi parametri sono disponibili a livello di bucket. Tuttavia, puoi definire un filtro per i parametri di richiesta utilizzando un prefisso condiviso, tag oggetto o un punto di accesso. Quando crei un filtro con un punto di accesso, la configurazione dei parametri della richiesta include le richieste al punto di accesso specificato. Puoi ricevere parametri, impostare allarmi e accedere ai pannelli di controllo per visualizzare le operazioni eseguite in tempo reale tramite questo punto di accesso.

Devi acconsentire esplicitamente ai parametri di richiesta configurandoli nella console o utilizzando l'API Amazon S3. I parametri di richiesta sono disponibili a intervalli di 1 minuto dopo una determinata latenza per l'elaborazione. Le metriche delle richieste vengono fatturate alla stessa tariffa delle metriche personalizzate. CloudWatch Per ulteriori informazioni, consulta [i prezzi di Amazon CloudWatch](#).

Per creare una configurazione dei parametri di richiesta che filtra in base al punto di accesso, vedi [Creazione di una configurazione dei parametri che filtra in base al prefisso, al tag oggetto o al punto di accesso](#).

AWS CloudTrail registri delle richieste effettuate tramite punti di accesso

Puoi registrare le richieste effettuate tramite i punti di accesso e le richieste effettuate alle API che li gestiscono, ad esempio `CreateAccessPoint` e `GetAccessPointPolicy`, utilizzando la registrazione degli accessi al server e AWS CloudTrail.

CloudTrail le voci di registro per le richieste effettuate tramite i punti di accesso includono l'ARN del punto di accesso nella `resources` sezione del registro.

Si prenda come esempio la seguente configurazione:

- Un bucket denominato *amzn-s3-demo-bucket1* nella Regione *us-west-2* che contiene un oggetto denominato *my-image.jpg*
- Un punto di accesso denominato *my-bucket-ap* associato a *amzn-s3-demo-bucket1*
- Un Account AWS ID di *123456789012*

L'esempio seguente mostra la `resources` sezione di una voce di CloudTrail registro relativa alla configurazione precedente:

```
"resources": [  
  {"type": "AWS::S3::Object",  
    "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1/my-image.jpg"  
  },  
  {"accountId": "123456789012",  
    "type": "AWS::S3::Bucket",  
    "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1"  
  },  
  {"accountId": "123456789012",  
    "type": "AWS::S3::AccessPoint",  
    "ARN": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-bucket-ap"  
  }  
]
```

Se utilizzi un punto di accesso collegato a un volume su un file system Amazon FSx, la `resources` sezione di una voce di CloudTrail registro avrà un aspetto diverso. Ad esempio:

```
"resources": [  
  {  
    "accountId": "123456789012",
```

```
    "type": "AWS::FSx::Volume",
    "ARN": "arn:aws:fsx:us-east-1:123456789012:volume/fs-0123456789abcdef9/
fsvol-01234567891112223"
  }
]
```

Se utilizzi un punto di accesso collegato a un punto di ripristino S3 AWS Backup, le richieste del piano dati (come `GetObject` e `ListObjectsV2`) vengono registrate allo stesso modo CloudTrail delle richieste tramite punti di accesso S3 standard. Ad esempio:

```
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::Backup::BackupAccessPoint",
    "ARN": "arn:aws:backup:us-east-1:123456789012:accesspoint/my-access-point"
  },
  {
    "type": "AWS::S3::Object",
    "ARN": "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point/
object/path/to/my-file.txt"
  },
  {
    "accountId": "123456789012",
    "type": "AWS::S3::AccessPoint",
    "ARN": "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point"
  }
]
```

Le operazioni del piano di controllo per i punti di accesso di backup (come `CreateBackupAccessPoint` e `DeleteBackupAccessPoint`) vengono registrate come eventi. AWS Backup Per ulteriori informazioni, consulta [Monitoring AWS Backup](#) nella AWS Backup Developer Guide.

Per ulteriori informazioni sui log degli accessi al server S3, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#). Per ulteriori informazioni su AWS CloudTrail, vedi [Che cos'è AWS CloudTrail?](#) nella Guida AWS CloudTrail per l'utente.

Creazione di un access point

Puoi creare punti di accesso S3 utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI), AWS SDK o l'API REST di Amazon S3. I punti di accesso sono denominati endpoint

di rete collegati a un'origine dati come un bucket, un volume Amazon FSx for ONTAP o un volume Amazon FSx for OpenZFS.

Per impostazione predefinita, è possibile creare fino a 10.000 punti di accesso per Regione per ciascuno dei tuoi Account AWS. Se hai bisogno di più di 10.000 punti di accesso per un singolo account in una singola Regione, puoi richiedere un aumento della quota di servizio. Per ulteriori informazioni su Service Quotas e la richiesta di un aumento, consulta [AWS Service Quotas](#) in Riferimenti generali di AWS.

Argomenti

- [Creazione di punti di accesso con bucket S3](#)
- [Creazione di punti di accesso con Amazon FSx](#)
- [Creazione di punti di accesso con AWS Backup](#)
- [Creazione di access point limitati a un cloud privato virtuale](#)
- [Gestione dell'accesso pubblico ai punti di accesso per bucket per uso generico](#)

Creazione di punti di accesso con bucket S3

Un punto di accesso è associato esattamente a un bucket per uso generico Amazon S3. Se desideri utilizzare un bucket nel tuo Account AWS, devi prima crearne uno. Per ulteriori informazioni sulla creazione dei bucket, consulta [Creazione, configurazione e utilizzo di bucket per uso generico Amazon S3](#).

Puoi anche creare un punto di accesso multi-account associato a un bucket in un altro Account AWS, purché tu conosca il nome del bucket e l'ID dell'account del proprietario del bucket. Tuttavia, la creazione di punti di accesso multi-account non consente l'accesso ai dati nel bucket finché non vengono concesse le autorizzazioni dal proprietario del bucket. Il proprietario del bucket deve concedere all'account del proprietario del punto di accesso (il tuo account) l'accesso al bucket tramite la policy di bucket. Per ulteriori informazioni, consulta [Concessione delle autorizzazioni per i punti di accesso multi-account](#).

Utilizzo della console S3

Come creare un punto di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui si desidera creare un punto di accesso. Il punto di accesso deve essere creato nella stessa Regione del bucket associato.
3. Nel pannello di navigazione a sinistra, scegli Access Points (Punti di accesso).
4. Nella pagina Punto di accesso, scegli Crea punto di accesso.
5. Nel campo Nome del punto di accesso immetti il nome per il punto di accesso. Per ulteriori informazioni sulla denominazione dei punti di accesso, consulta [Regole di denominazione dei punti di accesso](#).
6. Per Origine dati specifica il bucket S3 che desideri utilizzare con il punto di accesso.

Per usare un bucket nel tuo account, seleziona Scegli un bucket in questo account e digita o cerca il nome del bucket.

Per utilizzare un bucket in un altro Account AWS, scegli Specifica un bucket in un altro account e inserisci l' Account AWS ID e il nome del bucket. Se utilizzi un bucket in un altro Account AWS, il proprietario del bucket deve aggiornare la policy del bucket per autorizzare le richieste dal punto di accesso. Per un esempio di policy di bucket, consulta [Concessione delle autorizzazioni per i punti di accesso multi-account](#).

 Note

Per informazioni sull'utilizzo di un volume FSx per OpenZFS come origine dati, consulta [Creazione di punti di accesso con Amazon FSx](#).

7. Per Origine della rete scegli Internet o Cloud privato virtuale (VPC). Se scegli Cloud privato virtuale (VPC), immetti l'ID VPC che desideri utilizzare con il punto di accesso.

Per ulteriori informazioni sulle origini della rete per i punti di accesso, consulta [Creazione di access point limitati a un cloud privato virtuale](#).

8. In Block Public Access settings for this Access Point (Impostazioni punto di accesso per blocco dell'accesso pubblico), seleziona le impostazioni di blocco dell'accesso pubblico da applicare all'access point. Tutte le impostazioni di blocco dell'accesso pubblico sono abilitate per impostazione predefinita per i nuovi punti di accesso. È consigliabile lasciare tutte le impostazioni abilitate, a meno che tu non debba necessariamente disabilitarne una specifica.

 Note

Dopo aver creato un punto di accesso, non è più possibile modificare le impostazioni di blocco dell'accesso pubblico.

Per ulteriori informazioni sull'uso del blocco dell'accesso pubblico di Amazon S3 con i punti di accesso, consulta [Gestione dell'accesso pubblico ai punti di accesso per bucket per uso generico](#).

9. (Facoltativo) In Policy del punto di accesso - facoltativo, specificare la policy dell'access point. Prima di salvare la policy, assicurati di risolvere gli avvisi di sicurezza, gli errori, gli avvisi generali e i suggerimenti. Per ulteriori informazioni sulla specifica di una policy dei punti di accesso, consulta [Esempi di policy per i punti di accesso](#).
10. Selezionare Crea punto di accesso.

Utilizzo di AWS CLI

Il comando di esempio seguente crea un punto di accesso denominato *example-ap* per il bucket *amzn-s3-demo-bucket* nell'account *111122223333*. Per creare il punto di accesso, devi inviare una richiesta ad Amazon S3 che specifica quanto segue:

- Nome del punto di accesso. Per informazioni sulle regole di denominazione, consulta [the section called "Regole di denominazione dei punti di accesso"](#).
- Nome del bucket a cui si desidera associare il punto di accesso.
- L'ID dell'account del proprietario del punto Account AWS di accesso.

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --  
bucket amzn-s3-demo-bucket
```

Quando crei un punto di accesso utilizzando un bucket in un altro Account AWS, includi il `--bucket-account-id` parametro. Il seguente comando di esempio crea un punto di accesso nell'Account AWS *111122223333*, utilizzando il bucket *amzn-s3-demo-bucket2*, che si trova nell'Account AWS *444455556666*.

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --  
bucket amzn-s3-demo-bucket --bucket-account-id 444455556666
```

Utilizzo della REST API

È possibile utilizzare la REST API per creare un punto di accesso. Per ulteriori informazioni, consulta [CreateAccessPoint](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Creazione di punti di accesso con Amazon FSx

Puoi creare e collegare un punto di accesso a un volume FSx per OpenZFS utilizzando la console o l'API di Amazon FSx. AWS CLI Una volta collegato, si possono utilizzare le API degli oggetti S3 per accedere ai dati dei file. I dati continuano a risiedere nel file system Amazon FSx e continuano a essere direttamente accessibili per i carichi di lavoro esistenti. È possibile continuare a gestire l'archiviazione utilizzando tutte le funzionalità di gestione dell'archiviazione di FSx per OpenZFS, inclusi backup, snapshot, quote di utenti e gruppi e compressione.

Per istruzioni su come creare un punto di accesso e collegarlo a un volume FSx per OpenZFS, consulta [Creazione di un punto di accesso](#) nella Guida per l'utente di FSx per OpenZFS.

Creazione di punti di accesso con AWS Backup

AWS Backup crea e collega punti di accesso ai punti di ripristino S3, fornendo accesso in sola lettura ai dati di backup S3 utilizzando le API S3. Questi punti di accesso vengono creati tramite la AWS Backup console o l'API, non tramite le `CreateBackupAccessPoint` API dei punti di accesso S3.

Per istruzioni sulla creazione di un punto di accesso di backup, consulta i punti di accesso di [backup](#) nella Guida per gli AWS Backup sviluppatori.

Creazione di access point limitati a un cloud privato virtuale

Quando si crea un punto di accesso, è possibile scegliere di renderlo accessibile da Internet oppure specificare che tutte le richieste effettuate tramite tale punto di accesso debbano provenire da uno specifico cloud privato virtuale (VPC). Un access point accessibile da Internet ha l'origine di rete Internet. Può essere utilizzato da qualsiasi punto di Internet, fatte salve altre limitazioni di accesso in vigore per il punto di accesso, l'origine dati sottostante e le risorse correlate, come gli oggetti richiesti. Un access point accessibile solo da un VPC specificato ha l'origine di rete VPC e Amazon S3 rifiuta qualsiasi richiesta fatta all'access point che non provenga da quel VPC.

⚠ Important

Puoi specificare l'origine di rete di un access point solo quando crei l'access point. Dopo aver creato l'access point, non è più possibile modificare l'origine di rete.

Per limitare l'accesso a un punto di VPC-only accesso, includi il `VpcConfiguration` parametro nella richiesta di creazione del punto di accesso. Nel parametro `VpcConfiguration`, specificare l'ID VPC che si desidera utilizzare l'access point. Se una richiesta viene effettuata tramite il punto di accesso, la richiesta deve provenire dal VPC o Amazon S3 la rifiuterà.

È possibile recuperare l'origine della rete di un punto di accesso utilizzando gli AWS CLI AWS SDK o le API REST. Se per un access point è specificata una configurazione VPC, la sua origine di rete è VPC. In caso contrario, l'origine della rete dell'access point è Internet.

Esempio: creare e limitare un punto di accesso a un ID VPC

Nell'esempio seguente viene creato un punto di accesso denominato `example-vpc-ap` per il bucket `amzn-s3-demo-bucket` nell'account 123456789012 che consente l'accesso solo dal VPC `vpc-1a2b3c`. L'esempio verifica quindi che il nuovo access point abbia l'origine di rete VPC.

AWS CLI

```
aws s3control create-access-point --name example-vpc-ap --account-id 123456789012 --  
bucket amzn-s3-demo-bucket --vpc-configuration VpcId=vpc-1a2b3c
```

```
aws s3control get-access-point --name example-vpc-ap --account-id 123456789012  
  
{  
  "Name": "example-vpc-ap",  
  "Bucket": "amzn-s3-demo-bucket",  
  "NetworkOrigin": "VPC",  
  "VpcConfiguration": {  
    "VpcId": "vpc-1a2b3c"  
  },  
  "PublicAccessBlockConfiguration": {  
    "BlockPublicAcls": true,  
    "IgnorePublicAcls": true,  
    "BlockPublicPolicy": true,  
    "RestrictPublicBuckets": true  
  },  
}
```



```
"CreationDate": "2019-11-27T00:00:00Z"
}
```

Per utilizzare un access point con un VPC, è necessario modificare la policy di accesso per l'endpoint VPC. Gli endpoint VPC consentono al traffico di fluire dal VPC ad Amazon S3. Dispongono di policy di controllo dell'accesso che controllano il modo in cui le risorse all'interno del VPC possono interagire con Amazon S3. Le richieste dal VPC ad Amazon S3 hanno esito positivo solo tramite un punto di accesso se la policy dell'endpoint VPC concede l'accesso sia al punto di accesso che al bucket sottostante.

Note

Per rendere le risorse accessibili solo all'interno di un VPC, assicurati di creare una [zona ospitata privata](#) per l'endpoint VPC. Per utilizzare una zona ospitata privata, [modificare le impostazioni del VPC](#) in modo che gli [attributi di rete VPC](#) `enableDnsHostnames` e `enableDnsSupport` siano impostati su `true`.

L'istruzione di policy di esempio riportata di seguito configura un endpoint VPC per consentire le chiamate a `GetObject` per un bucket denominato `awsexamplebucket1` e un access point denominato `example-vpc-ap`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::awsexamplebucket1/*",
        "arn:aws:s3:us-west-2:123456789012:accesspoint/example-vpc-ap/object/*"
      ]
    }
  ]
}
```

```
}
```

Note

La dichiarazione "Resource" in questo esempio utilizza un Amazon Resource Name (ARN) per specificare l'access point. Per ulteriori informazioni sugli ARN dei punti di accesso, consulta [Riferimento ai punti di accesso con ARN, alias di punti di accesso o URI virtual-hosted-style](#).

Per ulteriori informazioni sulle policy degli endpoint VPC, consulta [Utilizzo delle policy degli endpoint per Amazon S3](#) nella Guida per l'utente del VPC.

Per un tutorial sulla creazione di punti di accesso con endpoint VPC, consulta [Gestione dell'accesso Amazon S3 con endpoint VPC e punti di accesso](#).

Esempio: creare e limitare un punto di accesso collegato a un volume FSx for OpenZFS a un ID VPC

Puoi creare un punto di accesso collegato a un volume FSx per OpenZFS utilizzando la console o l'API di Amazon FSx. AWS CLI Una volta collegato, si possono utilizzare le API degli oggetti S3 per accedere ai dati dei file da un VPC specificato.

Per istruzioni su come creare e limitare un punto di accesso collegato a un volume FSx for OpenZFS, consulta la [Creazione di punti di accesso limitati a un cloud privato virtuale \(VPC\) nella Guida per l'utente di FSx for OpenZFS](#).

Esempio: creare e limitare un punto di accesso collegato a un volume FSx for ONTAP a un ID VPC

Puoi creare un punto di accesso collegato a un volume FSx for ONTAP utilizzando la console o l'API di Amazon FSx. AWS CLI Una volta collegato, si possono utilizzare le API degli oggetti S3 per accedere ai dati dei file da un VPC specificato.

Per istruzioni su come creare e limitare un punto di accesso collegato a un volume FSx for ONTAP, consulta la Guida per l'utente di FSx for ONTAP.

Gestione dell'accesso pubblico ai punti di accesso per bucket per uso generico

Gli Punti di accesso Amazon S3 supportano le impostazioni di blocco dell'accesso pubblico indipendenti per ciascun access point. Quando crei un access point, puoi specificare le impostazioni

di blocco dell'accesso pubblico applicabili all'access point. Per qualsiasi richiesta effettuata tramite un access point, Amazon S3 valuta le impostazioni di blocco dell'accesso pubblico per l'access point, il bucket sottostante e l'account del proprietario del bucket. Se una di queste impostazioni indica che la richiesta deve essere bloccata, Amazon S3 rifiuta la richiesta.

Per ulteriori informazioni sulla funzionalità di blocco dell'accesso pubblico S3, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Important

- Tutte le impostazioni di blocco dell'accesso pubblico sono abilitate per impostazione predefinita per gli access point. Durante la creazione del punto di accesso, è necessario disattivare esplicitamente tutte le impostazioni indesiderate.
- Non è possibile disattivare le impostazioni di blocco dell'accesso pubblico quando si crea o si utilizza un punto di accesso collegato a un file system Amazon FSx.
- Dopo aver creato un punto di accesso, non è più possibile modificare le impostazioni di blocco dell'accesso pubblico.

Example

Esempio: creare un access point con impostazioni di blocco dell'accesso pubblico personalizzate

In questo esempio viene creato un access point denominato `example-ap` per il bucket `amzn-s3-demo-bucket` nell'account 123456789012 con impostazioni di blocco dell'accesso pubblico non predefinite. L'esempio recupera quindi la configurazione del nuovo access point per verificarne le impostazioni di blocco dell'accesso pubblico.

AWS CLI

```
aws s3control create-access-point --name example-ap --account-id
123456789012 --bucket amzn-s3-demo-bucket --public-access-block-configuration
BlockPublicAcls=false,IgnorePublicAcls=false,BlockPublicPolicy=true,RestrictPublicBuckets=t
```

```
aws s3control get-access-point --name example-ap --account-id 123456789012

{
  "Name": "example-ap",
```

```
{
  "Bucket": "amzn-s3-demo-bucket",
  "NetworkOrigin": "Internet",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": false,
    "IgnorePublicAcls": false,
    "BlockPublicPolicy": true,
    "RestrictPublicBuckets": true
  },
  "CreationDate": "2019-11-27T00:00:00Z"
}
```

Gestione dei punti di accesso Amazon S3 per bucket per uso generico

Questa sezione spiega come gestire i punti di accesso Amazon S3 per bucket generici utilizzando l'API, o REST. Console di gestione AWS AWS Command Line Interface Per informazioni sulla gestione dei punti di accesso collegati a un volume FSx per OpenZFS, consulta [Gestione dei punti di accesso Amazon S3](#) nella Guida per l'utente di FSx per OpenZFS.

Note

Puoi utilizzare gli access point solo per eseguire le operazioni sugli oggetti. Non è possibile utilizzare i punti di accesso per eseguire altre operazioni Amazon S3, come l'eliminazione di bucket o la creazione di configurazioni di replica S3. Per un elenco completo delle operazioni S3 che supportano i punti di accesso, consulta [Compatibilità dei punti di accesso](#).

Argomenti

- [Elenco dei punti di accesso per bucket per uso generico](#)
- [Visualizzazione dei dettagli del punto di accesso per bucket per uso generico](#)
- [Eliminazione del punto di accesso per un bucket per uso generico](#)

Elenco dei punti di accesso per bucket per uso generico

Questa sezione spiega come elencare i punti di accesso per bucket generici utilizzando l'API Console di gestione AWS, AWS Command Line Interface, o REST.

Utilizzo della console S3

Per elencare i punti di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.

Utilizzo di AWS CLI

Il seguente comando di `list-access-points` esempio mostra come è possibile utilizzare AWS CLI per elencare i punti di accesso.

Il comando seguente elenca i punti di accesso per Account AWS **111122223333**.

```
aws s3control list-access-points --account-id 111122223333
```

Il comando seguente elenca i punti Account AWS **111122223333** di accesso collegati al bucket **amzn-s3-demo-bucket**

```
aws s3control list-access-points --account-id 111122223333 --bucket amzn-s3-demo-bucket
```

Per ulteriori informazioni ed esempi, consulta [list-access-points](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per elencare i punti di accesso. Per ulteriori informazioni, consulta [ListAccessPoints](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Visualizzazione dei dettagli del punto di accesso per bucket per uso generico

Questa sezione spiega come visualizzare i dettagli del punto di accesso per un bucket generico utilizzando l'API Console di gestione AWS, AWS Command Line Interface, o REST.

Utilizzo della console S3

Per visualizzare i dettagli del punto di accesso nel Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.
6. Seleziona la scheda Proprietà per visualizzare l'origine dati del punto di accesso, l'ID dell'account, la data di creazione Regione AWS, l'origine della rete, l'URI S3, l'ARN e l'alias del punto di accesso per il punto di accesso selezionato.
7. Seleziona la scheda Autorizzazioni per visualizzare le impostazioni di blocco dell'accesso pubblico e la policy per il punto di accesso selezionato.

Note

Non è possibile modificare le impostazioni del blocco dell'accesso pubblico per un punto di accesso dopo la sua creazione.

Utilizzo di AWS CLI

Il comando di `get-access-point` esempio seguente mostra come è possibile utilizzare il AWS CLI per visualizzare i dettagli del punto di accesso.

Il comando seguente elenca i dettagli del punto *my-access-point* di accesso Account AWS *111122223333* collegato al *amzn-s3-demo-bucket* bucket S3.

```
aws s3control get-access-point --name my-access-point --account-id 111122223333
```

Output di esempio:

```
{
  "Name": "my-access-point",
  "Bucket": "amzn-s3-demo-bucket",
  "NetworkOrigin": "Internet",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "IgnorePublicAcls": true,
    "BlockPublicPolicy": true,
    "RestrictPublicBuckets": true
  },
  "CreationDate": "2016-08-29T22:57:52Z",
  "Alias": "my-access-point-u1ny6bhm7moymqx8cuon8o1g4mwikuse2a-s3alias",
  "AccessPointArn": "arn:aws:s3:Regione AWS:111122223333:accesspoint/my-access-point",
  "Endpoints": {
    "ipv4": "s3-accesspoint.Regione AWS.amazonaws.com",
    "fips": "s3-accesspoint-fips.Regione AWS.amazonaws.com",
    "fips_dualstack": "s3-accesspoint-fips.dualstack.Regione AWS.amazonaws.com",
    "dualstack": "s3-accesspoint.dualstack.Regione AWS.amazonaws.com"
  },
  "BucketAccountId": "111122223333"
}
```

Il comando seguente elenca i dettagli del punto *example-fsx-ap* di accesso per. Account AWS *444455556666* Questo punto di accesso è collegato a un file system Amazon FSx.

```
aws s3control get-access-point --name example-fsx-ap --account-id 444455556666
```

Output di esempio:

```
{
  "Name": "example-fsx-ap",
  "Bucket": "",
  "NetworkOrigin": "Internet",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
```

```
    "IgnorePublicAcls": true,  
    "BlockPublicPolicy": true,  
    "RestrictPublicBuckets": true  
  },  
  "CreationDate": "2025-01-19T14:16:12Z",  
  "Alias": "example-fsx-ap-qrqbyebjtsxorhhaa5exx6r3q7-ext-s3alias",  
  "AccessPointArn": "arn:aws:s3:Regione AWS:444455556666:accesspoint/example-fsx-ap",  
  "Endpoints": {  
    "ipv4": "s3-accesspoint.Regione AWS.amazonaws.com",  
    "fips": "s3-accesspoint-fips.Regione AWS.amazonaws.com",  
    "fips_dualstack": "s3-accesspoint-fips.dualstack.Regione AWS.amazonaws.com",  
    "dualstack": "s3-accesspoint.dualstack.Regione AWS.amazonaws.com"  
  },  
  "DataSourceId": "arn:aws:fsx:Regione AWS:444455556666:file-system/  
fs-5432106789abcdef0/volume/vol-0123456789abcdef0",  
  "DataSourceType": "FSX_OPENZFS"  
}
```

Per ulteriori informazioni ed esempi, consulta [get-access-point](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per visualizzare i dettagli del punto di accesso. Per ulteriori informazioni, consulta [GetAccessPoint](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Eliminazione del punto di accesso per un bucket per uso generico

Questa sezione spiega come eliminare il punto di accesso per un bucket generico utilizzando l'API Console di gestione AWS, AWS Command Line Interface, o REST.

Utilizzo della console S3

Per eliminare i tuoi punti di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.

3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.
6. Dalla pagina Punto di accesso, seleziona Elimina per eliminare il punto di accesso selezionato.
7. Digita il nome del punto di accesso per confermare l'eliminazione, quindi scegli Elimina.

Utilizzo di AWS CLI

Il seguente comando di `delete-access-point` esempio mostra come è possibile utilizzare AWS CLI per eliminare il punto di accesso.

Il comando seguente elimina il punto di accesso *my-access-point* per Account AWS *111122223333*.

```
aws s3control delete-access-point --name my-access-point --account-id 111122223333
```

Per ulteriori informazioni ed esempi, consulta [delete-access-point](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per visualizzare i dettagli del punto di accesso. Per ulteriori informazioni, consulta [DeleteAccessPoint](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo dei punti di accesso Amazon S3 per bucket per uso generico

Gli esempi seguenti mostrano come utilizzare i punti di accesso per bucket per uso generico con operazioni compatibili in Amazon S3.

Note

S3 genera automaticamente gli alias per tutti i punti di accesso e questi alias possono essere utilizzati ovunque venga utilizzato un nome di bucket per eseguire operazioni a livello di oggetto. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

È possibile utilizzare punti di accesso solo per bucket per uso generico per eseguire operazioni sugli oggetti. Non puoi utilizzare access point per eseguire altre operazioni in Amazon S3, ad esempio la modifica o l'eliminazione dei bucket. Per un elenco completo delle operazioni S3 che supportano i punti di accesso, consulta [Compatibilità dei punti di accesso](#).

Argomenti

- [Elenco degli oggetti tramite un punto di accesso per un bucket per uso generico](#)
- [Download di un oggetto tramite un punto di accesso per un bucket per uso generico](#)
- [Configurazione delle liste di controllo degli accessi \(ACL\) tramite un punto di accesso per un bucket per uso generico](#)
- [Caricamento di un oggetto tramite un punto di accesso per un bucket per uso generico](#)
- [Aggiunta di un set di tag tramite un punto di accesso per un bucket per uso generico](#)
- [Eliminazione di un oggetto tramite un punto di accesso per un bucket per uso generico](#)

Elenco degli oggetti tramite un punto di accesso per un bucket per uso generico

Questa sezione spiega come elencare gli oggetti tramite un punto di accesso per un bucket generico utilizzando l' Console di gestione AWS API,, o REST. AWS Command Line Interface

Utilizzo della console S3

Per elencare i tuoi oggetti tramite un punto di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.
6. Nella scheda Oggetti è possibile vedere il nome degli oggetti a cui accedere tramite il punto di accesso. Durante l'utilizzo dell'access point, è possibile eseguire solo le operazioni sugli oggetti consentite dalle autorizzazioni dell'access point.

 Note

- La visualizzazione della console mostra sempre tutti gli oggetti presenti nel bucket. L'utilizzo di un access point tipo quello descritto in questa procedura limita le operazioni che puoi eseguire sugli oggetti, ma non la visualizzazione degli oggetti presenti nel bucket.
- Console di gestione AWS Non supporta l'utilizzo di access point di cloud privato virtuale (VPC) per accedere alle risorse del bucket. Per accedere alle risorse del bucket da un punto di accesso VPC, utilizza gli AWS SDK o le API AWS CLI REST di Amazon S3.

Utilizzo di AWS CLI

Il seguente comando di `list-objects-v2` esempio mostra come puoi usare il AWS CLI per elencare il tuo oggetto tramite un punto di accesso.

Il comando seguente elenca gli oggetti per Account AWS **111122223333** l'utilizzo del punto di accesso ***my-access-point***.

```
aws s3api list-objects-v2 --bucket arn:aws:s3:Regione AWS:111122223333:accesspoint/my-access-point
```

 Note

S3 genera automaticamente gli alias per tutti i punti di accesso e questi alias possono essere utilizzati ovunque venga utilizzato un nome di bucket per eseguire operazioni a livello di oggetto. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

Per ulteriori informazioni ed esempi, consulta [list-access-points](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per elencare i punti di accesso. Per ulteriori informazioni, consulta [ListObjectsV2](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Download di un oggetto tramite un punto di accesso per un bucket per uso generico

Questa sezione spiega come scaricare un oggetto tramite un punto di accesso per un bucket generico utilizzando l'API Console di gestione AWS, AWS Command Line Interface, o REST.

Utilizzo della console S3

Per scaricare un oggetto tramite un punto di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.
6. Nella scheda Oggetti, seleziona il nome dell'oggetto da scaricare.
7. Scegli Scarica.

Utilizzo di AWS CLI

Il seguente comando di `get-object` esempio mostra come è possibile utilizzare il AWS CLI per scaricare un oggetto tramite un punto di accesso.

Il comando seguente scarica l'oggetto `puppy.jpg` per l' Account AWS **111122223333** utilizzo del punto di accesso **my-access-point**. È necessario includere un `outfile`, che è un nome di file per l'oggetto scaricato, ad esempio **my_downloaded_image.jpg**.

```
aws s3api get-object --bucket arn:aws:s3:Regione AWS:111122223333:accesspoint/my-access-point --key puppy.jpg my_downloaded_image.jpg
```

 Note

S3 genera automaticamente gli alias per tutti i punti di accesso e questi alias possono essere utilizzati ovunque venga utilizzato un nome di bucket per eseguire operazioni a livello di oggetto. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

Per ulteriori informazioni ed esempi, consulta [get-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per scaricare un oggetto tramite un punto di accesso. Per ulteriori informazioni, consulta [GetObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

È possibile utilizzare l' AWS SDK per Python per scaricare un oggetto tramite un punto di accesso.

Python

Nell'esempio seguente, il file denominato *hello.txt* viene scaricato per l' AWS account *111122223333* utilizzando il punto di accesso denominato *my-access-point*

```
import boto3
s3 = boto3.client('s3')
s3.download_file('arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point',
'hello.txt', '/tmp/hello.txt')
```

Configurazione delle liste di controllo degli accessi (ACL) tramite un punto di accesso per un bucket per uso generico

Questa sezione spiega come configurare gli ACL tramite un punto di accesso per un bucket generico utilizzando l'API Console di gestione AWS, AWS Command Line Interface, o REST. Per ulteriori informazioni sulle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

Utilizzo della console S3

Per configurare gli ACL tramite un punto di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.
6. Nella scheda Oggetti, seleziona il nome dell'oggetto per cui desideri configurare un'ACL.
7. Nella scheda Autorizzazioni, seleziona Modifica per configurare l'ACL dell'oggetto.

Note

Amazon S3 attualmente non supporta la modifica delle impostazioni di blocco dell'accesso pubblico di un punto di accesso dopo la creazione del punto di accesso.

Utilizzo di AWS CLI

Il seguente comando di `put-object-acl` esempio mostra come è possibile utilizzare il AWS CLI per configurare le autorizzazioni di accesso tramite un punto di accesso utilizzando un ACL.

Il comando seguente applica un ACL a un oggetto esistente `puppy.jpg` tramite un punto di accesso di proprietà di Account AWS **111122223333**

```
aws s3api put-object-acl --bucket arn:aws:s3:Regione AWS:111122223333:accesspoint/my-access-point --key puppy.jpg --acl private
```

 Note

S3 genera automaticamente gli alias per tutti i punti di accesso e questi alias possono essere utilizzati ovunque venga utilizzato un nome di bucket per eseguire operazioni a livello di oggetto. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

Per ulteriori informazioni ed esempi, consulta [put-object-acl](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per configurare le autorizzazioni di accesso tramite un punto di accesso utilizzando un'ACL. Per ulteriori informazioni, consulta [PutObjectAcl](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Caricamento di un oggetto tramite un punto di accesso per un bucket per uso generico

Questa sezione spiega come caricare un oggetto tramite un punto di accesso per un bucket generico utilizzando l'API Console di gestione AWS, AWS Command Line Interface, o REST.

Utilizzo della console S3

Per caricare un oggetto tramite un punto di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.
6. Nella scheda Oggetti, seleziona Carica.
7. Trascina i file e le cartelle che desideri caricare oppure scegli Aggiungi file o Aggiungi cartella.

 Note

La dimensione massima di un file che è possibile caricare utilizzando la console di Amazon S3 è 160 GB. Per caricare un file di dimensioni superiori a 160 GB, utilizza AWS Command Line Interface (AWS CLI), AWS SDK o l'API REST di Amazon S3.

8. Per modificare le autorizzazioni della lista di controllo degli accessi, scegli Permissions (Autorizzazioni).
9. In Access control list (ACL) Lista di controllo degli accessi (ACL), modifica le autorizzazioni.

Per informazioni sulle autorizzazioni di accesso agli oggetti, consulta [Utilizzo della console S3 per impostare le autorizzazioni ACL per un oggetto](#). Puoi concedere l'accesso in lettura ai tuoi oggetti al pubblico (chiunque) per tutti i file che stai caricando. Ti consigliamo di non modificare l'impostazione di default per l'accesso pubblico in lettura. La concessione dell'accesso pubblico in lettura si applica a un piccolo sottoinsieme di casi d'uso, ad esempio quando i bucket vengono usati per i siti Web. È sempre possibile apportare modifiche alle autorizzazioni dell'oggetto dopo averlo caricato.

10. Per configurare altre proprietà scegli Properties (Proprietà).
11. Nella sezione Classe di storage seleziona la classe di storage per i file che si stanno caricando.

Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

12. Per aggiornare le impostazioni di crittografia per i tuoi oggetti, in Impostazioni di Server-side crittografia, procedi come segue.
 - a. Scegli Specify an encryption key (Specifica una chiave di crittografia).
 - b. In Impostazioni di crittografia, scegli Utilizza le impostazioni del bucket per la crittografia predefinita o Ignora le impostazioni del bucket per la crittografia predefinita.
 - c. Se scegli Ignora le impostazioni del bucket per la crittografia predefinita, dovrai configurare le seguenti impostazioni di crittografia.
 - Per crittografare i file caricati utilizzando chiavi gestite da Amazon S3, scegli Amazon S3 managed key (). SSE-S3

Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).

- Per crittografare i file caricati utilizzando le chiavi memorizzate in AWS Key Management Service (AWS KMS), scegli AWS Key Management Service key (). SSE-KMS Quindi scegli una delle seguenti opzioni per Chiave AWS KMS :
- Per scegliere da un elenco di chiavi KMS disponibili, seleziona Scegli tra le chiavi AWS KMS keys, quindi scegli la chiave KMS dall'elenco delle chiavi disponibili.

Sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente vengono visualizzate in questo elenco. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per inserire l'ARN della chiave KMS, scegli Inserisci AWS KMS key ARN, quindi inserisci l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

 Important

È possibile utilizzare solo le chiavi KMS disponibili nello Regione AWS stesso bucket. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, devi inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione necessaria per l'uso della chiave e quindi inserire l'ARN della chiave KMS.

Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

13. Per utilizzare checksum aggiuntivi, scegli On (Attivato). Per Checksum function (Funzione checksum), scegli la funzione che desideri utilizzare. Amazon S3 calcola e archivia il valore del checksum dopo aver ricevuto l'intero oggetto. Puoi utilizzare la casella Precalculated value (Valore precalcolato) per fornire un valore precalcolato. In tal caso, Amazon S3 confronta il valore specificato con il valore calcolato. Se i due valori non corrispondono, Amazon S3 genera un errore.

I checksum aggiuntivi ti consentono di specificare l'algoritmo di checksum che desideri utilizzare per verificare i dati. Per ulteriori informazioni sui checksum aggiuntivi, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

14. Per aggiungere tag a tutti gli oggetti che si stanno caricando, scegliere Add tag (Aggiungi tag). Immetti un nome di tag nel campo Chiave. Immetti un valore per il tag.

Il tagging ti consente di catalogare lo storage. Ogni tag è una coppia chiave-valore. I valori delle chiavi e dei tag fanno distinzione tra maiuscole e minuscole. Puoi avere un massimo di 10 tag per oggetto. Una chiave di tag può essere composta da un massimo di 128 caratteri Unicode e i valori di tag possono essere composti da un massimo di 255 caratteri Unicode. Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#).

15. Per aggiungere metadati, seleziona Aggiungi metadati.

- a. In Tipo seleziona Definito dal sistema o Definito dall'utente.

Per i metadati definiti dal sistema, puoi selezionare intestazioni HTTP comuni, come e. Content-Type Content-Disposition Per un elenco di metadati definiti dal sistema e informazioni sulla possibilità di aggiungere il valore, consulta [System-defined metadati degli oggetti](#). Tutti i metadati che iniziano con il prefisso vengono trattati come metadati definiti dall'utente. x-amz-meta- User-defined metadati vengono archiviati con l'oggetto e vengono restituiti quando si scarica l'oggetto. Sia le chiavi che i relativi valori devono essere conformi agli standard. US-ASCII User-defined i metadati possono avere una dimensione massima di 2 KB. Per ulteriori informazioni sui metadati definiti dal sistema e definiti dall'utente, consulta [Utilizzo dei metadati degli oggetti](#).

- b. Per Chiave, seleziona una chiave.

- c. Digitare un valore per la chiave.

16. Per caricare i tuoi oggetti, scegli Carica.

Amazon S3 caricherà l'oggetto. Al termine del caricamento, sarà visualizzato un messaggio di successo nella pagina Carica: stato .

Utilizzo di AWS CLI

Il comando di put-object esempio seguente mostra come è possibile utilizzare il AWS CLI per caricare un oggetto tramite un punto di accesso.

Il comando seguente carica l'oggetto `puppy.jpg` per l' Account AWS **111122223333** utilizzo del punto ***my-access-point*** di accesso.

```
aws s3api put-object --bucket arn:aws:s3:Regione AWS:111122223333:accesspoint/my-  
access-point --key puppy.jpg --body puppy.jpg
```

Note

S3 genera automaticamente gli alias per tutti i punti di accesso e gli alias di punti di accesso possono essere utilizzati ovunque venga utilizzato un nome di bucket per eseguire operazioni a livello di oggetto. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

Per ulteriori informazioni ed esempi, consulta [put-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per caricare un oggetto tramite un punto di accesso. Per ulteriori informazioni, consulta [PutObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

È possibile utilizzare l' AWS SDK per Python per caricare un oggetto tramite un punto di accesso.

Python

Nell'esempio seguente, il file denominato ***hello.txt*** viene caricato per l' AWS account **111122223333** utilizzando il punto di accesso denominato ***my-access-point***

```
import boto3  
s3 = boto3.client('s3')  
s3.upload_file('/tmp/hello.txt', 'arn:aws:s3:us-east-1:111122223333:accesspoint/my-  
access-point', 'hello.txt')
```

Aggiunta di un set di tag tramite un punto di accesso per un bucket per uso generico

Questa sezione spiega come aggiungere un set di tag tramite un punto di accesso per un bucket generico utilizzando l'API Console di gestione AWS, AWS Command Line Interface, o REST. Per ulteriori informazioni, consulta [Etichettare i tuoi oggetti](#).

Utilizzo della console S3

Per aggiungere un set di tag tramite un punto di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.
6. Nella scheda Oggetti, seleziona il nome dell'oggetto a cui desideri aggiungere un set di tag.
7. Nella scheda Proprietà, trova il riquadro Tag e scegli Modifica.
8. Esamina gli oggetti elencati e scegli Aggiungi tag.
9. Ogni tag oggetto è una coppia chiave-valore. Immettere una chiave e un valore. Per aggiungere un altro tag, scegliere Add Tag (Aggiungi tag).

È possibile immettere fino a un massimo di 10 tag per ciascun oggetto.

10. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Il seguente comando di `put-object-tagging` esempio mostra come è possibile utilizzare il AWS CLI per aggiungere un set di tag tramite un punto di accesso.

Il comando seguente aggiunge un set di tag per un oggetto `puppy.jpg` esistente utilizzando il punto di accesso. *my-access-point*

```
aws s3api put-object-tagging --bucket arn:aws:s3:Regione
AWS:111122223333:accesspoint/my-access-point --key puppy.jpg --tagging
TagSet=[{Key="animal",Value="true"}]
```

Note

S3 genera automaticamente gli alias per tutti i punti di accesso e gli alias di punti di accesso possono essere utilizzati ovunque venga utilizzato un nome di bucket per eseguire operazioni a livello di oggetto. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

Per ulteriori informazioni ed esempi, consulta [put-object-tagging](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per aggiungere un set di tag a un oggetto tramite un punto di accesso. Per ulteriori informazioni, consulta [PutObjectTagging](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Eliminazione di un oggetto tramite un punto di accesso per un bucket per uso generico

Questa sezione spiega come eliminare un oggetto tramite un punto di accesso per un bucket generico utilizzando l'API Console di gestione AWS, AWS Command Line Interface, o REST.

Utilizzo della console S3

Per eliminare uno o più oggetti tramite un punto di accesso nel tuo Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione nella parte superiore della pagina, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione per la quale si desidera elencare i punti di accesso.
3. Nel riquadro di navigazione sul lato sinistro della console scegli Punti di accesso.
4. (Facoltativo) Cerca i punti di accesso per nome. Qui Regione AWS verranno visualizzati solo i punti di accesso selezionati.
5. Scegliere il nome del punto di accesso che si desidera gestire o utilizzare.

6. Nella scheda Oggetti, seleziona il nome dell'oggetto o degli oggetti da eliminare.
7. Esamina gli oggetti elencati per l'eliminazione e digita delete nella casella di conferma.
8. Scegliere Delete objects (Elimina oggetti).

Utilizzo di AWS CLI

Il seguente comando di `delete-object` esempio mostra come è possibile utilizzare il AWS CLI per eliminare un oggetto tramite un punto di accesso.

Il comando seguente elimina l'oggetto esistente `puppy.jpg` utilizzando il punto *my-access-point* di accesso.

```
aws s3api delete-object --bucket arn:aws:s3:Regione AWS:111122223333:accesspoint/my-access-point --key puppy.jpg
```

Note

S3 genera automaticamente gli alias per tutti i punti di accesso e gli alias di punti di accesso possono essere utilizzati ovunque venga utilizzato un nome di bucket per eseguire operazioni a livello di oggetto. Per ulteriori informazioni, consulta [Alias del punto di accesso](#).

Per ulteriori informazioni ed esempi, consulta [delete-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

È possibile utilizzare la REST API per eliminare un oggetto tramite un punto di accesso. Per ulteriori informazioni, consulta [DeleteObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di tag con punti di accesso S3 per bucket per uso generico

Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso Amazon S3 Access Points. È possibile applicare i tag ai punti di accesso al momento della creazione o gestire i tag dei punti di accesso esistenti. Per informazioni generali sui tag, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

 Note

Non sono previsti costi aggiuntivi per l'utilizzo dei tag sui punti di accesso oltre alle tariffe di richiesta API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Metodi comuni per utilizzare i tag con i punti di accesso

Attribute-based il controllo degli accessi (ABAC) consente di scalare le autorizzazioni di accesso e concedere l'accesso ai punti di accesso in base ai relativi tag. Per ulteriori informazioni su ABAC in Amazon S3, consulta [Utilizzo dei tag per ABAC](#).

ABAC per Punti di accesso S3

Punti di accesso Amazon S3 supporta il controllo degli accessi basato su attributi (ABAC) tramite tag. Utilizza le chiavi di condizione basate su tag nelle policy AWS delle tue organizzazioni, IAM e Access Points. Per le aziende, ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle policy IAM, è possibile controllare l'accesso ai punti di accesso in base ai tag dei punti di accesso utilizzando le seguenti [chiavi di condizione globali](#):

- `aws:ResourceTag/key-name`

 Important

La chiave di condizione `aws:ResourceTag` può essere utilizzata solo per le azioni S3 eseguite tramite l'ARN di un punto di accesso per bucket per uso generico e copre solo i tag del punto di accesso sottostante.

- Utilizzare questa chiave per confrontare la coppia chiave-valore del tag specificata nella policy con la coppia chiave-valore associata alla risorsa. Ad esempio, puoi richiedere che l'accesso a una risorsa sia consentito solo se la risorsa dispone di una chiave di tag `Dept` collegata al valore `Marketing`. Per ulteriori informazioni, consulta [Controllare l'accesso alle AWS risorse](#).
- `aws:RequestTag/key-name`
 - Utilizzare questa chiave per confrontare la coppia chiave-valore del tag passata nella richiesta con la coppia del tag specificata nella policy. Ad esempio, è possibile controllare che la richiesta includa la chiave del tag `Dept` e che abbia il valore `Accounting`. Per ulteriori informazioni,

vedere [Controllo dell'accesso durante AWS le richieste](#). È possibile utilizzare questa chiave di condizione per limitare quali coppie chiave-valore di tag possono essere passate durante le operazioni API TagResource e CreateAccessPoint.

- `aws:TagKeys`
 - Utilizzare questa chiave per confrontare le chiavi dei tag in una richiesta con quelle specificate nella policy. Nell'utilizzo delle policy per controllare gli accessi tramite tag, è consigliabile utilizzare la chiave di condizione `aws:TagKeys` per definire le chiavi di tag ammesse. Per esempi di policy e ulteriori informazioni, consulta [Controllo dell'accesso in base alle chiavi di tag](#). È possibile creare un punto di accesso con tag. Per consentire il tagging durante l'operazione API CreateAccessPoint, è necessario creare una policy che comprende entrambe le azioni `s3:TagResource` e `s3:CreateAccessPoint`. È quindi possibile utilizzare la chiave di condizione `aws:TagKeys` per implementare nella richiesta CreateAccessPoint specifici tag.
- `s3:AccessPointTag/tag-key`
 - Utilizzare questa chiave di condizione per fornire le autorizzazioni a dati specifici tramite punti di accesso con tag. Quando si utilizza `aws:ResourceTag/tag-key` in una policy IAM, sia il punto di accesso sia il bucket a cui punta il punto di accesso devono avere lo stesso tag perché entrambi vengono presi in considerazione durante l'autorizzazione. Per controllare l'accesso ai dati in modo specifico solo tramite il tag del punto di accesso, è possibile utilizzare la chiave di condizione `s3:AccessPointTag/tag-key`.

Esempi di policy ABAC per i punti di accesso

Di seguito sono riportati esempi di policy ABAC per Punti di accesso Amazon S3.

1.1 - Policy IAM per creare o modificare bucket con tag specifici

In questa policy IAM, gli utenti o i ruoli con questa policy possono creare punti di accesso solo se applicano ai punti di accesso i tag con la chiave di tag `project` e il valore di tag `Trinity` nella richiesta di creazione dei punti di accesso. Possono anche aggiungere o modificare i tag sui punti di accesso esistenti, purché la richiesta TagResource includa la coppia chiave-valore `project:Trinity` del tag.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAccessPointWithTags",
```



```

    "Effect": "Allow",
    "Action": [
        "s3:CreateAccessPoint",
        "s3:TagResource"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/project": [
                "Trinity"
            ]
        }
    }
}

```

1.2 - Policy del punto di accesso per limitare le operazioni sul punto di accesso con tag

In questa policy del punto di accesso, i principali IAM (utenti e ruoli) possono eseguire operazioni utilizzando l'azione `GetObject` sul punto di accesso solo se il valore del tag `project` del punto di accesso corrisponde al valore del tag `project` del principale.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowObjectOperations",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws::s3:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
            "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
          }
      }
    }
  ]
}

```

1.3 - Policy IAM per modificare i tag sulle risorse esistenti mantenendo la governance dei tag

In questa policy IAM, i principali IAM (utenti o ruoli) possono modificare i tag su un punto di accesso solo se il valore del tag `project` del punto di accesso corrisponde al valore del tag `project` del principale. Solo i quattro tag `project`, `environment`, `owner` e `cost-center` specificati nelle chiavi di condizione `aws:TagKeys` sono consentiti per questi punti di accesso. Ciò aiuta a rafforzare la governance dei tag, impedisce modifiche non autorizzate dei tag e mantiene lo schema di tagging coerente tra i punti di accesso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3:TagResource"
      ],
      "Resource": "arn:aws::s3:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",
            "owner",
            "cost-center"
          ]
        }
      }
    }
  ]
}
```

1.4 - Utilizzo della chiave s3: AccessPointTag condition

In questa policy IAM, l'istruzione di condizione consente l'accesso ai dati del bucket se il punto di accesso ha la chiave di tag `Environment` e il valore di tag `Production`.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowAccessToSpecificAccessPoint",
    "Effect": "Allow",
    "Action": "*",
    "Resource": "arn:aws::s3:region:111122223333:accesspoint/my-access-point",
    "Condition": {
      "StringEquals": {
        "s3:AccessPointTag/Environment": "Production"
      }
    }
  }
]
}

```

1.5 - Utilizzo di una policy di delega del bucket

In Amazon S3, puoi delegare l'accesso o il controllo della tua policy del bucket S3 a un altro AWS account o a un utente o ruolo specifico AWS Identity and Access Management (IAM) nell'altro account. La policy di bucket con delega fornisce all'altro account, utente o ruolo l'autorizzazione al bucket e ai suoi oggetti. Per ulteriori informazioni, consulta [Delega delle autorizzazioni](#).

Se si utilizza una policy di bucket con delega, come la seguente:

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Principal": {"AWS": "*"},
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource": ["arn:aws::s3::amzn-s3-demo-bucket/*", "arn:aws::s3::amzn-s3-demo-bucket"],
    "Condition": {
      "StringEquals" : {
        "s3:DataAccessPointAccount" : "111122223333"
      }
    }
  }
}

```

Nella seguente policy IAM, l'istruzione condizionale consente l'accesso ai dati del bucket se il punto di accesso ha la chiave di tag Environment e il valore di tag Production.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToSpecificAccessPoint",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws::s3:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "s3:AccessPointTag/Environment": "Production"
        }
      }
    }
  ]
}
```

Utilizzo dei tag per i punti di accesso per bucket per uso generico

Puoi aggiungere o gestire tag per i punti di accesso utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI), gli AWS SDK o utilizzando le API S3:, e. [TagResource](#) [UntagResource](#) [ListTagsForResource](#) Per ulteriori informazioni, consulta:

Argomenti

- [Creazione di punti di accesso con tag](#)
- [Aggiunta di tag a un punto di accesso](#)
- [Visualizzazione dei tag dei punti di accesso](#)
- [Eliminazione di un tag da un punto di accesso](#)

Creazione di punti di accesso con tag

È possibile applicare i tag ai punti di accesso al momento della loro creazione. Non sono previsti costi aggiuntivi per l'utilizzo dei tag sui punti di accesso oltre alle tariffe di richiesta API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sul tagging dei punti di accesso, consulta [Utilizzo di tag con punti di accesso S3 per bucket per uso generico](#).

Permissions

Per creare un punto di accesso con tag, è necessario disporre delle seguenti autorizzazioni:

- `s3:CreateBucket`
- `s3:TagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di creare un punto di accesso con tag, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per creare il punto di accesso e aggiungervi un tag.
- Controllare la policy dell'utente IAM per eventuali condizioni del controllo degli accessi basato su attributi (ABAC). Potrebbe essere necessario etichettare i punti di accesso solo con chiavi e valori di tag specifici. Per ulteriori informazioni, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

Fasi

Puoi creare un punto di accesso con tag applicati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e AWS gli SDK.

Utilizzo della console S3

Per creare un punto di accesso con tag utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso (bucket per uso generico).
3. Scegli Crea punto di accesso per creare un nuovo punto di accesso.
4. Nella pagina Crea punto di accesso, Tag è un'opzione per la creazione di un nuovo punto di accesso.
5. Immetti un nome per il punto di accesso. Per ulteriori informazioni, consulta [Regole di denominazione, restrizioni e limitazioni dei punti di accesso](#).
6. Scegli Aggiungi nuovo tag per aprire l'editor di tag e inserisci una coppia chiave-valore di tag. La chiave di tag è obbligatoria, mentre il valore è facoltativo.
7. Per aggiungere un altro tag, scegli nuovamente Aggiungi nuovo tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
8. Dopo aver specificato le opzioni per il nuovo punto di accesso, scegli Crea punto di accesso.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come creare un punto di accesso con tag utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
CreateAccessPointRequest createAccessPointRequest =  
    CreateAccessPointRequest.builder()  
        .accountId(111122223333)  
        .name(my-access-point)  
        .bucket(amzn-s3-demo-bucket)  
  
        .tags(Collections.singletonList(Tag.builder().key("key1").value("value1").build()))  
        .build();  
awss3Control.createAccessPoint(createAccessPointRequest);
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la creazione di un punto di accesso con tag, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [CreateAccessPoint](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come creare un punto di accesso con tag utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control create-access-point --name my-access-point \  
--bucket amzn-s3-demo-bucket \  
--account-id 111122223333 \ --profile personal \  
--tags [{Key=key1,Value=value1},{Key=key2,Value=value2}] \  
--region region
```

Aggiunta di tag a un punto di accesso

È possibile aggiungere i tag ai Punti di accesso Amazon S3 e modificare questi tag. Non sono previsti costi aggiuntivi per l'utilizzo dei tag sui punti di accesso oltre alle tariffe di richiesta API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sul tagging dei punti di accesso, consulta [Utilizzo di tag con punti di accesso S3 per bucket per uso generico](#).

Permissions

Per aggiungere un tag a un punto di accesso, è necessario disporre della seguente autorizzazione:

- `s3:TagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di aggiungere un tag a un punto di accesso, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per aggiungere un tag a un punto di accesso.
- Se hai tentato di aggiungere una chiave tag che inizia con il prefisso AWS riservato `aws:`, cambia la chiave del tag e riprova.

Fasi

Puoi aggiungere tag ai punti di accesso utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per aggiungere tag a un punto di accesso utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso (bucket per uso generico).
3. Scegliere il nome del punto di accesso.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri la sezione Tag e scegli Aggiungi nuovo tag.
6. Viene visualizzata la pagina Aggiungi tag. È possibile inserire fino a 50 coppie chiave-valore di tag.

7. Se si aggiunge un nuovo tag con lo stesso nome di chiave di un tag esistente, il valore del nuovo tag sovrascrive il valore del tag esistente.
8. In questa pagina è anche possibile modificare i valori dei tag esistenti.
9. Dopo aver aggiunto i tag, scegli Salva le modifiche.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come aggiungere tag a un punto di accesso utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
TagResourceRequest tagResourceRequest =
    TagResourceRequest.builder().resourceArn(arn:aws:s3:region:111122223333:accesspoint/
my-access-point/*)
    .accountId(111122223333)
    .tags(List.of(Tag.builder().key("key1").value("value1").build(),
Tag.builder().key("key2").value("value2").build()))
    .build();
awss3Control.tagResource(tagResourceRequest);
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'aggiunta di tag a un punto di accesso, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [TagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come aggiungere tag a un punto di accesso utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:


```
aws s3control tag-resource \  
--account-id 111122223333 \  
--resource-arn arn:aws::s3:region:111122223333:accesspoint/my-access-point/* \  
--tags "Key=key1,Value=value1"
```

Risposta:

```
{  
  "ResponseMetadata": {  
    "RequestId": "EXAMPLE123456789",  
    "HTTPStatusCode": 200,  
    "HTTPHeaders": {  
      "date": "Wed, 19 Jun 2025 10:30:00 GMT",  
      "content-length": "0"  
    },  
    "RetryAttempts": 0  
  }  
}
```

Visualizzazione dei tag dei punti di accesso

È possibile visualizzare o elencare i tag applicati ai punti di accesso. Per ulteriori informazioni sui tag, consulta [Utilizzo di tag con punti di accesso S3 per bucket per uso generico](#).

Permissions

Per visualizzare i tag applicati a un punto di accesso, è necessario disporre della seguente autorizzazione:

- `s3:ListTagsForResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di elencare o visualizzare i tag di un punto di accesso, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per visualizzare o elencare i tag del punto di accesso.

Fasi

Puoi visualizzare i tag applicati ai punti di accesso utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare i tag applicati a un punto di accesso utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso (bucket per uso generico).
3. Scegliere il nome del punto di accesso.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag per visualizzare tutti i tag applicati al punto di accesso.
6. La sezione Tag mostra i User-defined tag per impostazione predefinita. È possibile selezionare la scheda dei tag AWS generati per visualizzare i tag applicati al punto di accesso dai AWS servizi.

Utilizzo di AWS SDK

Questa sezione fornisce un esempio di come visualizzare i tag applicati a un punto di accesso utilizzando gli AWS SDK.

SDK for Java 2.x

Questo esempio mostra come visualizzare i tag applicati a un punto di accesso utilizzando AWS SDK for Java 2.x.

```
ListTagsForResourceRequest listTagsForResourceRequest = ListTagsForResourceRequest
    .builder().resourceArn(arn:aws::s3:region:111122223333:accesspoint/my-access-point/
        *)
        .accountId(111122223333).build();
awss3Control.listTagsForResource(listTagsForResourceRequest);
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la visualizzazione dei tag applicati a un punto di accesso, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [ListTagsforResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come visualizzare i tag applicati un punto di accesso. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control list-tags-for-resource \  
--account-id 111122223333 \  
--resource-arn arn:aws::s3:region:444455556666:bucket/prefix--use1-az4--x-s3 \  

```

Risposta con tag:

```
{  
  "Tags": [  
    {  
      "Key": "MyKey1",  
      "Value": "MyValue1"  
    },  
    {  
      "Key": "MyKey2",  
      "Value": "MyValue2"  
    },  
    {  
      "Key": "MyKey3",  
      "Value": "MyValue3"  
    }  
  ]  
}
```

Risposta senza tag:

```
{  
  "Tags": []  
}
```

Eliminazione di un tag da un punto di accesso

È possibile rimuovere i tag dai Punti di accesso Amazon S3. Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso gli Access Point. Per ulteriori informazioni sui tag, consulta [Utilizzo di tag con punti di accesso S3 per bucket per uso generico](#).

Note

Se si elimina un tag e in seguito si scopre che veniva utilizzato per monitorare i costi o per il controllo degli accessi, è possibile aggiungere nuovamente il tag al punto di accesso.

Permissions

Per eliminare un tag da un punto di accesso, è necessario disporre della seguente autorizzazione:

- `s3:UntagResource`

Risoluzione degli errori

Se si verifica un errore durante il tentativo di eliminare un tag da un punto di accesso, è possibile effettuare quanto segue:

- Verificare di disporre delle [Permissions](#) richieste per eliminare un tag da un punto di accesso.

Fasi

Puoi eliminare i tag dai punti di accesso utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per eliminare i tag da un punto di accesso utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Punti di accesso (bucket per uso generico).
3. Scegliere il nome del punto di accesso.
4. Scegliere la scheda Properties (Proprietà).

5. Scorri fino alla sezione Tag e seleziona la casella di controllo accanto al tag o ai tag che desideri eliminare.
6. Scegliere Elimina.
7. Viene visualizzato il pop-up Elimina tag definiti dall'utente che chiede di confermare l'eliminazione del tag o dei tag selezionati.
8. Seleziona Elimina per confermare.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come eliminare i tag da un punto di accesso utilizzando AWS SDK for Java 2.x. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

```
UntagResourceRequest tagResourceRequest = UntagResourceRequest.builder()
    .resourceArn(arn:aws:s3:region:111122223333:accesspoint/my-access-
point/*)
    .accountId(111122223333)
    .tagKeys(List.of("key1", "key2")).build();
awss3Control.untagResource(tagResourceRequest);
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'eliminazione dei tag da un punto di accesso, consulta la sezione seguente nella Guida di riferimento delle API di Amazon Simple Storage Service:

- [UnTagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Il seguente esempio della CLI mostra come eliminare i tag da un punto di accesso utilizzando la AWS CLI. Per utilizzare il comando, sostituiscilo *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control untag-resource \  
--account-id 111122223333 \  
--resource-arn arn:aws::s3:region:444455556666:access-point/my-access-point \  
--tag-keys "tagkey1" "tagkey2"  
  
aws s3control untag-resource \  
--account-id 111122223333 \  
--resource-arn arn:aws::s3:region:444455556666:accesspointmy-access-point/* \  
--tag-keys "key1" "key2"
```

Risposta:

```
{  
  "ResponseMetadata": {  
    "RequestId": "EXAMPLE123456789",  
    "HTTPStatusCode": 204,  
    "HTTPHeaders": {  
      "date": "Wed, 19 Jun 2025 10:30:00 GMT",  
      "content-length": "0"  
    },  
    "RetryAttempts": 0  
  }  
}
```

Gestione dell'accesso con S3 Access Grants

Per aderire al principio del privilegio minimo, definisci l'accesso granulare ai dati di Amazon S3 in base ad applicazioni, personaggi, gruppi o unità organizzative. Puoi utilizzare diversi approcci per ottenere un accesso granulare ai tuoi dati in Amazon S3, a seconda della dimensione e della complessità dei modelli di accesso.

L'approccio più semplice per gestire l'accesso a un numero medio-piccolo di set di dati in Amazon S3 tramite principali AWS Identity and Access Management (IAM) consiste nel definire le [policy di autorizzazione IAM](#) e le [policy dei bucket S3](#). Questa strategia funziona, a condizione che le policy necessarie rientrino nei limiti di dimensione delle policy del bucket S3 (20 KB) e delle policy IAM (5 KB), nonché nel [numero di principali IAM consentiti per account](#).

Man mano che il numero di set di dati e di casi d'uso aumenta, potresti aver bisogno di più spazio per le policy. Un approccio che offre uno spazio significativamente maggiore per le istruzioni di policy consiste nell'utilizzare i [Punti di accesso S3](#) come endpoint aggiuntivi per i bucket S3, poiché ogni punto di accesso può avere una propria policy. È possibile definire schemi di controllo degli accessi piuttosto granulari, poiché è possibile avere migliaia di punti di accesso Regione AWS per account, con una politica di dimensioni fino a 20 KB per ogni punto di accesso. Sebbene i Punti di accesso S3 aumentino la quantità di spazio disponibile per le policy, è necessario un meccanismo che consenta ai client di individuare il punto di accesso corretto per il set di dati corretto.

Un terzo approccio consiste nell'implementare un modello di [broker di sessione IAM](#), in cui si implementa la logica di decisione di accesso e si generano dinamicamente credenziali di sessione IAM a breve termine per ogni sessione di accesso. Mentre l'approccio del broker di sessione IAM supporta arbitrariamente modelli di autorizzazioni dinamici nonché una scalabilità efficace, è necessario costruire la logica dei modelli di accesso.

Invece di utilizzare questi approcci, è possibile utilizzare S3 Access Grants per gestire l'accesso ai dati Amazon S3. S3 Access Grants fornisce un modello semplificato per definire le autorizzazioni di accesso ai dati in Amazon S3 per prefisso, bucket o oggetto. Inoltre, puoi utilizzare S3 Access Grants per concedere l'accesso sia ai principali IAM che direttamente a utenti o gruppi dalla tua directory aziendale.

In genere si definiscono le autorizzazioni per i dati in Amazon S3 mappando utenti e gruppi a set di dati. Puoi utilizzare S3 Access Grants per definire mappature di accesso diretto dei prefissi S3 a utenti e ruoli all'interno di bucket e oggetti Amazon S3. Con lo schema di accesso semplificato di S3 Access Grants, puoi concedere l'accesso in sola lettura, sola scrittura o lettura-scrittura su S3-prefix base individuale sia ai principali IAM sia direttamente agli utenti o ai gruppi da una directory aziendale. Con queste funzionalità di S3 Access Grants, le applicazioni possono richiedere dati da Amazon S3 per conto dell'utente attualmente autenticato dell'applicazione.

Quando integri S3 Access Grants con la [funzionalità di propagazione delle identità](#) attendibili di Centro identità AWS IAM, le tue applicazioni possono effettuare richieste Servizi AWS (incluse S3 Access Grants) direttamente per conto di un utente autenticato della directory aziendale. Le tue applicazioni non devono più mappare prima l'utente a un principale IAM. Inoltre, poiché le identità degli utenti finali vengono propagate fino ad Amazon S3, l'audit degli utenti che hanno avuto accesso a un determinato oggetto S3 è semplificato. Non è più necessario ricostruire la relazione tra diversi utenti e sessioni IAM. Quando utilizzi S3 Access Grants con la propagazione delle identità attendibili del Centro identità IAM, ogni evento relativo ai dati [AWS CloudTrail](#) per Amazon S3 contiene un riferimento diretto all'utente finale per conto del quale è stato effettuato l'accesso ai dati.

[La propagazione affidabile delle identità](#) è una Centro identità AWS IAM funzionalità che gli amministratori di connected Servizi AWS possono utilizzare per concedere e controllare l'accesso ai dati del servizio. L'accesso a questi dati si basa su attributi utente come le associazioni di gruppo. L'impostazione di una propagazione affidabile delle identità richiede la collaborazione tra gli amministratori di connected Servizi AWS e gli amministratori dello IAM Identity Center. Per ulteriori informazioni, consulta [Prerequisites and considerations](#).

Per ulteriori informazioni sugli S3 Access Grants, consulta i seguenti argomenti.

Argomenti

- [Concetti di S3 Access Grants](#)
- [S3 Access Grants e identità delle directory aziendali](#)
- [Nozioni di base su S3 Access Grants](#)
- [Operazioni con le istanze S3 Access Grants](#)
- [Operazioni con le posizioni S3 Access Grants](#)
- [Operazioni con le concessioni in S3 Access Grants](#)
- [Ottenere i dati S3 utilizzando i grant di accesso](#)
- [Accesso multi-account S3 Access Grants](#)
- [Gestione dei tag per S3 Access Grants](#)
- [Limitazioni di S3 Access Grants](#)
- [Integrazioni con S3 Access Grants](#)

Concetti di S3 Access Grants

Flusso di lavoro per S3 Access Grants

Il flusso di lavoro per S3 Access Grants è il seguente:

1. Crea un'istanza S3 Access Grants. Consulta [Operazioni con le istanze S3 Access Grants](#).
2. All'interno della tua istanza S3 Access Grants, registra le posizioni nei tuoi dati Amazon S3 e associale ai ruoli (IAM). AWS Identity and Access Management Consulta [Registrazione di una posizione](#).
3. Crea concessioni per i beneficiari, che danno loro accesso alle tue risorse S3. Consulta [Operazioni con le concessioni in S3 Access Grants](#).

4. Il beneficiario richiede le credenziali temporanee a S3 Access Grants. Consulta [Richiedi l'accesso ai dati di Amazon S3 tramite S3 Access Grants](#).
5. Il beneficiario accede ai dati S3 utilizzando queste credenziali temporanee. Consulta [Accedere ai dati S3 utilizzando le credenziali fornite da S3 Access Grants](#).

Per ulteriori informazioni, consulta [Nozioni di base su S3 Access Grants](#).

Istanze S3 Access Grants

Un'istanza S3 Access Grants è un container logico per singole concessioni. Quando si crea un'istanza S3 Access Grants, è necessario specificare Regione AWS. Ciascuna Regione AWS delle tue Account AWS può avere un'istanza S3 Access Grants. Per ulteriori informazioni, consulta [Operazioni con le istanze S3 Access Grants](#).

Se desideri utilizzare S3 Access Grants per concedere l'accesso alle identità di utenti e gruppi dalla tua directory aziendale, devi anche associare l'istanza S3 Access Grants a un'istanza. Centro identità AWS IAM Per ulteriori informazioni, consulta [S3 Access Grants e identità delle directory aziendali](#).

Un'istanza S3 Access Grants appena creata è vuota. È necessario registrare una posizione nell'istanza, che può essere il percorso predefinito di S3 (`s3://`), un bucket o un prefisso all'interno di un bucket. Dopo aver registrato almeno un'ubicazione, è possibile creare dei permessi di accesso che consentono di accedere ai dati di questa ubicazione registrata.

Posizioni

Una sede di S3 Access Grants associa bucket o prefissi a un ruolo (IAM). AWS Identity and Access Management S3 Access Grants assume questo ruolo IAM per vendere credenziali temporanee al beneficiario che accede a quella particolare posizione. Prima di poter creare una concessione di accesso, è necessario registrare almeno una posizione nell'istanza S3 Access Grants.

Si consiglia di registrare la posizione predefinita (`s3://`) e di mapparla a un ruolo IAM. La posizione nel percorso S3 predefinito (`s3://`) copre l'accesso a tutti i bucket S3 nel tuo account. Regione AWS Quando si crea una concessione di accesso, è possibile restringere l'ambito della concessione a un bucket, a un prefisso o a un oggetto all'interno della posizione predefinita.

Casi di utilizzo della gestione degli accessi più complessi potrebbero richiedere la registrazione di più posizioni rispetto a quella predefinita. Alcuni esempi di questi casi d'uso sono:

- Si supponga che il bucket *amzn-s3-demo-bucket* sia una posizione registrata nella tua istanza S3 Access Grants con un ruolo IAM mappato su di essa, ma a questo ruolo IAM sia negato l'accesso a un particolare prefisso all'interno del bucket. In questo caso, è possibile registrare il prefisso a cui il ruolo IAM non ha accesso come posizione separata e mappare tale posizione a un altro ruolo IAM con l'accesso necessario.
- Si supponga di voler creare dei grant che limitino l'accesso solo agli utenti all'interno di un endpoint di un cloud privato virtuale (VPC). In questo caso, è possibile registrare una posizione per un bucket in cui il ruolo IAM limita l'accesso all'endpoint VPC. Successivamente, quando un beneficiario chiede le credenziali a S3 Access Grants, S3 Access Grants assume il ruolo IAM della sede per vendere le credenziali temporanee. Questa credenziale negherà l'accesso al bucket specifico a meno che il chiamante non si trovi all'interno dell'endpoint VPC. Questa autorizzazione di negazione viene applicata in aggiunta alle normali autorizzazioni READ, WRITE o READWRITE specificate nella concessione.

Se il caso d'uso richiede la registrazione di più posizioni nell'istanza di S3 Access Grants, è possibile registrare uno dei seguenti elementi:

- Il percorso S3 predefinito (`s3://`)
- Un bucket (ad esempio, *amzn-s3-demo-bucket*) o più bucket
- Un bucket e un prefisso (ad esempio, *amzn-s3-demo-bucket/prefix**) o più prefissi

Per il numero massimo di sedi che è possibile registrare nell'istanza di S3 Access Grants, consulta [Limitazioni di S3 Access Grants](#). Per ulteriori informazioni sulla registrazione di una posizione S3 Access Grants, consulta [Registrazione di una posizione](#).

Dopo aver registrato la prima posizione nell'istanza S3 Access Grants, l'istanza non ha ancora alcun singolo accesso garantito. Pertanto, non è ancora stato concesso l'accesso a nessuno dei dati S3. È ora possibile creare concessioni di accesso per concedere l'accesso. Per ulteriori informazioni sulla creazione di concessioni, consulta [Operazioni con le concessioni in S3 Access Grants](#).

Concessioni

Una concessione individuale in un'istanza S3 Access Grants consente a un'identità specifica, un principale IAM o un utente o un gruppo di una directory aziendale, di ottenere l'accesso all'interno di una posizione registrata nell'istanza S3 Access Grants.

Quando si crea una concessione, non è necessario concedere l'accesso all'intera postazione registrata. È possibile restringere l'ambito di accesso della concessione all'interno di una località.

Se la posizione registrata è il percorso S3 predefinito (`s3://`), è necessario restringere l'ambito della concessione a un bucket, a un prefisso all'interno di un bucket o a un oggetto specifico. Se la posizione registrata del grant è un bucket o un prefisso, si può dare accesso all'intero bucket o prefisso, oppure si può restringere l'ambito del grant a un prefisso, sottoprefisso o oggetto.

Nella concessione, si imposta anche il livello di accesso della concessione su `READ`, `WRITE` o `READWRITE`. Si supponga di avere una concessione che dia al gruppo della directory aziendale `01234567-89ab-cdef-0123-456789abcdef` l'accesso in lettura al bucket `s3://amzn-s3-demo-bucket/projects/items/*`. Gli utenti di questo gruppo possono avere accesso in modalità `READ` a tutti gli oggetti che hanno un nome di chiave dell'oggetto che inizia con il prefisso `projects/items/` nel bucket denominato *amzn-s3-demo-bucket*.

Per il numero massimo di concessioni che è possibile creare nell'istanza S3 Access Grants, consulta [Limitazioni di S3 Access Grants](#). Per ulteriori informazioni sulla creazione di concessioni, consulta [Creazione di concessioni](#).

Credenziali temporanee di S3 Access Grants

Dopo aver creato una concessione, un'applicazione autorizzata che utilizza l'identità specificata nella concessione può richiedere le credenziali di accesso just-in-time. Per fare ciò, l'applicazione chiama l'operazione API [GetDataAccess](#) S3. I beneficiari possono utilizzare questa operazione API per richiedere l'accesso ai dati S3 che hai condiviso con loro.

L'istanza S3 Access Grants valuta la richiesta `GetDataAccess` rispetto alle concessioni di cui dispone. Se esiste una concessione corrispondente per il richiedente, S3 Access Grants assume il ruolo IAM associato alla posizione registrata del grant corrispondente. S3 Access Concede i permessi delle credenziali temporanee per accedere solo al bucket, al prefisso o all'oggetto S3 specificato dall'ambito del grant.

Il tempo di scadenza delle credenziali di accesso temporanee è predefinito a 1 ora, ma è possibile impostarlo su qualsiasi valore compreso tra 15 minuti e 12 ore. Vedi la durata massima della sessione nel riferimento [AssumeRole](#) API.

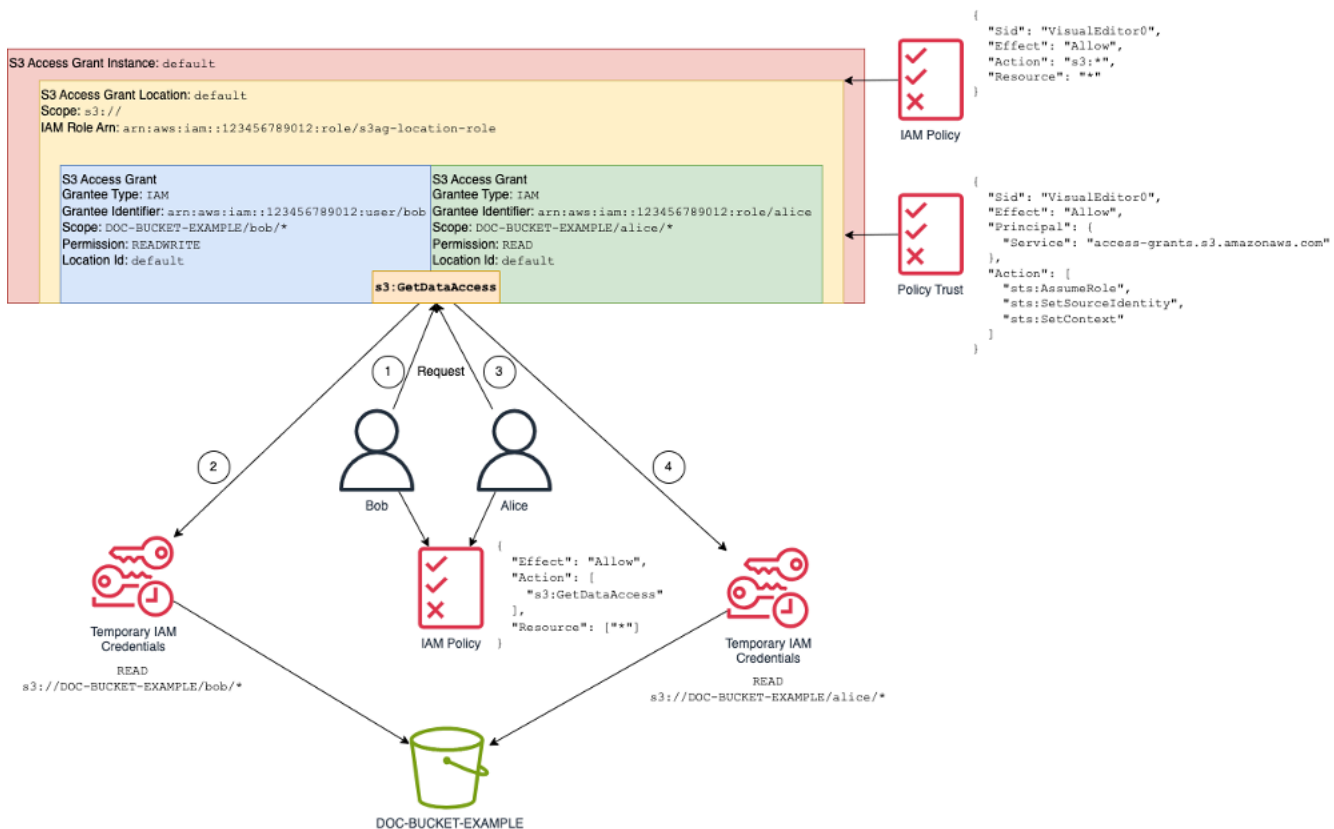
Come funziona

Nel diagramma seguente, una posizione Amazon S3 predefinita con l'ambito `s3://` è registrata con il ruolo IAM `s3ag-location-role`. Questo ruolo IAM dispone delle autorizzazioni per eseguire azioni Amazon S3 all'interno dell'account quando le sue credenziali vengono ottenute tramite S3 Access Grants.

In questa posizione, vengono create due concessioni di accesso individuali per due utenti IAM. All'utente IAM Bob vengono concessi gli accessi READ e WRITE al prefisso bob/ nel bucket DOC-BUCKET-EXAMPLE. A un altro ruolo IAM, Alice, viene concesso solo l'accesso a READ sul prefisso alice/ nel bucket DOC-BUCKET-EXAMPLE. Viene definita una concessione, colorata in blu, per consentire a Bob di accedere al prefisso bob/ nel bucket DOC-BUCKET-EXAMPLE. Viene definita una concessione, colorata in verde, per consentire ad Alice di accedere al prefisso alice/ nel bucket DOC-BUCKET-EXAMPLE.

Quando è il momento per Bob di elaborare READ i dati, il ruolo IAM associato alla sede in cui si trova la sua concessione chiama l'operazione [GetDataAccess](#) API S3 Access Grants. Se Bob tenta di leggere (READ) un qualsiasi prefisso o oggetto S3 che inizia con s3://DOC-BUCKET-EXAMPLE/bob/*, la richiesta GetDataAccess restituisce un set di credenziali di sessione IAM temporanee con autorizzazione a s3://DOC-BUCKET-EXAMPLE/bob/*. Allo stesso modo, Bob può scrivere (WRITE) su qualsiasi prefisso o oggetto S3 che inizi con s3://DOC-BUCKET-EXAMPLE/bob/*, perché anche la concessione lo consente.

Alice, invece, può leggere (READ) tutto ciò che inizia con s3://DOC-BUCKET-EXAMPLE/alice/. Tuttavia, se prova a scrivere (WRITE) qualunque cosa su un qualsiasi bucket, prefisso o oggetto in s3://, riceverà un errore Accesso negato (403), perché non esiste alcuna concessione che le dia accesso in scrittura (WRITE) ai dati. Inoltre, se Alice richiede un qualsiasi livello di accesso (READ o WRITE) ai dati esterni as3://DOC-BUCKET-EXAMPLE/alice/, riceverà nuovamente un errore di accesso negato.



Questo modello si adatta a un numero elevato di utenti e bucket e semplifica la gestione di tali autorizzazioni. Aniché modificare le policy dei bucket S3 potenzialmente grandi ogni volta che desideri aggiungere o rimuovere una relazione di accesso prefisso-utente individuale, puoi aggiungere e rimuovere concessioni individuali e discrete.

S3 Access Grants e identità delle directory aziendali

Puoi utilizzare Amazon S3 Access Grants per concedere l'accesso ai principali AWS Identity and Access Management (IAM) (utenti o ruoli), sia nello stesso che in altri. Account AWS Tuttavia, in molti casi, l'entità che accede ai dati è un utente finale della directory aziendale. Invece di concedere l'accesso ai principali IAM, puoi utilizzare S3 Access Grants per concedere l'accesso direttamente agli utenti e ai gruppi aziendali. Con S3 Access Grants, non è più necessario mappare le identità aziendali a principali IAM intermedi per accedere ai dati S3 tramite le applicazioni aziendali.

Questa nuova funzionalità, il supporto per l'utilizzo delle identità degli utenti finali per l'accesso ai dati, viene fornita associando l'istanza S3 Access Grants a un'istanza. Centro identità AWS IAM Identity Center supporta provider di identità basati su standard ed è il fulcro di qualsiasi servizio o funzionalità, incluso S3 Access Grants, che supporta le identità degli utenti finali AWS. Il Centro identità IAM fornisce supporto per l'autenticazione delle identità aziendali attraverso la

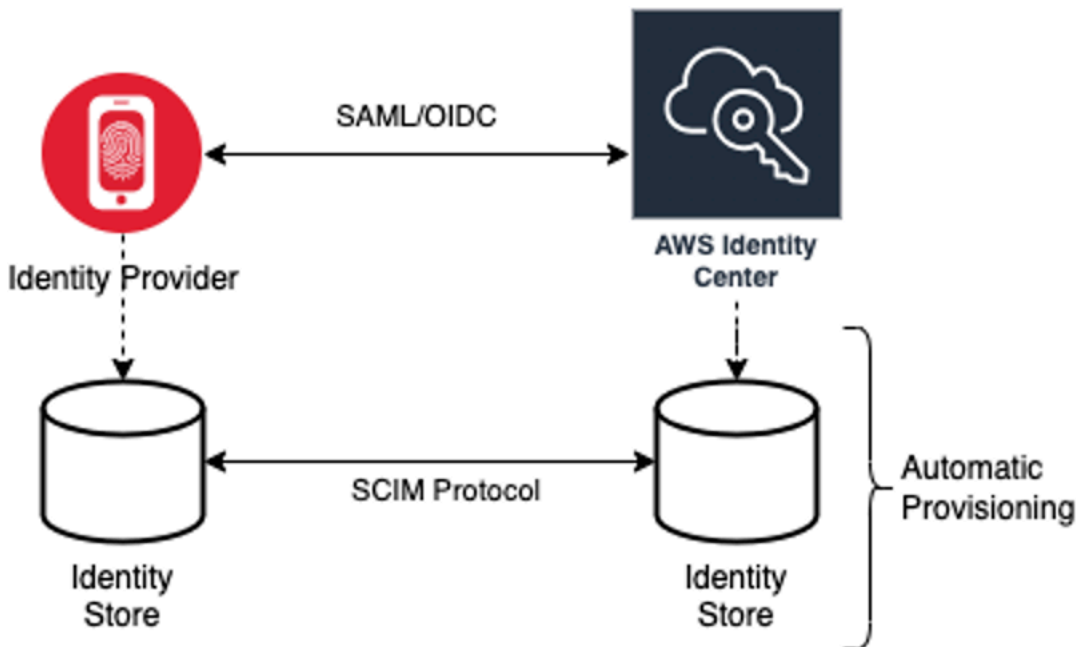
sua funzionalità Propagazione delle identità attendibili. Per ulteriori informazioni, consulta la pagina [Propagazione delle identità attendibili tra le applicazioni](#).

Prima di iniziare con il supporto delle identità della forza lavoro in S3 Access Grants, devi configurare il provisioning delle identità tra il tuo gestore delle identità aziendali e il Centro identità IAM, come prerequisito. IAM Identity Center supporta provider di identità aziendali come Okta Microsoft Entra ID (precedentemente Azure Active Directory) o qualsiasi altro provider di identità esterno (IdP) che supporti il protocollo System for Identity Management (SCIM). Cross-domain Quando connetti il Centro identità IAM al tuo gestore dell'identità digitale (IdP) e abiliti il provisioning automatico, gli utenti e i gruppi del tuo IdP vengono sincronizzati nell'archivio di identità nel Centro identità IAM. Dopo questo passaggio, IAM Identity Center ha una propria visione degli utenti e dei gruppi, in modo da potervi fare riferimento utilizzando altre funzionalità, come Servizi AWS S3 Access Grants. Per ulteriori informazioni sulla configurazione del provisioning automatico del Centro identità IAM, consulta la sezione [Provisioning automatico](#) nella Guida per l'utente di Centro identità AWS IAM .

IAM Identity Center è integrato AWS Organizations in modo da poter gestire centralmente le autorizzazioni su più account Account AWS senza configurare manualmente ciascuno dei tuoi account. In un'organizzazione tipica, l'amministratore delle identità configura un'istanza del Centro identità IAM per l'intera organizzazione, come unico punto di sincronizzazione delle identità. Questa istanza di IAM Identity Center viene in genere eseguita in un ambiente dedicato all' Account AWS interno dell'organizzazione. In questa configurazione comune, puoi fare riferimento alle identità di utenti e gruppi in S3 Access Grants di qualsiasi Account AWS membro dell'organizzazione.

Tuttavia, se AWS Organizations l'amministratore non ha ancora configurato un'istanza centrale di IAM Identity Center, puoi crearne una locale nello stesso account e Regione AWS nell'istanza S3 Access Grants. Se hai un'istanza IAM Identity Center configurata in un'istanza diversa Regione AWS, puoi anche [replicare](#) questa istanza nella Regione AWS stessa istanza di S3 Access Grants. Questa configurazione è più comune per i casi di proof-of-concept o di sviluppo locale. In tutti i casi, l'istanza IAM Identity Center deve trovarsi nella Regione AWS stessa istanza S3 Access Grants a cui sarà associata.

Nel diagramma seguente di una configurazione del Centro identità IAM con un gestore dell'identità digitale (IdP) esterno, l'IdP è configurato con SCIM per sincronizzare l'archivio di identità dal gestore dell'IdP all'archivio di identità nel Centro identità IAM.



Per utilizzare le identità delle directory aziendali con S3 Access Grants, procedi come segue:

- Configura il [provisioning automatico](#) nel Centro identità IAM per sincronizzare le informazioni su utenti e gruppi dal tuo gestore dell'identità digitale (IdP) nel Centro identità IAM.
- Configura l'origine di identità esterna nel Centro identità IAM come emittente del token affidabile. Per ulteriori informazioni, consulta la pagina [Propagazione delle identità attendibili tra le applicazioni](#) nella Guida per l'utente di Centro identità AWS IAM .
- Associa l'istanza S3 Access Grants all'istanza del Centro identità IAM. Puoi farlo quando [crei la tua istanza S3 Access Grants](#). Se hai già creato la tua istanza S3 Access Grants, consulta [Associazione o annullamento dell'associazione dell'istanza del Centro identità IAM](#).

In che modo le identità delle directory possono accedere ai dati S3

Supponiamo di avere utenti della directory aziendale che devono accedere ai dati S3 attraverso un'applicazione aziendale, ad esempio un'applicazione per la visualizzazione di documenti, che è integrata con il gestore dell'identità digitale (IdP) esterno (ad esempio, Okta) per autenticare gli utenti. L'autenticazione dell'utente in queste applicazioni viene in genere effettuata tramite reindirizzamenti nel browser web dell'utente. Poiché gli utenti presenti nella directory non sono principali IAM, l'applicazione necessita di credenziali IAM con cui richiamare l'operazione API `GetDataAccess` S3 Access Grants per [ottenere le credenziali di accesso ai dati S3](#) per conto degli utenti. A differenza degli utenti e dei ruoli IAM che ottengono le credenziali da soli, l'applicazione necessita di un modo

per rappresentare un utente della directory, che non è mappato a un ruolo IAM, in modo che l'utente possa accedere ai dati tramite S3 Access Grants.

Questa transizione, da utente di directory autenticato a chiamante IAM in grado di effettuare richieste a S3 Access Grants per conto dell'utente della directory, viene effettuata dall'applicazione tramite la funzionalità Emittente del token affidabile del Centro identità IAM. L'applicazione, dopo aver autenticato l'utente della directory, dispone di un token di identità dell'IdP (ad esempio, Okta) che rappresenta l'utente della directory in base a Okta. La configurazione dell'emittente del token affidabile nel Centro identità IAM consente all'applicazione di scambiare questo token Okta (il tenant Okta è configurato come "emittente attendibile") con un token di identità diverso dal Centro identità IAM che rappresenterà in modo sicuro l'utente della directory all'interno dei Servizi AWS. L'applicazione dati assumerà quindi un ruolo IAM, fornendo il token dell'utente della directory proveniente dal Centro identità IAM come contesto aggiuntivo. L'applicazione può utilizzare la sessione IAM risultante per chiamare S3 Access Grants. Il token rappresenta sia l'identità dell'applicazione (il principale IAM stesso) sia l'identità dell'utente della directory.

Il passaggio principale di questa transizione è lo scambio di token. L'applicazione esegue questo scambio di token chiamando l'operazione API `CreateTokenWithIAM` nel Centro identità IAM. Ovviamente anche questa è una chiamata AWS API e richiede che un responsabile IAM la firmi. Il principale IAM che effettua questa richiesta è in genere un ruolo IAM associato all'applicazione. Ad esempio, se l'applicazione viene eseguita su Amazon EC2, la richiesta `CreateTokenWithIAM` viene in genere eseguita dal ruolo IAM associato all'istanza EC2 su cui viene eseguita l'applicazione. Il risultato di una `CreateTokenWithIAM` chiamata riuscita è un nuovo token di identità, che verrà riconosciuto all'interno Servizi AWS.

Il passaggio successivo, prima che l'applicazione possa chiamare `GetDataAccess` per conto dell'utente della directory, prevede che l'applicazione ottenga una sessione IAM che includa l'identità dell'utente della directory. L'applicazione esegue questa operazione con una `AssumeRole` richiesta Servizio di token di sicurezza AWS (AWS STS) che include anche il token IAM Identity Center per l'utente della directory come contesto di identità aggiuntivo. Questo contesto aggiuntivo consente al Centro identità IAM di propagare l'identità dell'utente della directory alla fase successiva. Il ruolo IAM assunto dall'applicazione è il ruolo che necessiterà delle autorizzazioni IAM per chiamare l'operazione `GetDataAccess`.

Dopo aver assunto il ruolo IAM di portatore di identità con il token del Centro identità IAM per l'utente della directory come contesto aggiuntivo, l'applicazione dispone ora di tutti gli elementi necessari per inviare una richiesta firmata a `GetDataAccess` per conto dell'utente della directory autenticato.

La propagazione dei token si basa sui seguenti passaggi:

Creazione di un'applicazione del Centro identità IAM

Innanzitutto, crea una nuova applicazione nel Centro identità IAM. Questa applicazione utilizzerà un modello che consente al Centro identità IAM di identificare il tipo di impostazioni dell'applicazione che è possibile utilizzare. Il comando per creare l'applicazione richiede di fornire il nome della risorsa Amazon (ARN) dell'istanza del Centro identità IAM, un nome di applicazione e il nome della risorsa Amazon (ARN) del provider dell'applicazione. Il provider dell'applicazione è il provider dell'applicazione SAML o OAuth che l'applicazione utilizzerà per effettuare le chiamate al Centro identità IAM.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws sso-admin create-application \  
  --instance-arn "arn:aws:sso:::instance/ssoins-ssoins-1234567890abcdef" \  
  --application-provider-arn "arn:aws:sso::aws:applicationProvider/custom" \  
  --name MyDataApplication
```

Risposta:

```
{  
  "ApplicationArn": "arn:aws:sso:::123456789012:application/ssoins-  
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"  
}
```

Creazione di un emittente del token affidabile

Ora che hai la tua applicazione del Centro identità IAM, il passaggio successivo consiste nel configurare un emittente del token affidabile che verrà utilizzato per scambiare i valori IdToken del tuo gestore dell'identità digitale con i token del Centro identità IAM. Per completare questa fase, sono necessari i seguenti elementi:

- L'URL dell'emittente del gestore dell'identità
- Il nome emittente del token affidabile
- Il percorso dell'attributo claim
- Il percorso dell'attributo identity store
- L'opzione di recupero JSON Web Key Set (JWKS)

Il percorso dell'attributo claim è l'attributo del gestore delle identità che verrà utilizzato per mappare l'attributo identity store. Normalmente, il percorso dell'attributo claim è l'indirizzo e-mail dell'utente, ma è possibile utilizzare altri attributi per eseguire la mappatura.

Crea un file denominato `oidc-configuration.json` con le informazioni seguenti. Per utilizzare questo file, sostituisci *user input placeholders* con le tue informazioni specifiche.

```
{
  "OidcJwtConfiguration":
  {
    "IssuerUrl": "https://login.microsoftonline.com/a1b2c3d4-abcd-1234-b7d5-
b154440ac123/v2.0",
    "ClaimAttributePath": "preferred_username",
    "IdentityStoreAttributePath": "userName",
    "JwksRetrievalOption": "OPEN_ID_DISCOVERY"
  }
}
```

Per creare l'emittente del token affidabile, esegui questo comando. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws sso-admin create-trusted-token-issuer \
  --instance-arn "arn:aws:sso::instance/ssoins-1234567890abcdef" \
  --name MyEntraIDTrustedIssuer \
  --trusted-token-issuer-type OIDC_JWT \
  --trusted-token-issuer-configuration file://./oidc-configuration.json
```

Risposta

```
{
  "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234"
}
```

Connessione dell'applicazione del Centro identità IAM con l'emittente del token affidabile

L'emittente del token affidabile richiede alcune altre impostazioni di configurazione per funzionare. Imposta i destinatari di cui si fiderà l'emittente del token affidabile. I destinatari rappresentano il valore all'interno di IdToken che è identificato dalla chiave e può essere trovato nelle impostazioni del gestore dell'identità. Ad esempio:

```
1234973b-abcd-1234-abcd-345c5a9c1234
```

Crea un file denominato `grant.json` che abbia il seguente contenuto. Per utilizzare questo file, modifica i destinatari in modo che corrispondano alle impostazioni del tuo gestore dell'identità e fornisci il nome della risorsa Amazon (ARN) dell'emittente del token affidabile che è stato restituito dal comando precedente.

```
{
  "JwtBearer":
  {
    "AuthorizedTokenIssuers":
    [
      {
        "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234",
        "AuthorizedAudiences":
        [
          "1234973b-abcd-1234-abcd-345c5a9c1234"
        ]
      }
    ]
  }
}
```

Esegui il seguente comando di esempio. Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws sso-admin put-application-grant \
  --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
  --grant-type "urn:ietf:params:oauth:grant-type:jwt-bearer" \
  --grant file:///./grant.json \
```

Questo comando configura l'emittente del token affidabile in modo che consideri attendibili i destinatari presenti nel file `grant.json` e li colleghi all'applicazione creata nel primo passaggio per lo scambio di token del tipo `jwt-bearer`. La stringa `urn:ietf:params:oauth:grant-type:jwt-bearer` non è una stringa arbitraria. È uno spazio dei nomi registrato nei profili di asserzione OAuth JSON Web Token (JWT). Puoi trovare ulteriori informazioni su questo spazio dei nomi in [RFC 7523](https://tools.ietf.org/html/rfc7523).

Successivamente, utilizza il seguente comando per impostare gli ambiti che l'emittente del token affidabile includerà nello scambio dei valori IdToken dal tuo provider dell'identità. Per S3 Access Grants, il valore del parametro `--scope` è `s3:access_grants:read_write`.

```
aws sso-admin put-application-access-scope \  
  --application-arn "arn:aws:sso::111122223333:application/ssoins-  
ssoins-111122223333abcdef/apl-abcd1234a1b2c3d" \  
  --scope "s3:access_grants:read_write"
```

L'ultimo passaggio consiste nell'allegare una policy delle risorse all'applicazione del Centro identità IAM. Questa policy consentirà al ruolo IAM dell'applicazione di effettuare richieste all'operazione API `sso-oauth:CreateTokenWithIAM` e ricevere i valori IdToken dal Centro identità IAM.

Crea un file denominato `authentication-method.json` che abbia il seguente contenuto. Sostituisci `123456789012` con l'ID del tuo account.

```
{  
  "Iam":  
  {  
    "ActorPolicy":  
    {  
      "Version": "2012-10-17",  
      "Statement":  
      [  
        {  
          "Effect": "Allow",  
          "Principal":  
          {  
            "AWS": "arn:aws:iam::123456789012:role/webapp"  
          },  
          "Action": "sso-oauth:CreateTokenWithIAM",  
          "Resource": ""  
        }  
      ]  
    }  
  }  
}
```

Per collegare la policy all'applicazione del Centro identità IAM, esegui il comando:

```
aws sso-admin put-application-authentication-method \  

```

```
--application-arn "arn:aws:sso::123456789012:application/ssoins-  
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \  
--authentication-method-type IAM \  
--authentication-method file://./authentication-method.json
```

Questo completa le impostazioni di configurazione per l'utilizzo di S3 Access Grants con gli utenti della directory tramite un'applicazione web. Puoi testare questa configurazione direttamente nell'applicazione oppure puoi chiamare l'operazione API `CreateTokenWithIAM` utilizzando il seguente comando da un ruolo IAM consentito nella policy dell'applicazione del Centro identità IAM:

```
aws sso-oidc create-token-with-iam \  
--client-id "arn:aws:sso::123456789012:application/ssoins-ssoins-1234567890abcdef/  
apl-abcd1234a1b2c3d" \  
--grant-type urn:ietf:params:oauth:grant-type:jwt-bearer \  
--assertion IdToken
```

La risposta sarà simile alla seguente:

```
{  
  "accessToken": "<suppressed long string to reduce space>",  
  "tokenType": "Bearer",  
  "expiresIn": 3600,  
  "refreshToken": "<suppressed long string to reduce space>",  
  "idToken": "<suppressed long string to reduce space>",  
  "issuedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",  
  "scope": [  
    "sts:identity_context",  
    "s3:access_grants:read_write",  
    "openid",  
    "aws"  
  ]  
}
```

Se decodifichi il valore `IdToken` codificato con base64, puoi vedere le coppie chiave-valore in formato JSON. La chiave `sts:identity_context` contiene il valore che l'applicazione deve inviare nella richiesta `sts:AssumeRole` per includere le informazioni sull'identità dell'utente della directory. Di seguito è riportato un esempio di `IdToken` decodificato:

```
{  
  "aws:identity_store_id": "d-996773e796",  
  "sts:identity_context": "AQoJb3JpZ2ZlX2VjE0Tt1;<SUPRESSED>",
```

```

"sub": "83d43802-00b1-7054-db02-f1d683aacba5",
"aws:instance_account": "123456789012",
"iss": "https://identitycenter.amazonaws.com/ssoins-1234567890abcdef",
"sts:audit_context": "AQoJb3JpZ2luX2VjE0T<SUPRESSED>==",
"aws:identity_store_arn": "arn:aws:identitystore::232642235904:identitystore/
d-996773e796",
"aud": "abcd12344U0gi7n4Yyp0-WV1LWN1bnRyYWwtMQ",
"aws:instance_arn": "arn:aws:sso:::instance/ssoins-6987d7fb04cf7a51",
"aws:credential_id": "EXAMPLEHI5glPh40y9TpApJn8...",
"act": {
  "sub": "arn:aws:sso::232642235904:trustedTokenIssuer/
ssoins-6987d7fb04cf7a51/43b4a822-1020-7053-3631-cb2d3e28d10e"
},
"auth_time": "2023-11-01T20:24:28Z",
"exp": 1698873868,
"iat": 1698870268
}

```

Puoi ottenere il valore da `sts:identity_context` e trasmettere queste informazioni in una chiamata `sts:AssumeRole`. Di seguito è riportato un esempio di sintassi CLI. Il ruolo da assumere è un ruolo temporaneo con autorizzazioni per richiamare `s3:GetDataAccess`.

```

aws sts assume-role \
  --role-arn "arn:aws:iam::123456789012:role/temp-role" \
  --role-session-name "TempDirectoryUserRole" \
  --provided-contexts ProviderArn="arn:aws:iam::aws:contextProvider/
IdentityCenter",ContextAssertion="value from sts:identity_context"

```

Ora puoi utilizzare le credenziali ricevute da questa chiamata per richiamare l'operazione API `s3:GetDataAccess` e ricevere le credenziali finali con accesso alle risorse S3.

Nozioni di base su S3 Access Grants

Amazon S3 Access Grants è una funzionalità di Amazon S3 che fornisce una soluzione scalabile di controllo degli accessi per i dati S3. S3 Access Grants è un fornitore di credenziali S3, il che significa che devi registrare su S3 Access Grants il tuo elenco di concessioni e specificarne il livello. Successivamente, quando gli utenti o i client devono accedere ai tuoi dati S3, devono prima chiedere le credenziali a S3 Access Grants. Se esiste una concessione corrispondente che autorizza l'accesso, S3 Access Grants fornisce credenziali di accesso temporanee con privilegi minimi. Gli utenti o i client possono quindi utilizzare le credenziali fornite da S3 Access Grants per accedere ai dati S3. Tenendo presente questo, se i requisiti relativi ai dati S3 richiedono una configurazione di

autorizzazioni complessa o di grandi dimensioni, puoi utilizzare S3 Access Grants per dimensionare le autorizzazioni relative ai dati S3 per utenti, gruppi, ruoli e applicazioni.

Nella maggior parte dei casi d'uso, puoi gestire il controllo degli accessi per i tuoi dati S3 utilizzando AWS Identity and Access Management (IAM) con politiche bucket o policy IAM basate sull'identità.

Tuttavia, se hai requisiti di controllo degli accessi S3 complessi, come i seguenti, puoi ottenere grandi vantaggi dall'utilizzo di S3 Access Grants:

- Stai per raggiungere il limite di dimensioni della policy del bucket di 20 KB.
- Concedi alle identità umane, ad esempio agli utenti e ai gruppi Microsoft Entra ID (in precedenza Azure Active Directory), Okta o Ping, l'accesso ai dati S3 per analisi e big data.
- Devi fornire l'accesso multi-account senza apportare aggiornamenti frequenti alle policy IAM.
- I tuoi dati non sono strutturati e sono a livello di oggetto anziché strutturati, in formato riga e colonna.

Di seguito è riportato il flusso di lavoro di S3 Access Grants:

Fasi	Description
1	Creazione di un'istanza S3 Access Grants Per iniziare, avvia un'istanza S3 Access Grants che conterrà le tue concessioni di accesso individuali.
2	Registrazione di una posizione In secondo luogo, registra una posizione dati S3 (ad esempio quella predefinita <code>s3://</code>), quindi specifica un ruolo IAM predefinito che S3 Access Grants assume quando fornisce l'accesso alla posizione dei dati S3. Puoi anche aggiungere posizioni personalizzate a bucket o prefissi specifici e mapparle a ruoli IAM personalizzati.
3	Creazione di concessioni Crea concessioni di autorizzazione individuali. In queste concessioni di autorizzazioni devi specificare la posizione S3

Fasi	Description
	registrata, l'ambito di accesso ai dati all'interno della posizione , l'identità dell'assegnatario e il suo livello di accesso (READ, WRITE o READWRITE).
4	Richiesta di accesso ai dati S3 Quando gli utenti e le applicazioni Servizi AWS desiderano accedere ai dati S3, effettuano prima una richiesta di accesso. S3 Access Grants determina se la richiesta deve essere autorizzata. Se esiste una concessione corrispondente che autorizza l'accesso, S3 Access Grants utilizza il ruolo IAM della posizione registrata associato a tale concessione per fornire le credenziali temporanee al richiedente.
5	Accesso ai dati S3 Le applicazioni utilizzano le credenziali temporanee fornite da S3 Access Grants per accedere ai dati S3.

Operazioni con le istanze S3 Access Grants

Per iniziare a usare Amazon S3 Access Grants, devi prima creare un'istanza S3 Access Grants. Puoi creare una sola istanza di S3 Access Grants per account. Regione AWS L'istanza S3 Access Grants funge da container per le risorse S3 Access Grants, che includono concessioni e posizioni registrate.

Con S3 Access Grants, puoi creare autorizzazioni per i tuoi dati S3 per utenti e ruoli AWS Identity and Access Management (IAM). Se hai [aggiunto la tua directory di identità aziendale](#) a Centro identità AWS IAM, puoi associare questa istanza IAM Identity Center della tua directory aziendale alla tua istanza S3 Access Grants. Quindi, puoi creare concessioni di accesso per gli utenti e i gruppi aziendali. Se non hai ancora aggiunto la tua directory aziendale al Centro identità IAM, puoi associare la tua istanza S3 Access Grants a un'istanza Centro identità IAM in un secondo momento.

Argomenti

- [Creazione di un'istanza S3 Access Grants](#)
- [Ottenimento dei dettagli di un'istanza S3 Access Grants](#)
- [Elenco delle istanze S3 Access Grants](#)

- [Associazione o annullamento dell'associazione dell'istanza del Centro identità IAM](#)
- [Eliminazione di un'istanza S3 Access Grants](#)

Creazione di un'istanza S3 Access Grants

Per iniziare a usare Amazon S3 Access Grants, devi prima creare un'istanza S3 Access Grants. Puoi creare una sola istanza S3 Access Grants per account. Regione AWS L'istanza S3 Access Grants funge da container per le risorse S3 Access Grants, che includono concessioni e posizioni registrate.

Con S3 Access Grants, puoi creare autorizzazioni per i tuoi dati S3 per utenti e ruoli AWS Identity and Access Management (IAM). Se hai [aggiunto la tua directory di identità aziendale](#) a Centro identità AWS IAM, puoi associare questa istanza IAM Identity Center della tua directory aziendale alla tua istanza S3 Access Grants. Quindi, puoi creare concessioni di accesso per gli utenti e i gruppi aziendali. Se non hai ancora aggiunto la tua directory aziendale al Centro identità IAM, puoi associare la tua istanza S3 Access Grants a un'istanza Centro identità IAM in un secondo momento.

Puoi creare un'istanza S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Prima di poter concedere l'accesso ai tuoi dati S3 con S3 Access Grants, devi creare un'istanza S3 Access Grants nello stesso formato dei tuoi dati S3. Regione AWS

Prerequisiti

Se desideri concedere l'accesso ai tuoi dati S3 utilizzando le identità della tua directory aziendale, [aggiungi la tua directory di identità aziendale](#) a Centro identità AWS IAM. Se ritieni che non sia ancora il momento per farlo, puoi associare la tua istanza S3 Access Grants a un'istanza del Centro identità IAM in un secondo momento.

Per creare un'istanza S3 Access Grants

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione a cui passare.
3. Nel pannello di navigazione a sinistra, scegli Access Grants.

4. Nella pagina S3 Access Grants, scegli Crea un'istanza S3 Access Grants.

- a. Nel Passaggio 1 della procedura guidata Configura l'istanza Access Grants, verifica di voler creare l'istanza nella Regione AWS corrente. Assicurati che sia lo stesso Regione AWS in cui si trovano i tuoi dati S3. Puoi creare un'istanza di S3 Access Grants per account. Regione AWS
- b. (Facoltativo) Se hai [aggiunto la tua directory di identità aziendale](#) a Centro identità AWS IAM, puoi associare questa istanza IAM Identity Center della tua directory aziendale alla tua istanza S3 Access Grants.

Per farlo, seleziona Aggiungi istanza IAM Identity Center in. **region** Quindi inserisci il nome della risorsa Amazon (ARN) dell'istanza del Centro identità IAM.

Se non hai ancora aggiunto la tua directory di identità aziendale al Centro identità IAM, puoi associare l'istanza S3 Access Grants a un'istanza del Centro identità IAM in un secondo momento.

- c. Per creare l'istanza S3 Access Grants, scegli Avanti. Per registrare una posizione, consulta [Passaggio 2: registrare una posizione](#).

5. Se l'opzione Avanti o Crea istanza S3 Access Grants è disabilitata:

Non puoi creare un'istanza

- Potresti avere già un'istanza S3 Access Grants nella stessa Regione AWS. Nel pannello di navigazione a sinistra, scegli Access Grants. Nella pagina S3 Access Grants, scorri verso il basso fino alla sezione Istanza S3 Access Grants nel tuo account per stabilire se un'istanza esiste già.
- Potresti non disporre dell'autorizzazione `s3:CreateAccessGrantsInstance` richiesta per creare un'istanza S3 Access Grants. Contatta l'amministratore dell'account. Per le autorizzazioni aggiuntive necessarie per associare un'istanza del Centro identità IAM alla tua istanza S3 Access Grants, consulta [CreateAccessGrantsInstance](#).

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida AWS Command Line Interface per l'utente.

Per utilizzare il seguente comando di esempio, sostituisci ***user input placeholders*** con le tue informazioni.

Example Creazione di un'istanza S3 Access Grants

```
aws s3control create-access-grants-instance \  
--account-id 111122223333 \  
--region us-east-2
```

Risposta:

```
{  
  "CreatedAt": "2023-05-31T17:54:07.893000+00:00",  
  "AccessGrantsInstanceId": "default",  
  "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/  
default"  
}
```

Utilizzo della REST API

Puoi utilizzare la REST API di Amazon S3 per creare un'istanza S3 Access Grants. Per informazioni sul supporto REST API per la gestione di un'istanza S3 Access Grants, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [AssociateAccessGrantsIdentityCenter](#)
- [CreateAccessGrantsInstance](#)
- [DeleteAccessGrantsInstance](#)
- [DissociateAccessGrantsIdentityCenter](#)
- [GetAccessGrantsInstance](#)
- [GetAccessGrantsInstanceForPrefix](#)
- [GetAccessGrantsInstanceResourcePolicy](#)
- [ListAccessGrantsInstances](#)
- [PutAccessGrantsInstanceResourcePolicy](#)

Utilizzo di AWS SDK

Questa sezione fornisce un esempio di come creare un'istanza S3 Access Grants utilizzando gli AWS SDK.

Java

Questo esempio crea l'istanza S3 Access Grants, che funge da container per le tue concessioni di accesso individuali. Puoi avere un'istanza di S3 Access Grants per ogni Regione AWS account. La risposta include l'ID dell'istanza default e un nome della risorsa Amazon (ARN) generato per la tua istanza S3 Access Grants.

Example Creazione di una richiesta di istanza S3 Access Grants

```
public void createAccessGrantsInstance() {  
    CreateAccessGrantsInstanceRequest createRequest =  
        CreateAccessGrantsInstanceRequest.builder().accountId("111122223333").build();  
    CreateAccessGrantsInstanceResponse createResponse =  
        s3Control.createAccessGrantsInstance(createRequest);LOGGER.info("CreateAccessGrantsInstance  
    " + createResponse);  
}
```

Risposta:

```
CreateAccessGrantsInstanceResponse(  
    CreatedAt=2023-06-07T01:46:20.507Z,  
    AccessGrantsInstanceId=default,  
    AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default)
```

Ottenimento dei dettagli di un'istanza S3 Access Grants

È possibile ottenere i dettagli dell'istanza di Amazon S3 Access Grants in un particolare Regione AWS. Puoi ottenere i dettagli della tua istanza S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per ottenere i dettagli di un'istanza di S3 Access Grants

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la Regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.

- La pagina S3 Access Grants elenca le istanze S3 Access Grants e tutte le istanze multi-account che sono state condivise con il tuo account. Per visualizzare i dettagli di un'istanza, scegli [Visualizza dettagli](#).

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Ottieni i dettagli di un'istanza S3 Access Grants

```
aws s3control get-access-grants-instance \
  --account-id 111122223333 \
  --region us-east-2
```

Risposta:

```
{
  "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default",
  "AccessGrantsInstanceId": "default",
  "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API Amazon S3 per la gestione di un'istanza S3 Access Grants, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [GetAccessGrantsInstance](#)
- [GetAccessGrantsInstanceForPrefix](#)

Utilizzo di AWS SDK

Questa sezione fornisce esempi su come ottenere i dettagli di un'istanza di S3 Access Grants utilizzando gli AWS SDK.

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Java

Example– Ottieni un'istanza S3 Access Grants

```
public void getAccessGrantsInstance() {
    GetAccessGrantsInstanceRequest getRequest = GetAccessGrantsInstanceRequest.builder()
        .accountId("111122223333")
        .build();
    GetAccessGrantsInstanceResponse getResponse =
        s3Control.getAccessGrantsInstance(getRequest);
    LOGGER.info("GetAccessGrantsInstanceResponse: " + getResponse);
}
```

Risposta:

```
GetAccessGrantsInstanceResponse(
    AccessGrantsInstanceArn=arn:aws:s3:us-east-2: 111122223333:access-grants/default,
    CreatedAt=2023-06-07T01:46:20.507Z)
```

Elenco delle istanze S3 Access Grants

Puoi elencare le tue istanze S3 Access Grants, incluse le istanze che sono state condivise con te tramite (). AWS Resource Access Manager AWS RAM

Puoi elencare le tue istanze S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per elencare le istanze S3 Access Grants

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la Regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.

4. La pagina S3 Access Grants elenca le istanze S3 Access Grants e tutte le istanze multi-account che sono state condivise con il tuo account. Per visualizzare i dettagli di un'istanza, scegli [Visualizza dettagli](#).

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Elenca tutte le istanze S3 Access Grants relative a un account

Questa azione elenca le istanze S3 Access Grants per un account. Puoi avere una sola istanza di S3 Access Grants per. Regione AWS Questa azione elenca anche altre istanze S3 Access Grants multi-account a cui il tuo account ha accesso.

```
aws s3control list-access-grants-instances \
  --account-id 111122223333 \
  --region us-east-2
```

Risposta:

```
{
  "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default",
  "AccessGrantsInstanceId": "default",
  "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API Amazon S3 per la gestione di un'istanza S3 Access Grants, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [ListAccessGrantsInstances](#)

Utilizzo di AWS SDK

Questa sezione fornisce esempi su come ottenere i dettagli di un'istanza S3 Access Grants utilizzando gli SDK. AWS

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Java

Example– Elenca tutte le istanze S3 Access Grants relative a un account

Questa azione elenca le istanze S3 Access Grants per un account. Puoi avere una sola istanza S3 Access Grants per regione. Questa azione può elencare anche altre istanze S3 Access Grants multi-account a cui il tuo account ha accesso.

```
public void listAccessGrantsInstances() {
    ListAccessGrantsInstancesRequest listRequest =
        ListAccessGrantsInstancesRequest.builder()
            .accountId("111122223333")
            .build();
    ListAccessGrantsInstancesResponse listResponse =
        s3Control.listAccessGrantsInstances(listRequest);
    LOGGER.info("ListAccessGrantsInstancesResponse: " + listResponse);
}
```

Risposta:

```
ListAccessGrantsInstancesResponse(
    AccessGrantsInstancesList=[
        ListAccessGrantsInstanceEntry(
            AccessGrantsInstanceId=default,
            AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default,
            CreatedAt=2023-06-07T04:28:11.728Z
        )
    ]
)
```

Associazione o annullamento dell'associazione dell'istanza del Centro identità IAM

In Amazon S3 Access Grants, puoi associare l' Centro identità AWS IAM istanza della tua directory di identità aziendale a un'istanza S3 Access Grants. Dopo averlo fatto, puoi creare autorizzazioni di

accesso per gli utenti e i gruppi della tua directory aziendale, oltre agli utenti e ai ruoli AWS Identity and Access Management (IAM).

Se non desideri più creare concessioni di accesso per gli utenti e i gruppi della tua directory aziendale, puoi annullare l'associazione dell'istanza del Centro identità IAM dall'istanza S3 Access Grants.

Puoi associare o annullare l'associazione di un'istanza del Centro identità IAM utilizzando la console Amazon S3, l' AWS Command Line Interface (AWS CLI), la REST API di Amazon S3 e gli AWS SDK.

Utilizzo della console S3

Prima di associare l'istanza del Centro identità IAM all'istanza S3 Access Grants, devi aggiungere la directory di identità aziendale al Centro identità IAM. Per ulteriori informazioni, consulta [the section called “S3 Access Grants e identità delle directory aziendali”](#).

Per associare un'istanza S3 Access Grants a un'istanza del Centro identità IAM

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.
4. Scegli Visualizza dettagli per l'istanza.
5. Nella pagina dei dettagli, nella sezione Centro identità IAM, scegli di aggiungere un'istanza del Centro identità IAM o di annullare la registrazione di un'istanza del Centro identità IAM già associata.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Associa un'istanza S3 Access Grants a un'istanza del Centro identità IAM

```
aws s3control associate-access-grants-identity-center \
```

```
--account-id 111122223333 \  
--identity-center-arn arn:aws:sso:::instance/ssoins-1234a567bb89012c \  
--profile access-grants-profile \  
--region eu-central-1
```

```
// No response body
```

Example– Annulla associazione di un'istanza S3 Access Grants da un'istanza del Centro identità IAM

```
aws s3control dissociate-access-grants-identity-center \  
--account-id 111122223333 \  
--profile access-grants-profile \  
--region eu-central-1
```

```
// No response body
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la gestione dell'associazione tra un'istanza del Centro identità IAM e un'istanza S3 Access Grants, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [AssociateAccessGrantsIdentityCenter](#)
- [DissociateAccessGrantsIdentityCenter](#)

Eliminazione di un'istanza S3 Access Grants

Puoi eliminare un'istanza di Amazon S3 Access Grants da un Regione AWS account. Tuttavia, prima di eliminare un'istanza S3 Access Grants, devi eseguire queste operazioni:

- Elimina tutte le risorse all'interno dell'istanza S3 Access Grants, incluse tutte le concessioni e le posizioni. Per ulteriori informazioni, consulta [Eliminazione di una concessione](#) ed [Eliminazione di una posizione](#).
- Se hai associato un'istanza del Centro identità AWS IAM alla tua istanza S3 Access Grants, devi dissociare l'istanza IAM Identity Center. Per ulteriori informazioni, consulta [Associazione o annullamento dell'associazione dell'istanza del Centro identità IAM](#).

 Important

Se elimini un'istanza S3 Access Grants, l'eliminazione è permanente e non può essere annullata. Tutti gli assegnatari a cui è stato fornito l'accesso grazie alle concessioni in questa istanza S3 Access Grants perderanno l'accesso ai tuoi dati S3.

Puoi eliminare un'istanza S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per eliminare un'istanza S3 Access Grants

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.
4. Scegli Visualizza dettagli per l'istanza.
5. Nella pagina dei dettagli dell'istanza, scegli Elimina istanza.
6. Nella finestra di dialogo visualizzata, seleziona Elimina. Questa azione non può essere annullata.

Utilizzo di AWS CLI

Per installarlo AWS CLI, vedere [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

 Note

Prima di poter eliminare un'istanza S3 Access Grants, devi eliminare tutte le concessioni e le posizioni create all'interno dell'istanza S3 Access Grants. Se hai associato un'istanza del Centro identità IAM alla tua istanza S3 Access Grants, devi prima annullare l'associazione dell'istanza del Centro identità IAM.

Example– Elimina un'istanza S3 Access Grants

```
aws s3control delete-access-grants-instance \  
--account-id 111122223333 \  
--profile access-grants-profile \  
--region us-east-2 \  
--endpoint-url https://s3-control.us-east-2.amazonaws.com \  
  
// No response body
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'eliminazione di un'istanza S3 Access Grants, consulta [DeleteAccessGrantsInstance](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di AWS SDK

Questa sezione fornisce esempi di come eliminare un'istanza S3 Access Grants utilizzando gli AWS SDK.

Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le tue informazioni.

Java

Note

Prima di poter eliminare un'istanza S3 Access Grants, devi eliminare tutte le concessioni e le posizioni create all'interno dell'istanza S3 Access Grants. Se hai associato un'istanza del Centro identità IAM alla tua istanza S3 Access Grants, devi prima annullare l'associazione dell'istanza del Centro identità IAM.

Example– Elimina un'istanza S3 Access Grants

```
public void deleteAccessGrantsInstance() {  
    DeleteAccessGrantsInstanceRequest deleteRequest =  
        DeleteAccessGrantsInstanceRequest.builder()  
            .accountId("111122223333")  
            .build();  
    DeleteAccessGrantsInstanceResponse deleteResponse =  
        s3Control.deleteAccessGrantsInstance(deleteRequest);  
}
```

```
LOGGER.info("DeleteAccessGrantsInstanceResponse: " + deleteResponse);  
}
```

Operazioni con le posizioni S3 Access Grants

Dopo aver [creato un'istanza di Amazon S3 Access Grants](#) Regione AWS in un account, registri una sede S3 in quell'istanza. Una sede S3 Access Grants mappa la posizione S3 predefinita (s3://), un bucket o un prefisso di un ruolo (IAM). AWS Identity and Access Management S3 Access Grants assume questo ruolo IAM per vendere credenziali temporanee al beneficiario che accede a quella particolare posizione. Prima di poter creare una concessione di accesso, è necessario registrare almeno una posizione nell'istanza S3 Access Grants.

È possibile registrare una posizione, visualizzarne i dettagli, modificarla ed eliminarla.

Note

Dopo aver registrato la prima posizione nell'istanza S3 Access Grants, l'istanza non ha ancora alcun singolo accesso garantito. Per creare una concessione di accesso, consulta [Creazione di concessioni](#).

Argomenti

- [Registrazione di una posizione](#)
- [Visualizza i dettagli di una posizione registrata](#)
- [Aggiornamento di una posizione registrata](#)
- [Eliminazione di una posizione registrata](#)

Registrazione di una posizione

Dopo aver [creato un'istanza Amazon S3 Access Grants](#) Regione AWS in un account, registri una sede S3 in quell'istanza. Una sede S3 Access Grants mappa la posizione S3 predefinita (s3://), un bucket o un prefisso di un ruolo (IAM). AWS Identity and Access Management S3 Access Grants assume questo ruolo IAM per vendere credenziali temporanee al beneficiario che accede a quella particolare posizione. Prima di poter creare una concessione di accesso, è necessario registrare almeno una posizione nell'istanza S3 Access Grants.

Caso d'uso consigliato

Si consiglia di registrare la posizione predefinita (`s3://`) e di mapparla a un ruolo IAM. La posizione nel percorso S3 predefinito (`s3://`) copre l'accesso a tutti i bucket S3 in quello del tuo account. Regione AWS Quando si crea una concessione di accesso, è possibile restringere l'ambito della concessione a un bucket, a un prefisso o a un oggetto all'interno della posizione predefinita.

Casi d'uso complessi per la gestione degli accessi

Casi di utilizzo della gestione degli accessi più complessi potrebbero richiedere la registrazione di più posizioni rispetto a quella predefinita. Alcuni esempi di questi casi d'uso sono:

- Si supponga che il bucket *amzn-s3-demo-bucket* sia una posizione registrata nella tua istanza S3 Access Grants con un ruolo IAM mappato su di essa, ma a questo ruolo IAM sia negato l'accesso a un particolare prefisso all'interno del bucket. In questo caso, è possibile registrare il prefisso a cui il ruolo IAM non ha accesso come posizione separata e mappare tale posizione a un altro ruolo IAM con l'accesso necessario.
- Si supponga di voler creare dei grant che limitino l'accesso solo agli utenti all'interno di un endpoint di un cloud privato virtuale (VPC). In questo caso, è possibile registrare una posizione per un bucket in cui il ruolo IAM limita l'accesso all'endpoint VPC. Successivamente, quando un beneficiario chiede le credenziali a S3 Access Grants, S3 Access Grants assume il ruolo IAM della sede per vendere le credenziali temporanee. Questa credenziale negherà l'accesso al bucket specifico a meno che il chiamante non si trovi all'interno dell'endpoint VPC. Questa autorizzazione di negazione viene applicata in aggiunta alle normali autorizzazioni READ, WRITE o READWRITE specificate nella concessione.

Quando si registra una posizione, è necessario specificare anche il ruolo IAM che S3 Access Grants assume per la vendita delle credenziali temporanee e per l'ambito delle autorizzazioni per una concessione specifica.

Se il caso d'uso richiede la registrazione di più posizioni nell'istanza di S3 Access Grants, è possibile registrare uno dei seguenti elementi:

URI S3	Ruolo IAM	Description
<code>s3://</code>	<i>Default-IAM-role</i>	La posizione predefinita, <code>s3://</code> , include tutti i bucket nella Regione AWS.
<code>s3://amzn-s3-demo-bucket1 /</code>	<i>IAM-role-For-bucket</i>	Questa posizione include tutti gli oggetti nel bucket specificato.

URI S3	Ruolo IAM	Description
<code>s3://<i>amzn-s3-demo-bucket1</i> /<i>prefix-name</i></code>	<i>IAM-role-For-prefix</i>	Questa posizione include tutti gli oggetti del bucket con un nome di chiave dell'oggetto che inizia con questo prefisso.

Prima di registrare un bucket o un prefisso specifico, accertarsi di aver eseguito le seguenti operazioni:

- Crea uno o più bucket contenenti i dati a cui desideri concedere l'accesso. Questi bucket devono trovarsi nella stessa istanza di S3 Regione AWS Access Grants. Per ulteriori informazioni, consulta [Creazione di un bucket](#).

L'aggiunta di un prefisso è facoltativa. I prefissi sono stringhe all'inizio del nome della chiave di un oggetto. Si possono usare per organizzare gli oggetti nel bucket e per gestire gli accessi. Per aggiungere un prefisso a un bucket, consulta [Creazione dei nomi delle chiavi degli oggetti](#).

- Creare un ruolo IAM che abbia il permesso di accedere ai dati S3 in Regione AWS. Per ulteriori informazioni, consulta la sezione [Creazione di ruoli IAM](#) nella Guida all'utente Centro identità AWS IAM .
- Nella policy di attendibilità del ruolo IAM, concedi al principale del servizio S3 Access Grants (`access-grants.s3.amazonaws.com`) l'accesso al ruolo IAM creato. A tal fine, è possibile creare un file JSON contenente le seguenti istruzioni. Per aggiungere la policy di attendibilità all'account, consulta [Creare un ruolo utilizzando policy di attendibilità personalizzati](#).

TestRolePolicy.json

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TestRolePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
```

```

        "sts:SetSourceIdentity"
    ],
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn": "arn:aws:s3::111122223333:access-grants/default"
        }
    }
}
]
}

```

In alternativa, per un caso d'uso di Centro identità IAM, utilizza la seguente policy che include una seconda istruzione:

- Crea una policy IAM per collegare le autorizzazioni di Amazon S3 al ruolo IAM creato. Consulta il seguente file `iam-policy.json` di esempio e sostituisci *user input placeholders* con le tue informazioni.

Note

- Se utilizzi la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) per crittografare i tuoi dati, l'esempio seguente include le AWS KMS autorizzazioni necessarie per il ruolo IAM nella policy. Se non si utilizza questa funzione, è possibile rimuovere queste autorizzazioni dalla propria policy IAM.
- È possibile limitare il ruolo IAM per accedere ai dati S3 solo se le credenziali sono fornite da S3 Access Grants. Questo esempio mostra come aggiungere un'istruzione `Condition` per una specifica istanza S3 Access Grants. Per utilizzarla, sostituisci l'ARN dell'istanza S3 Access Grants nell'istruzione `Condition` con l'ARN dell'istanza S3 Access Grants. Questo ha il formato: `arn:aws:s3:region:accountId:access-grants/default`

iam-policy.json

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```



```

    "Sid": "ObjectLevelReadPermissions",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": { "aws:ResourceAccount": "accountId" },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": ["arn:aws:s3:region:accountId:access-
grants/default"]
        }
    }
},
{
    "Sid": "ObjectLevelWritePermissions",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": { "aws:ResourceAccount": "accountId" },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Regione
AWS:accountId:access-grants/default"]
        }
    }
},
{
    "Sid": "BucketLevelReadPermissions",

```

```

    "Effect": "Allow",
    "Action": [
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": { "aws:ResourceAccount": "accountId" },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Regione
AWS:accountId:access-grants/default"]
        }
    }
},
// Optionally add the following section if you use SSE-KMS encryption
{
    "Sid": "KMSPermissions",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

Puoi registrare una posizione nella tua istanza S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 o gli SDK. AWS

Note

Dopo aver registrato la prima posizione nell'istanza S3 Access Grants, l'istanza non ha ancora alcun singolo accesso garantito. Per creare una concessione di accesso, consulta [Creazione di concessioni](#).

Utilizzo della console S3

Prima di poter concedere l'accesso ai dati S3 con S3 Access Grants, devi avere almeno una posizione registrata.

Per registrare una posizione nella tua istanza S3 Access Grants

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.

Se utilizzi un'istanza S3 Access Grants per la prima volta, assicurati di aver completato il [Passaggio 1: crea un'istanza S3 Access Grants](#) e di aver eseguito il Passaggio 2 della procedura guidata Configurazione dell'istanza Access Grants. Se disponi già di un'istanza S3 Access Grants, seleziona Visualizza dettagli, quindi dalla scheda Posizioni, seleziona Registra posizione.

- a. Per Ambito della posizione, seleziona Sfoglia S3 o inserisci il percorso URI S3 della posizione che desideri registrare. Per i formati URI S3, consulta la tabella dei [formati di posizione](#). Dopo aver inserito un URI, puoi scegliere Visualizza per andare alla posizione.
- b. In Ruolo IAM, scegliere una delle seguenti opzioni:

- Scegli tra i ruoli IAM esistenti

Scegli un ruolo IAM dall'elenco a discesa. Dopo aver scelto un ruolo, scegli Visualizza per avere la certezza che questo ruolo disponga delle autorizzazioni necessarie per gestire la posizione che stai registrando. In particolare, assicurati che questo ruolo conceda a S3 Access Grants le autorizzazioni `sts:AssumeRole` e `sts:SetSourceIdentity`.

- Inserisci l'ARN del ruolo IAM

Accedi alla [Console IAM](#). Copia il nome della risorsa Amazon (ARN) del ruolo IAM e incollalo in questa casella.

- c. Per finire, scegli Avanti o Registra posizione.

4. Risoluzione dei problemi

Impossibile registrare la posizione

- La posizione potrebbe essere già registrata.

Potresti non avere l'autorizzazione `s3:CreateAccessGrantsLocation` per registrare le posizioni. Contatta l'amministratore dell'account.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Puoi registrare la posizione predefinita, `s3://`, o una posizione personalizzata nella tua istanza S3 Access Grants. Assicurati di creare prima un ruolo IAM con accesso del principale alla posizione, quindi assicurati di concedere a S3 Access Grants l'autorizzazione ad assumere questo ruolo.

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example Creazione di una policy di risorse

Crea una policy che consenta a S3 Access Grants di assumere il ruolo IAM. A questo proposito, puoi creare un file JSON contenente le istruzioni elencate di seguito. Per aggiungere la policy della risorsa al tuo account, consulta [Creazione e collegamento della prima policy gestita dal cliente](#).

TestRolePolicy.json

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Action": ["sts:AssumeRole", "sts:SetSourceIdentity"],
      "Effect": "Allow",
      "Principal": {"Service": "access-grants.s3.amazonaws.com"}
    }
  ]
}
```

Example Creazione del ruolo

Per creare il ruolo, esegui il comando IAM seguente.

```
aws iam create-role --role-name accessGrantsTestRole \  
  --region us-east-2 \  
  --assume-role-policy-document file://TestRolePolicy.json
```

L'esecuzione del comando `create-role` restituisce la policy:

```
{  
  "Role": {  
    "Path": "/",  
    "RoleName": "accessGrantsTestRole",  
    "RoleId": "AROASRDGX4WM4GH55GIDA",  
    "Arn": "arn:aws:iam::111122223333:role/accessGrantsTestRole",  
    "CreateDate": "2023-05-31T18:11:06+00:00",  
    "AssumeRolePolicyDocument": {  
      "Version": "2012-10-17",  
      "Statement": [  
        {  
          "Sid": "Stmt1685556427189",  
          "Action": [  
            "sts:AssumeRole",  
            "sts:SetSourceIdentity"  
          ],  
          "Effect": "Allow",  
          "Principal": {  
            "Service": "access-grants.s3.amazonaws.com"  
          }  
        }  
      ]  
    }  
  }  
}
```

Example

Creare una policy IAM per collegare le autorizzazioni di Amazon S3 al ruolo IAM. Consulta il seguente file `iam-policy.json` di esempio e sostituisci *user input placeholders* con le tue informazioni.

 Note

Se utilizzi la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) per crittografare i tuoi dati, l'esempio seguente aggiunge le AWS KMS autorizzazioni necessarie per il ruolo IAM nella policy. Se non utilizzi questa funzionalità, puoi rimuovere queste autorizzazioni dalla tua policy IAM.

Per avere la certezza che il ruolo IAM possa essere usato per accedere ai dati in S3 solo se le credenziali sono distribuite da S3 Access Grants, questo esempio mostra come aggiungere un'istruzione Condition che specifichi l'istanza S3 Access Grants (s3:AccessGrantsInstance: *InstanceArn*) nella policy IAM. Quando utilizzi la seguente policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

iam-policy.json

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": [
        "arn:aws:s3::*"
      ],
      "Condition": {
        "StringEquals": { "aws:ResourceAccount": "111122223333" },
        "ArnEquals": {
          "s3:AccessGrantsInstanceArn": ["arn:aws:s3:us-east-1::access-grants/default"]
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "ObjectLevelWritePermissions",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:PutObjectVersionAcl",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:AbortMultipartUpload"
    ],
    "Resource": [
      "arn:aws:s3:::*"
    ],
    "Condition": {
      "StringEquals": { "aws:ResourceAccount": "111122223333" },
      "ArnEquals": {
        "s3:AccessGrantsInstanceArn": ["arn:aws:s3:us-east-1::access-
grants/default"]
      }
    }
  },
  {
    "Sid": "BucketLevelReadPermissions",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::*"
    ],
    "Condition": {
      "StringEquals": { "aws:ResourceAccount": "111122223333" },
      "ArnEquals": {
        "s3:AccessGrantsInstanceArn": ["arn:aws:s3:us-east-1::access-
grants/default"]
      }
    }
  },
  {
    "Sid": "KMSPermissions",

```

```

    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "s3.us-east-1.amazonaws.com"
        }
    }
}
]
}

```

Example

Esegui il comando seguente:

```

aws iam put-role-policy \
--role-name accessGrantsTestRole \
--policy-name accessGrantsTestRole \
--policy-document file://iam-policy.json

```

Example Registra la posizione predefinita

```

aws s3control create-access-grants-location \
--account-id 111122223333 \
--location-scope s3:// \
--iam-role-arn arn:aws:iam::111122223333:role/accessGrantsTestRole

```

Risposta:

```

{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
 "AccessGrantsLocationId": "default",
 "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
 "LocationScope": "s3://"
}

```



```
"IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example Registra una posizione personalizzata

```
aws s3control create-access-grants-location \
  --account-id 111122223333 \
  --location-scope s3://DOC-BUCKET-EXAMPLE/ \
  --iam-role-arn arn:aws:iam::123456789012:role/accessGrantsTestRole
```

Risposta:

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
  "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
  "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
  "LocationScope": "s3://DOC-BUCKET-EXAMPLE/",
  "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la gestione di un'istanza S3 Access Grants, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [CreateAccessGrantsLocation](#)
- [DeleteAccessGrantsLocation](#)
- [GetAccessGrantsLocation](#)
- [ListAccessGrantsLocations](#)
- [UpdateAccessGrantsLocation](#)

Utilizzo di AWS SDK

Questa sezione fornisce esempi di come registrare posizioni tramite gli AWS SDK.

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Java

Puoi registrare la posizione predefinita, `s3://`, o una posizione personalizzata nella tua istanza S3 Access Grants. Assicurati di creare prima un ruolo IAM con accesso del principale alla posizione, quindi assicurati di concedere a S3 Access Grants l'autorizzazione ad assumere questo ruolo.

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example Registra una posizione predefinita

Richiesta:

```
public void createAccessGrantsLocation() {
    CreateAccessGrantsLocationRequest createRequest =
        CreateAccessGrantsLocationRequest.builder()
            .accountId("111122223333")
            .locationScope("s3://")
            .iamRoleArn("arn:aws:iam::123456789012:role/accessGrantsTestRole")
            .build();
    CreateAccessGrantsLocationResponse createResponse =
        s3Control.createAccessGrantsLocation(createRequest);
    LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

Risposta:

```
CreateAccessGrantsLocationResponse(
    CreatedAt=2023-06-07T04:35:11.027Z,
    AccessGrantsLocationId=default,
    AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
    location/default,
    LocationScope=s3://,
    IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example Registra una posizione personalizzata

Richiesta:

```
public void createAccessGrantsLocation() {
```

```
CreateAccessGrantsLocationRequest createRequest =  
    CreateAccessGrantsLocationRequest.builder()  
        .accountId("111122223333")  
        .locationScope("s3://DOC-BUCKET-EXAMPLE/")  
        .iamRoleArn("arn:aws:iam::111122223333:role/accessGrantsTestRole")  
        .build();  
CreateAccessGrantsLocationResponse createResponse =  
    s3Control.createAccessGrantsLocation(createRequest);  
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);  
}
```

Risposta:

```
CreateAccessGrantsLocationResponse(  
    CreatedAt=2023-06-07T04:35:10.027Z,  
    AccessGrantsLocationId=18cfe6fb-eb5a-4ac5-aba9-8d79f04c2012,  
    AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/  
    location/18cfe6fb-eb5a-4ac5-aba9-8d79f04c2666,  
    LocationScope= s3://test-bucket-access-grants-user123/,  
    IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole  
)
```

Visualizza i dettagli di una posizione registrata

Puoi ottenere i dettagli di una posizione registrata nella tua istanza S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare le posizioni registrate nell'istanza S3 Access Grants

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.
4. Scegli Visualizza dettagli per l'istanza.
5. Nella pagina dei dettagli dell'istanza, scegli la scheda Posizioni.

6. Trova la posizione registrata che desideri visualizzare. Per filtrare l'elenco delle posizioni registrate, usa la casella di ricerca.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Ottieni i dettagli di una posizione registrata

```
aws s3control get-access-grants-location \  
--account-id 111122223333 \  
--access-grants-location-id default
```

Risposta:

```
{  
  "CreatedAt": "2023-05-31T18:23:48.107000+00:00",  
  "AccessGrantsLocationId": "default",  
  "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/  
default/location/default",  
  "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"  
}
```

Example– Elenca tutte le posizioni registrate in un'istanza di S3 Access Grants

Per limitare i risultati a un prefisso o un bucket S3, puoi opzionalmente utilizzare il parametro `--location-scope s3://bucket-and-or-prefix`.

```
aws s3control list-access-grants-locations \  
--account-id 111122223333 \  
--region us-east-2
```

Risposta:

```
{"AccessGrantsLocationsList": [  
  {
```

```

    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/location/default",
    "LocationScope": "s3://"
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
  },
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixA*",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
  }
]
}

```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per ottenere i dettagli di una posizione registrata o elencare tutte le posizioni registrate con un'istanza S3 Access Grants, consulta le seguenti sezioni nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [GetAccessGrantsLocation](#)
- [ListAccessGrantsLocations](#)

Utilizzo di AWS SDK

Questa sezione fornisce esempi di come ottenere i dettagli di una posizione registrata o elencare tutte le posizioni registrate in un'istanza S3 Access Grants utilizzando gli AWS SDK.

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Java

Example– Ottieni i dettagli di una posizione registrata

```

public void getAccessGrantsLocation() {
    GetAccessGrantsLocationRequest getAccessGrantsLocationRequest =
        GetAccessGrantsLocationRequest.builder()
            .accountId("111122223333")

```

```
.accessGrantsLocationId("default")
.build();
GetAccessGrantsLocationResponse getAccessGrantsLocationResponse =
    s3Control.getAccessGrantsLocation(getAccessGrantsLocationRequest);
LOGGER.info("GetAccessGrantsLocationResponse: " + getAccessGrantsLocationResponse);
}
```

Risposta:

```
GetAccessGrantsLocationResponse(
    CreatedAt=2023-06-07T04:35:10.027Z,
    AccessGrantsLocationId=default,
    AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
    location/default,
    LocationScope= s3://,
    IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example– Elenca tutte le posizioni registrate in un'istanza S3 Access Grants

Per limitare i risultati a un prefisso o un bucket S3, puoi opzionalmente passare un URI S3, ad esempio `s3://bucket-and-or-prefix`, nel parametro `LocationScope`.

```
public void listAccessGrantsLocations() {

    ListAccessGrantsLocationsRequest listRequest =
        ListAccessGrantsLocationsRequest.builder()
            .accountId("111122223333")
            .build();

    ListAccessGrantsLocationsResponse listResponse =
        s3Control.listAccessGrantsLocations(listRequest);
    LOGGER.info("ListAccessGrantsLocationsResponse: " + listResponse);
}
```

Risposta:

```
ListAccessGrantsLocationsResponse(
    AccessGrantsLocationsList=[
        ListAccessGrantsLocationsEntry(
            CreatedAt=2023-06-07T04:35:11.027Z,
            AccessGrantsLocationId=default,
```

```
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
),
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb456,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixA*,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
]
)
```

Aggiornamento di una posizione registrata

Puoi aggiornare il ruolo AWS Identity and Access Management (IAM) di una sede registrata nella tua istanza Amazon S3 Access Grants. Per ogni nuovo ruolo IAM che utilizzi per registrare una posizione in S3 Access Grants, assicurati di consentire al principale (access-grants.s3.amazonaws.com) del servizio di S3 Access Grants l'accesso a questo ruolo. Per fare ciò, aggiungi una voce per il nuovo ruolo IAM nello stesso file JSON della policy di attendibilità che hai usato quando hai registrato la [posizione per la prima volta](#).

Puoi aggiornare una posizione nella tua istanza S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per aggiornare il ruolo IAM di una posizione registrata con la tua istanza S3 Access Grants

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.
4. Scegli Visualizza dettagli per l'istanza.
5. Nella pagina dei dettagli dell'istanza, scegli la scheda Posizioni.

6. Trova la posizione che intendi aggiornare. Per filtrare l'elenco delle posizioni, usa la casella di ricerca.
7. Scegli il pulsante delle opzioni accanto alla posizione registrata che desideri aggiornare.
8. Aggiorna il ruolo IAM, quindi scegli Salva modifiche.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Aggiorna il ruolo IAM di una posizione registrata

```
aws s3control update-access-grants-location \  
--account-id 111122223333 \  
--access-grants-location-id 635f1139-1af2-4e43-8131-a4de006eb999 \  
--iam-role-arn arn:aws:iam::777788889999:role/accessGrantsTestRole
```

Risposta:

```
{  
  "CreatedAt": "2023-05-31T18:23:48.107000+00:00",  
  "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb999",  
  "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:777788889999:access-grants/  
default/location/635f1139-1af2-4e43-8131-a4de006eb888",  
  "LocationScope": "s3://amzn-s3-demo-bucket/prefixB*",  
  "IAMRoleArn": "arn:aws:iam::777788889999:role/accessGrantsTestRole"  
}
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'aggiornamento della posizione in un'istanza S3 Access Grants, consulta [UpdateAccessGrantsLocation](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di AWS SDK

Questa sezione fornisce esempi di come aggiornare il ruolo IAM di una sede registrata utilizzando gli AWS SDK.

Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate.

Java

Example– Aggiorna il ruolo IAM di una posizione registrata

```
public void updateAccessGrantsLocation() {
    UpdateAccessGrantsLocationRequest updateRequest =
        UpdateAccessGrantsLocationRequest.builder()
            .accountId("111122223333")
            .accessGrantsLocationId("635f1139-1af2-4e43-8131-a4de006eb999")
            .iamRoleArn("arn:aws:iam::777788889999:role/accessGrantsTestRole")
            .build();
    UpdateAccessGrantsLocationResponse updateResponse =
        s3Control.updateAccessGrantsLocation(updateRequest);
    LOGGER.info("UpdateAccessGrantsLocationResponse: " + updateResponse);
}
```

Risposta:

```
UpdateAccessGrantsLocationResponse(
    CreatedAt=2023-06-07T04:35:10.027Z,
    AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb999,
    AccessGrantsLocationArn=arn:aws:s3:us-east-2:777788889999:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
    LocationScope=s3://amzn-s3-demo-bucket/prefixB*,
    IAMRoleArn=arn:aws:iam::777788889999:role/accessGrantsTestRole
)
```

Eliminazione di una posizione registrata

Puoi eliminare la registrazione di una posizione da un'istanza Amazon S3 Access Grants. L'eliminazione della posizione ne annulla la registrazione dall'istanza S3 Access Grants.

Prima di poter rimuovere una registrazione di una posizione da un'istanza S3 Access Grants, devi eliminare tutte le concessioni associate a questa posizione. Per informazioni sull'eliminazione delle concessioni, consulta [Elimina una concessione](#).

Puoi eliminare una posizione nella tua istanza S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per eliminare la registrazione di una posizione dalla tua istanza Amazon S3 Access Grants

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.
4. Scegli Visualizza dettagli per l'istanza.
5. Nella pagina dei dettagli dell'istanza, scegli la scheda Posizioni.
6. Trova la posizione che intendi aggiornare. Per filtrare l'elenco delle posizioni, usa la casella di ricerca.
7. Scegli il pulsante di opzione accanto alla posizione registrata che desideri eliminare.
8. Scegli Annulla registrazione.
9. Viene visualizzata una finestra di dialogo che avverte che questa azione non può essere annullata. Per eliminare la posizione, scegli Annulla registrazione.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Elimina la registrazione di una posizione

```
aws s3control delete-access-grants-location \  
--account-id 111122223333 \  
--access-grants-location-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
// No response body
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per l'eliminazione di una posizione da un'istanza S3 Access Grants, consulta [DeleteAccessGrantsLocation](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di AWS SDK

Questa sezione fornisce esempi su come eliminare una posizione tramite gli AWS SDK.

Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate.

Java

Example– Elimina la registrazione di una posizione

```
public void deleteAccessGrantsLocation() {
    DeleteAccessGrantsLocationRequest deleteRequest =
        DeleteAccessGrantsLocationRequest.builder()
            .accountId("111122223333")
            .accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
            .build();
    DeleteAccessGrantsLocationResponse deleteResponse =
        s3Control.deleteAccessGrantsLocation(deleteRequest);
    LOGGER.info("DeleteAccessGrantsLocationResponse: " + deleteResponse);
}
```

Risposta:

```
DeleteAccessGrantsLocationResponse()
```

Operazioni con le concessioni in S3 Access Grants

Una concessione di accesso individuale in un'istanza di S3 Access Grants consente a un'identità specifica, un principale AWS Identity and Access Management (IAM) o un utente o gruppo in una directory aziendale, di ottenere l'accesso all'interno di una posizione registrata nell'istanza S3 Access Grants. Una posizione mappa i bucket o i prefissi a un ruolo IAM. S3 Access Grants assume questo ruolo IAM per vendere credenziali temporanee ai beneficiari.

Dopo aver [registrato almeno una posizione](#) nell'istanza di S3 Access Grants, è possibile creare una concessione di accesso.

Il beneficiario può essere un utente o un ruolo IAM oppure un utente o un gruppo della directory. Un utente della directory è un utente della directory aziendale o di una fonte di identità esterna che è stato [associato all'istanza S3 Access Grants](#). Per ulteriori informazioni, consulta [S3 Access Grants e](#)

[identità delle directory aziendali](#). Per creare una concessione per un utente o gruppo specifico della directory dal Centro identità IAM, trovare il GUID che il Centro identità IAM utilizza per identificare l'utente nel Centro identità IAM, ad esempio a1b2c3d4-5678-90ab-cdef-EXAMPLE11111. Per ulteriori informazioni su come utilizzare il Centro identità IAM per visualizzare le informazioni sugli utenti, consulta [Visualizzazione delle assegnazioni di utenti e gruppi](#) nella Guida all'utente Centro identità AWS IAM .

È possibile concedere l'accesso a un bucket, a un prefisso o a un oggetto. Un prefisso in Amazon S3 è una stringa di caratteri all'inizio del nome della chiave di un oggetto che viene utilizzata per organizzare gli oggetti all'interno di un bucket. Può essere una qualsiasi stringa di caratteri consentiti, ad esempio i nomi delle chiavi degli oggetti nel bucket che iniziano con il prefisso engineering/.

Argomenti

- [Creazione di concessioni](#)
- [Visualizza una concessione](#)
- [Eliminazione di una concessione](#)

Creazione di concessioni

Una concessione di accesso individuale in un'istanza S3 Access Grants consente a un'identità specifica, un principale AWS Identity and Access Management (IAM) o un utente o gruppo in una directory aziendale, di ottenere l'accesso all'interno di una posizione registrata nell'istanza S3 Access Grants. Una posizione mappa i bucket o i prefissi a un ruolo IAM. S3 Access Grants assume questo ruolo IAM per vendere credenziali temporanee ai beneficiari.

Dopo aver [registrato almeno una posizione](#) nell'istanza di S3 Access Grants, è possibile creare una concessione di accesso.

Il beneficiario può essere un utente o un ruolo IAM oppure un utente o un gruppo della directory. Un utente della directory è un utente della directory aziendale o di una fonte di identità esterna che è stato [associato all'istanza S3 Access Grants](#). Per ulteriori informazioni, consulta [S3 Access Grants e identità delle directory aziendali](#). Per creare una concessione per un utente o gruppo specifico della directory dal Centro identità IAM, trovare il GUID che il Centro identità IAM utilizza per identificare l'utente nel Centro identità IAM, ad esempio a1b2c3d4-5678-90ab-cdef-EXAMPLE11111. Per ulteriori informazioni su come utilizzare il Centro identità IAM per visualizzare le informazioni sugli utenti, consulta [Visualizzazione delle assegnazioni di utenti e gruppi](#) nella Guida all'utente Centro identità AWS IAM .

È possibile concedere l'accesso a un bucket, a un prefisso o a un oggetto. Un prefisso in Amazon S3 è una stringa di caratteri all'inizio del nome della chiave di un oggetto che viene utilizzata per organizzare gli oggetti all'interno di un bucket. Può essere una qualsiasi stringa di caratteri consentiti, ad esempio i nomi delle chiavi degli oggetti nel bucket che iniziano con il prefisso `engineering/`.

Sottoprefisso

Quando si concede l'accesso a una località registrata, è possibile utilizzare il campo `Subprefix` per restringere l'ambito di accesso a un sottoinsieme dell'ambito della località. Se la posizione registrata scelta per il grant è il percorso S3 predefinito (`s3://`), è necessario restringere l'ambito della concessione. Non è possibile creare una concessione di accesso per la posizione predefinita (`s3://`), che darebbe al beneficiario l'accesso a ogni bucket di Regione AWS. Invece, è necessario restringere l'ambito della concessione a uno dei seguenti punti:

- Un bucket: `s3://bucket/*`
- Un prefisso all'interno di un bucket: `s3://bucket/prefix*`
- Un prefisso all'interno di un prefisso: `s3://bucket/prefixA/prefixB*`
- Un oggetto: `s3://bucket/object-key-name`

Se si sta creando una concessione di accesso in cui la posizione registrata è un bucket, è possibile passare uno dei seguenti valori nel campo `Subprefix` per restringere l'ambito della concessione:

- Un prefisso all'interno del bucket: `prefix*`
- Un prefisso all'interno di un prefisso: `prefixA/prefixB*`
- Un oggetto: `/object-key-name`

Dopo aver creato la concessione, l'ambito di concessione visualizzato nella console Amazon S3 o GrantScope quello restituito nella risposta API o AWS Command Line Interface (AWS CLI) è il risultato della concatenazione del percorso della posizione con. `Subprefix` Assicurati che questo percorso concatenato sia mappato correttamente al bucket, al prefisso o all'oggetto S3 a cui desideri concedere l'accesso.

Note

- Se si desidera creare una concessione di accesso che garantisca l'accesso a un solo oggetto, è necessario specificare che il tipo di concessione è per un oggetto. Per fare

questo in una chiamata API o in un comando CLI, passare il parametro `s3PrefixType` con il valore `Object`. Nella console Amazon S3, quando si crea la concessione, dopo aver selezionato una posizione, in Ambito di concessione, seleziona la casella di controllo L'ambito di concessione è un oggetto.

- Non puoi creare una concessione a un bucket se il bucket non esiste ancora. Tuttavia, è possibile creare una concessione per un prefisso che ancora non esiste.
- Per il numero massimo di concessioni che è possibile creare nell'istanza S3 Access Grants, consulta [Limitazioni di S3 Access Grants](#).

Puoi creare una concessione di accesso utilizzando la console Amazon S3 AWS CLI, l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per creare una concessione di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.

Se utilizzi un'istanza S3 Access Grants per la prima volta, assicurati di aver completato il [Passaggio 2: registra una posizione](#) e di aver eseguito il Passaggio 3 della procedura guidata Configurazione dell'istanza Access Grants. Se hai già un'istanza S3 Access Grants, scegli Visualizza dettagli, quindi dalla scheda Concessioni, scegli Crea concessione.

- a. Nella sezione Ambito della concessione, seleziona o inserisci una posizione registrata.

Se hai selezionato la posizione `s3://` predefinita, utilizza la casella Sottoprefisso per restringere l'ambito della concessione di accesso. Per ulteriori informazioni, consulta [Sottoprefisso](#). Se concedi l'accesso solo a un oggetto, seleziona L'ambito della concessione è un oggetto.

- b. In Autorizzazioni e accesso, seleziona il livello di Autorizzazione, ovvero Lettura, Scrittura o entrambi.

Quindi seleziona Tipo di assegnatario. Se hai aggiunto la tua directory aziendale al Centro identità IAM e hai associato questa istanza del Centro identità IAM all'istanza S3 Access Grants, puoi scegliere Identità della directory dal Centro identità IAM. Se scegli questa opzione, ottieni l'ID dell'utente o del gruppo dal Centro identità IAM e inseriscilo in questa sezione.

Se Tipo di assegnatario è un utente o un ruolo IAM, scegli Principale IAM. In Tipo di principale IAM, scegli Utente o Ruolo. Quindi, in Utente principale IAM, seleziona dall'elenco o inserisci l'ID dell'identità.

c. Per creare la concessione S3 Access Grants, seleziona Avanti o Crea concessione.

4. Se l'opzione Avanti o Crea concessione è disabilitata:

Impossibile creare una concessione

- Potrebbe essere necessario [registrare prima una posizione](#) nell'istanza S3 Access Grants.
- Potresti non disporre dell'autorizzazione `s3:CreateAccessGrant` per creare una concessione di accesso. Contatta l'amministratore dell'account.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Gli esempi seguenti mostrano come creare una richiesta di concessione di accesso per un principale IAM e come creare una richiesta di concessione di accesso per un utente o un gruppo della directory aziendale.

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le tue informazioni.

Note

Se stai creando una concessione di accesso che conceda l'accesso a un solo oggetto, includi il parametro `--s3-prefix-type Object` richiesto.

Example Crea una richiesta di concessione di accesso per un principale IAM

```
aws s3control create-access-grant \
--account-id 111122223333 \
--access-grants-location-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
--access-grants-location-configuration S3SubPrefix=prefixB* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::123456789012:user/data-consumer-3
```

Example Crea una risposta alla concessione di accesso

```
{
  "CreatedAt": "2023-05-31T18:41:34.663000+00:00",
  "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/grant/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Grantee": {
    "GranteeType": "IAM",
    "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
  },
  "AccessGrantsLocationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "AccessGrantsLocationConfiguration": {
    "S3SubPrefix": "prefixB*"
  },
  "GrantScope": "s3://amzn-s3-demo-bucket/prefix*",
  "Permission": "READ"
}
```

Creazione di una richiesta di autorizzazione di accesso per un utente o un gruppo di utenti della directory

Per creare una richiesta di concessione di accesso per un utente o un gruppo della directory, è necessario innanzitutto ottenere il GUID per l'utente o il gruppo della directory eseguendo uno dei seguenti comandi.

Example Ottieni un GUID per un utente o un gruppo di utenti della directory

Puoi trovare il GUID di un utente di IAM Identity Center tramite la console IAM Identity Center o utilizzando gli AWS SDK AWS CLI or. Il comando seguente elenca gli utenti nell'istanza del Centro identità IAM specificata, con i relativi nomi e identificatori.

```
aws identitystore list-users --identity-store-id d-1a2b3c4d1234
```


Questo comando elenca i gruppi nell'istanza Centro identità IAM specificata.

```
aws identitystore list-groups --identity-store-id d-1a2b3c4d1234
```

Example Creazione di una concessione di accesso per un utente o un gruppo di directory

Questo comando è simile alla creazione di una concessione per utenti o ruoli IAM, tranne per il fatto che il tipo di assegnatario è DIRECTORY_USER o DIRECTORY_GROUP e l'identificatore dell'assegnatario è il GUID per l'utente o il gruppo di directory.

```
aws s3control create-access-grant \  
--account-id 123456789012 \  
--access-grants-location-id default \  
--access-grants-location-configuration S3SubPrefix="amzn-s3-demo-bucket/rafael/*" \  
--permission READWRITE \  
--grantee GranteeType=DIRECTORY_USER,GranteeIdentifier=83d43802-00b1-7054-db02-f1d683aacba5 \  

```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la gestione delle concessioni di accesso, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [CreateAccessGrant](#)
- [DeleteAccessGrant](#)
- [GetAccessGrant](#)
- [ListAccessGrants](#)

Utilizzo di AWS SDK

Questa sezione fornisce esempi di come creare una concessione di accesso utilizzando gli AWS SDK.

Java

Per utilizzare il seguente esempio, sostituisci *user input placeholders* con le tue informazioni.

Note

Se crei una concessione di accesso che conceda l'accesso a un solo oggetto, includi il parametro `.s3PrefixType(S3PrefixType.Object)` richiesto.

Example Crea una risposta alla concessione di accesso

```
public void createAccessGrant() {
    CreateAccessGrantRequest createRequest = CreateAccessGrantRequest.builder()
        .accountId("111122223333")
        .accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaa")
        .permission("READ")
        .accessGrantsLocationConfiguration(AccessGrantsLocationConfiguration.builder().s3SubPrefix("prefixB")
            .grantee(Grantee.builder().granteeType("IAM").granteeIdentifier("arn:aws:iam::111122223333:user/data-consumer-3").build())
            .build());
    CreateAccessGrantResponse createResponse =
        s3Control.createAccessGrant(createRequest);
    LOGGER.info("CreateAccessGrantResponse: " + createResponse);
}
```

Example Crea una risposta alla concessione di accesso

```
CreateAccessGrantResponse(
    CreatedAt=2023-06-07T05:20:26.330Z,
    AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
    AccessGrantArn=arn:aws:s3:us-east-2:444455556666:access-grants/default/grant/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
    Grantee=Grantee(
        GranteeType=IAM,
        GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
    ),
    AccessGrantsLocationId=a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa,
    AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
        S3SubPrefix=prefixB*
    ),
    GrantScope=s3://amzn-s3-demo-bucket/prefixB,
    Permission=READ
)
```

Visualizza una concessione

Puoi visualizzare i dettagli di una concessione di accesso nella tua istanza Amazon S3 Access Grants utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare i dettagli di una concessione di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.
4. Scegli Visualizza dettagli per l'istanza.
5. Nella pagina Dettagli, scegli la scheda Concessioni.
6. Nella sezione Concessioni, trova la concessione di accesso che desideri visualizzare. Puoi utilizzare la casella di ricerca per filtrare l'elenco delle concessioni.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le informazioni appropriate.

Example– Ottieni i dettagli di una concessione di accesso

```
aws s3control get-access-grant \  
--account-id 111122223333 \  
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Risposta:

```
{  
  "CreatedAt": "2023-05-31T18:41:34.663000+00:00",  
  "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
```

```

    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-a1b2c3d4-5678-90ab-cdef-EXAMPLE2222",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "Permission": "READ",
    "AccessGrantsLocationId": "12a6710f-5af8-41f5-b035-0bc795bf1a2b",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
    "GrantScope": "s3://amzn-s3-demo-bucket/"
}

```

Example– Elenca tutte le concessioni di accesso in un'istanza S3 Access Grants

Facoltativamente, puoi utilizzare i seguenti parametri per limitare i risultati a un prefisso S3 o a un'identità AWS Identity and Access Management (IAM):

- Sottoprefisso: `--grant-scope s3://bucket-name/prefix*`
- Identità IAM: `--grantee-type IAM` e `--grantee-identifier arn:aws:iam::123456789000:role/accessGrantsConsumerRole`

```

aws s3control list-access-grants \
--account-id 111122223333

```

Risposta:

```

{
    "AccessGrantsList": [{
        "CreatedAt": "2023-06-14T17:54:46.542000+00:00",
        "AccessGrantId": "dd8dd089-b224-4d82-95f6-975b4185bbaa",
        "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa",
        "Grantee": {
            "GranteeType": "IAM",
            "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
        },
        "Permission": "READ",
        "AccessGrantsLocationId": "23514a34-ea2e-4ddf-b425-d0d4bfcarda1",
        "GrantScope": "s3://amzn-s3-demo-bucket/prefixA*"
    },
}

```

```
{
  "CreatedAt": "2023-06-24T17:54:46.542000+00:00",
  "AccessGrantId": "ee8ee089-b224-4d72-85f6-975b4185a1b2",
  "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/grant/ee8ee089-b224-4d72-85f6-975b4185a1b2",
  "Grantee": {
    "GranteeType": "IAM",
    "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-9"
  },
  "Permission": "READ",
  "AccessGrantsLocationId": "12414a34-ea2e-4ddf-b425-d0d4bfcacao0",
  "GrantScope": "s3://amzn-s3-demo-bucket/prefixB*"
},
]
}
```

Utilizzo della REST API

Puoi utilizzare le operazioni API di Amazon S3 per visualizzare i dettagli di una concessione di accesso ed elencare tutte le concessioni di accesso in un'istanza S3 Access Grants. Per informazioni sul supporto REST API per la gestione delle concessioni di accesso, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [GetAccessGrant](#)
- [ListAccessGrants](#)

Utilizzo di AWS SDK

Questa sezione fornisce esempi di come ottenere i dettagli di una concessione di accesso utilizzando gli SDK. AWS

Per utilizzare gli esempi seguenti, sostituisci *user input placeholders* con le tue informazioni.

Java

Example– Ottieni i dettagli di una concessione di accesso

```
public void getAccessGrant() {
  GetAccessGrantRequest getRequest = GetAccessGrantRequest.builder()
    .accountId("111122223333")
    .accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE2222")
}
```

```
.build();
GetAccessGrantResponse getResponse = s3Control.getAccessGrant(getRequest);
LOGGER.info("GetAccessGrantResponse: " + getResponse);
}
```

Risposta:

```
GetAccessGrantResponse(
  CreatedAt=2023-06-07T05:20:26.330Z,
  AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE2222,
  AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-fd3a5086-42f7-4b34-9fad-472e2942c70e,
  Grantee=Grantee(
    GranteeType=IAM,
    GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
  ),
  Permission=READ,
  AccessGrantsLocationId=12a6710f-5af8-41f5-b035-0bc795bf1a2b,
  AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
    S3SubPrefix=prefixB*
  ),
  GrantScope=s3://amzn-s3-demo-bucket/
)
```

Example– Elenca tutte le concessioni di accesso in un'istanza S3 Access Grants

Facoltativamente, puoi utilizzare questi parametri per limitare i risultati a un prefisso S3 o un'identità IAM:

- Ambito: `GrantScope=s3://bucket-name/prefix*`
- Assegnatario: `GranteeType=IAM` e `GranteeIdentifier=arn:aws:iam::111122223333:role/accessGrantsConsumerRole`

```
public void listAccessGrants() {
  ListAccessGrantsRequest listRequest = ListAccessGrantsRequest.builder()
    .accountId("111122223333")
    .build();
  ListAccessGrantsResponse listResponse = s3Control.listAccessGrants(listRequest);
  LOGGER.info("ListAccessGrantsResponse: " + listResponse);
}
```

Risposta:

```
ListAccessGrantsResponse(
  AccessGrantsList=[
    ListAccessGrantEntry(
      CreatedAt=2023-06-14T17:54:46.540z,
      AccessGrantId=dd8dd089-b224-4d82-95f6-975b4185bbaa,
      AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa,
      Grantee=Grantee(
        GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-3
      ),
      Permission=READ,
      AccessGrantsLocationId=23514a34-ea2e-4ddf-b425-d0d4bfcada1,
      GrantScope=s3://amzn-s3-demo-bucket/prefixA
    ),
    ListAccessGrantEntry(
      CreatedAt=2023-06-24T17:54:46.540Z,
      AccessGrantId=ee8ee089-b224-4d72-85f6-975b4185a1b2,
      AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2,
      Grantee=Grantee(
        GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-9
      ),
      Permission=READ,
      AccessGrantsLocationId=12414a34-ea2e-4ddf-b425-d0d4bfcacao0,
      GrantScope=s3://amzn-s3-demo-bucket/prefixB*
    )
  ]
)
```

Eliminazione di una concessione

Puoi eliminare un'istanza di Amazon S3 Access Grants da una nel tuo account. L'eliminazione di una concessione di accesso non può essere annullata. Dopo aver eliminato una concessione di accesso, l'assegnatario non avrà più accesso ai tuoi dati Amazon S3.

Puoi eliminare una concessione di accesso utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per eliminare un'autorizzazione di accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Access Grants.
3. Nella pagina S3 Access Grants, scegli la regione che contiene l'istanza S3 Access Grants con cui vuoi lavorare.
4. Scegli Visualizza dettagli per l'istanza.
5. Nella pagina Dettagli, scegli la scheda Concessioni.
6. Cerca la concessione che intendi eliminare. Quando trovi la concessione, scegli il pulsante di opzione accanto a essa.
7. Scegliere Elimina. Viene visualizzata una finestra di dialogo che avverte che questa azione non può essere annullata. Scegli nuovamente Elimina per eliminare la concessione.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Eliminazione di una concessione di accesso

```
aws s3control delete-access-grant \  
--account-id 111122223333 \  
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111  
  
// No response body
```

Utilizzo della REST API

Per informazioni sul supporto REST API di Amazon S3 per la gestione delle concessioni di accesso, consulta [DeleteAccessGrant](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Utilizzo di AWS SDK

Questa sezione fornisce esempi di come eliminare una concessione di accesso utilizzando gli AWS SDK. Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate.

Java

Example– Eliminazione di una concessione di accesso

```
public void deleteAccessGrant() {
    DeleteAccessGrantRequest deleteRequest = DeleteAccessGrantRequest.builder()
        .accountId("111122223333")
        .accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
        .build();
    DeleteAccessGrantResponse deleteResponse =
        s3Control.deleteAccessGrant(deleteRequest);
    LOGGER.info("DeleteAccessGrantResponse: " + deleteResponse);
}
```

Risposta:

```
DeleteAccessGrantResponse()
```

Ottenere i dati S3 utilizzando i grant di accesso

I beneficiari che hanno ottenuto l'accesso ai dati S3 tramite S3 Access Grants devono richiedere le credenziali temporanee a S3 Access Grants, che utilizzano per accedere ai dati S3. Per ulteriori informazioni, consulta [Richiedi l'accesso ai dati di Amazon S3 tramite S3 Access Grants](#). I beneficiari utilizzano quindi le credenziali temporanee per eseguire azioni S3 consentite sui dati S3. Per ulteriori informazioni, consulta [Accedere ai dati S3 utilizzando le credenziali fornite da S3 Access Grants](#). I beneficiari possono facoltativamente richiedere un elenco delle loro autorizzazioni di accesso prima di richiedere queste credenziali. Account AWS Per ulteriori informazioni, consulta [Elenco dei permessi di accesso del chiamante](#).

Argomenti

- [Richiedi l'accesso ai dati di Amazon S3 tramite S3 Access Grants](#)
- [Accedere ai dati S3 utilizzando le credenziali fornite da S3 Access Grants](#)
- [Elenco dei permessi di accesso del chiamante](#)

Richiedi l'accesso ai dati di Amazon S3 tramite S3 Access Grants

Dopo aver [creato una concessione di accesso](#) utilizzando S3 Access Grants, gli assegnatari possono richiedere le credenziali per accedere ai dati S3 di cui dispongono delle autorizzazioni. I beneficiari possono essere titolari AWS Identity and Access Management (IAM), identità della directory aziendale o applicazioni autorizzate.

Un'applicazione o Servizio AWS può utilizzare l'operazione `GetDataAccess` API S3 Access Grants per chiedere a S3 Access Grants di accedere ai dati S3 per conto di un beneficiario. `GetDataAccess` verifica innanzitutto che tu abbia concesso a questa identità l'accesso ai dati. Quindi, S3 Access Grants utilizza l'operazione [AssumeRole](#) per ottenere un token credenziale temporaneo e lo invia al richiedente. Questo token di credenziali temporaneo è un token Servizio di token di sicurezza AWS (AWS STS).

La richiesta `GetDataAccess` deve includere il parametro `target`, che specifica l'ambito dei dati S3 a cui si applicano le credenziali temporanee. Questo ambito `target` può essere lo stesso dell'ambito della concessione o di un sottoinsieme di tale ambito, ma l'ambito `target` deve rientrare nell'ambito della concessione accordata all'assegnatario. La richiesta deve inoltre specificare il parametro `permission` per indicare il livello di autorizzazione per le credenziali temporanee, `READ`, `WRITE` o `READWRITE`.

Privilegio

Il richiedente può specificare il livello di privilegio del token temporaneo nella richiesta di credenziali. Utilizzando il parametro `privilege`, il richiedente può ridurre o ingrandire l'ambito di accesso delle credenziali temporanee entro i limiti dell'ambito della concessione. Il valore predefinito del parametro `privilege` è `Default`, il che significa che l'ambito di destinazione della credenziale restituita è l'ambito della concessione originale. L'altro valore possibile per `privilege` è `Minimal`. Se l'ambito `target` viene ridotto rispetto all'ambito della concessione originale, la credenziale temporanea viene ridimensionata per corrispondere all'ambito `target`, purché l'ambito `target` rientri nell'ambito della concessione.

La tabella seguente descrive in dettaglio l'effetto del parametro `privilege` su due concessioni. Una concessione ha l'ambito `S3://amzn-s3-demo-bucket1/bob/*`, che include l'intero prefisso `bob/` nel bucket `amzn-s3-demo-bucket1`. Una concessione ha l'ambito `S3://amzn-s3-demo-bucket1/bob/reports/*`, che include l'intero prefisso `bob/reports/` nel bucket `amzn-s3-demo-bucket1`.

Ambito della concessione	Ambito richiesto	Privilegio	Ambito restituito	Effetto
S3:// <i>amzn-s3-demo-bucket1</i> /bob/*	<i>amzn-s3-demo-bucket1</i> /bob/*	Default	<i>amzn-s3-demo-bucket1</i> /bob/*	Il richiedente ha accesso a tutti gli oggetti i cui nomi della chiave iniziano con il prefisso <i>bob/</i> nel bucket <i>amzn-s3-demo-bucket1</i> .
S3:// <i>amzn-s3-demo-bucket1</i> /bob/*	<i>amzn-s3-demo-bucket1</i> /bob/*	Minimal	<i>amzn-s3-demo-bucket1</i> /bob/	Senza un carattere jolly * dopo il nome del prefisso <i>bob/</i> , il richiedente ha accesso solo all'oggetto denominato <i>bob/</i> nel bucket <i>amzn-s3-demo-bucket1</i> . Non è comune avere un oggetto del genere. Il richiedente non ha accesso a nessun altro oggetto, compresi quelli con nomi chiave che iniziano con il prefisso <i>bob/</i> .
S3:// <i>amzn-s3-demo-bucket1</i> /bob/*	<i>amzn-s3-demo-bucket1</i> /bob/images/*	Minimal	<i>amzn-s3-demo-bucket1</i> /bob/images/*	Il richiedente ha accesso a tutti gli oggetti i cui nomi della chiave iniziano con il prefisso <i>bob/images/</i> * nel bucket <i>amzn-s3-demo-bucket1</i> .
S3:// <i>amzn-s3-demo-bucket1</i> /bob/*	<i>amzn-s3-demo-bucket1</i> /bob/reports/*	Default	<i>amzn-s3-demo-bucket1</i> /bob/reports/*	Il richiedente ha accesso a tutti gli oggetti i cui nomi della chiave iniziano con il

Ambito della concessione	Ambito richiesto	Privilegio	Ambito restituito	Effetto
<i>bucket1</i> /bob/ repo rts/*	<i>t1</i> /bob/ repo rts/ file. txt			prefisso bob/reports nel bucket <i>amzn-s3-demo-bucket1</i> , che è l'ambito della concessione corrispondente.
S3:// <i>amzn-s3-demo-bucket1</i> /bob/ repo rts/*	<i>amzn-s3-demo-bucket1</i> /bob/ repo rts/ file. txt	Minimal	<i>amzn-s3-demo-bucket1</i> /bob/reports/ file.txt	Il richiedente ha accesso solo all'oggetto con il nome della chiave bob/reports/file.txt nel bucket <i>amzn-s3-demo-bucket1</i> . Il richiedente non ha accesso a nessun altro oggetto.

Identità delle directory

GetDataAccess considera tutte le identità coinvolte in una richiesta quando corrispondono alle concessioni adeguate. Per le identità delle directory aziendali, GetDataAccess restituisce anche le concessioni dell'identità IAM utilizzata per la sessione con riconoscimento dell'identità. Per ulteriori informazioni sulle sessioni con riconoscimento dell'identità, consulta [Concessione delle autorizzazioni per l'utilizzo di sessioni di console con riconoscimento dell'identità](#) nella Guida per l'utente di AWS Identity and Access Management . GetDataAccess genera credenziali limitando l'ambito alla concessione più restrittiva, come illustrato nella tabella seguente:

Ambito di concessione per l'identità IAM	Ambito di concessione per l'identità delle directory	Ambito richiesto	Ambito restituito	Privilegio	Effetto
S3://amzn-s3-demo-bucket1 /	amzn-s3-demo-bucket1 / images/	S3://amzn-s3-demo-bucket1 / images/image1.jpeg	S3://amzn-s3-demo-bucket1 / bob/images/	Default	Il richiedente ha accesso a tutti gli oggetti con nomi di chiave che iniziano con il prefisso bob/ come parte della concessione per il ruolo IAM ma sono limitati ai prefissi bob/images/come parte della concessione per l'identità della directory. Sia il ruolo IAM sia l'identità delle directory forniscono l'accesso all'ambito richiesto, vale a dire bob/images/image1.jpeg , ma l'identità delle directory ha una concessione più restrittiva. Pertanto, l'ambito restituito è limitato alla concessione più restrittiva per l'identità delle directory.

Ambito di concessione per l'identità IAM	Ambito di concessione per l'identità delle directory	Ambito richiesto	Ambito restituito	Privilegio	Effetto
S3:// <i>amzn-s3-demo-bucket1</i> / bob/*	<i>amzn-s3-demo-bucket1</i> / bob/images/*	S3:// <i>amzn-s3-demo-bucket1</i> / bob/images/image1.jpeg	S3:// <i>amzn-s3-demo-bucket1</i> / bob/images/image1.jpeg	Minimal	Poiché il privilegio è impostato su Minimal, anche se l'identità ha accesso a un ambito più ampio, viene restituito solo l'ambito richiesto bob/images/image1.jpeg .

Ambito di concessione per l'identità IAM	Ambito di concessione per l'identità delle directory	Ambito richiesto	Ambito restituito	Privilegio	Effetto
S3://amzn-s3-demo-bucket1 / bob/images/	amzn-s3-demo-bucket1 / bob/*	S3://amzn-s3-demo-bucket1 / bob/images/	S3://amzn-s3-demo-bucket1 / bob/images/	Default	Il richiedente ha accesso a tutti gli oggetti con nomi di chiave che iniziano con il prefisso bob/ come parte della concessione per l'identità della directory ma è limitato ai prefissi bob/images/come parte della concessione per il ruolo IAM. Sia il ruolo IAM sia l'identità delle directory forniscono l'accesso all'ambito richiesto, vale a dire bob/images/ image1.jpeg , ma il ruolo IAM ha una concessione più restrittiva. Pertanto, l'ambito restituito è limitato alla concessione più restrittiva per il ruolo IAM.

Ambito di concessione per l'identità IAM	Ambito di concessione per l'identità delle directory	Ambito richiesto	Ambito restituito	Privilegio	Effetto
<code>S3://amzn-s3-demo-bucket1 / bob/images/</code>	<code>amzn-s3-demo-bucket1 / bob/*</code>	<code>S3://amzn-s3-demo-bucket1 / bob/images/</code>	<code>S3://amzn-s3-demo-bucket1 / bob/images/ image1.jpeg</code>	Minimal	Poiché il privilegio è impostato su Minimal, anche se l'identità ha accesso a un ambito più ampio, viene restituito solo l'ambito richiesto <code>bob/images/ image1.jpeg</code> .

Durata

Il parametro `durationSeconds` imposta la durata della credenziale temporanea, in secondi. Il valore predefinito è 3600 secondi (1 ora), ma il richiedente (l'assegnatario) può specificare un intervallo da 900 secondi (15 minuti) a 43200 secondi (12 ore). Se l'assegnatario richiede un valore superiore a questo valore massimo, la richiesta ha esito negativo.

Note

Nella richiesta di un token temporaneo, se la posizione è un oggetto, imposta il valore del parametro `targetType` nella richiesta a `Object`. Questo parametro è obbligatorio solo se la posizione è un oggetto e il livello di privilegio è `Minimal`. Se la posizione è un bucket o un prefisso, non devi specificare questo parametro.

Esempi

Puoi richiedere credenziali temporanee utilizzando AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS Consulta questi esempi.

Per ulteriori informazioni, consulta [Amazon `GetDataAccess` Simple Storage Service API Reference](#).

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida AWS Command Line Interface per l'utente.

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example Richiesta di credenziali temporanee

Richiesta:

```
aws s3control get-data-access \
--account-id 111122223333 \
--target s3://amzn-s3-demo-bucket/prefixA* \
--permission READ \
--privilege Default \
--region us-east-2
```

Risposta:

```
{
  "Credentials": {
    "AccessKeyId": "Example-key-id",
    "SecretAccessKey": "Example-access-key",
    "SessionToken": "Example-session-token",
    "Expiration": "2023-06-14T18:56:45+00:00"},
    "MatchedGrantTarget": "s3://amzn-s3-demo-bucket/prefixA**",
    "Grantee": {
      "GranteeType": "IAM",
      "GranteeIdentifier": "arn:aws:iam::111122223333:role/role-name"
    }
  }
}
```

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la richiesta di credenziali temporanee da S3 Access Grants, consulta l'Amazon Simple Storage [GetDataAccess](#) Service API Reference.

Utilizzo di AWS SDK

Questa sezione fornisce un esempio di come i beneficiari richiedono credenziali temporanee da S3 Access Grants utilizzando gli SDK. AWS

Java

Il seguente esempio di codice restituisce le credenziali temporanee utilizzate dall'assegnatario per accedere ai tuoi dati S3. Per utilizzare questo esempio di codice, sostituisci *user input placeholders* con le tue informazioni.

Example Ottenimento di credenziali temporanee

Richiesta:

```
public void getDataAccess() {
    GetDataAccessRequest getDataAccessRequest = GetDataAccessRequest.builder()
        .accountId("111122223333")
        .permission(Permission.READ)
        .privilege(Privilege.MINIMAL)
        .target("s3://amzn-s3-demo-bucket/prefixA*")
        .build();
    GetDataAccessResponse getDataAccessResponse =
        s3Control.getDataAccess(getDataAccessRequest);
    LOGGER.info("GetDataAccessResponse: " + getDataAccessResponse);
}
```

Risposta:

```
GetDataAccessResponse(
    Credentials=Credentials(
        AccessKeyId="Example-access-key-id",
        SecretAccessKey="Example-secret-access-key",
        SessionToken="Example-session-token",
        Expiration=2023-06-07T06:55:24Z
    ))
```

Accedere ai dati S3 utilizzando le credenziali fornite da S3 Access Grants

Dopo aver [ottenuto le credenziali temporanee](#) tramite la concessione di accesso, un assegnatario può utilizzare tali credenziali per chiamare le operazioni API di Amazon S3 per accedere ai tuoi dati.

I beneficiari possono accedere ai dati S3 utilizzando AWS Command Line Interface (AWS CLI), gli SDK e l'API REST di Amazon S3. AWS Inoltre, puoi utilizzare i plugin AWS [Python](#) e [Java](#) per chiamare S3 Access Grants

Utilizzo di AWS CLI

Dopo aver ottenuto le credenziali temporanee da S3 Access Grants, l'assegnatario può configurare un profilo con tali credenziali per richiamare i dati.

Per installarlo AWS CLI, vedere [Installazione di AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Configura un profilo

```
aws configure set aws_access_key_id "$accessKey" --profile access-grants-consumer-access-profile
aws configure set aws_secret_access_key "$secretKey" --profile access-grants-consumer-access-profile
aws configure set aws_session_token "$sessionToken" --profile access-grants-consumer-access-profile
```

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Ottieni i dati S3

Il beneficiario può utilizzare il [get-object](#) AWS CLI comando per accedere ai dati. Il beneficiario può anche utilizzare [put-object ls](#), e altri comandi S3. AWS CLI

```
aws s3api get-object \
--bucket amzn-s3-demo-bucket1 \
--key myprefix \
--region us-east-2 \
--profile access-grants-consumer-access-profile
```

Utilizzo di AWS SDK

Questa sezione fornisce esempi di come gli assegnatari possono accedere ai dati S3 utilizzando gli AWS SDK.

Java

Il seguente esempio di codice Java recupera un oggetto da un bucket S3. Per istruzioni su come creare e testare un campione funzionante, consulta [Nozioni di base](#) nella Guida per gli sviluppatori di AWS SDK per Java .

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GetObjectRequest;
import com.amazonaws.services.s3.model.ResponseHeaderOverrides;
import com.amazonaws.services.s3.model.S3Object;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;

public class GetObject2 {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "**** Bucket name ****";
        String key = "**** Object key ****";

        S3Object fullObject = null, objectPortion = null, headerOverrideObject =
null;
        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .withRegion(clientRegion)
                .withCredentials(new ProfileCredentialsProvider())
                .build();

            // Get an object and print its contents.
            System.out.println("Downloading an object");
            fullObject = s3Client.getObject(new GetObjectRequest(bucketName, key));
            System.out.println("Content-Type: " +
fullObject.getObjectMetadata().getContentType());
            System.out.println("Content: ");
```

```

        displayTextInputStream(fullObject.getObjectContent());

        // Get a range of bytes from an object and print the bytes.
        GetObjectRequest rangeObjectRequest = new GetObjectRequest(bucketName,
key)
            .withRange(0, 9);
        objectPortion = s3Client.getObject(rangeObjectRequest);
        System.out.println("Printing bytes retrieved.");
        displayTextInputStream(objectPortion.getObjectContent());

        // Get an entire object, overriding the specified response headers, and
print
        // the object's content.
        ResponseHeaderOverrides headerOverrides = new ResponseHeaderOverrides()
            .withCacheControl("No-cache")
            .withContentDisposition("attachment; filename=example.txt");
        GetObjectRequest getObjectRequestHeaderOverride = new
GetObjectRequest(bucketName, key)
            .withResponseHeaders(headerOverrides);
        headerOverrideObject =
s3Client.getObject(getObjectRequestHeaderOverride);
        displayTextInputStream(headerOverrideObject.getObjectContent());
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    } finally {
        // To ensure that the network connection doesn't remain open, close any
open
        // input streams.
        if (fullObject != null) {
            fullObject.close();
        }
        if (objectPortion != null) {
            objectPortion.close();
        }
        if (headerOverrideObject != null) {
            headerOverrideObject.close();
        }
    }
}

```

```
    }

    private static void displayTextInputStream(InputStream input) throws IOException
    {
        // Read the text input stream one line at a time and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line = null;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}
```

Azioni S3 supportate in S3 Access Grants

Un beneficiario può utilizzare la credenziale temporanea fornita da S3 Access Grants per eseguire azioni S3 sui dati S3 a cui ha accesso. Di seguito è riportato un elenco di azioni S3 consentite che un beneficiario può eseguire. Le azioni consentite dipendono dal livello di autorizzazione concesso nella concessione di accesso, READ, WRITE, o READWRITE.

 **Note**

Oltre alle autorizzazioni Amazon S3 elencate di seguito, Amazon S3 può chiamare l'autorizzazione AWS Key Management Service (AWS KMS) [Decrypt \(\) o l'autorizzazione \(kms:decrypt\)](#). READ AWS KMS [GenerateDataKey](#) kms:generateDataKey WRITE Queste autorizzazioni non consentono l'accesso diretto alla chiave. AWS KMS

Azione S3 IAM	Azione e documento API	Autorizzazione S3 Access Grants	Risorsa S3			
s3:GetObject	GetObject	READ	Oggetto			

Azione S3 IAM	Azione e documento API	Autorizzazione S3 Access Grants	Risorsa S3			
s3:GetObjectVersion	GetObject	READ	Oggetto			
s3:GetObjectAcl	GetObjectAcl	READ	Oggetto			
s3:GetObjectVersionAcl	GetObjectAcl	READ	Oggetto			
s3:ListMultipartUploads	ListParts	READ	Oggetto			
s3:PutObject	PutObject , CreateMultipartUpload , UploadPart , UploadPartCopy , CompleteMultipartUpload	WRITE	Oggetto			
s3:PutObjectAcl	PutObjectAcl	WRITE	Oggetto			
s3:PutObjectVersionAcl	PutObjectAcl	WRITE	Oggetto			
s3:DeleteObject	DeleteObject	WRITE	Oggetto			

Azione S3 IAM	Azione e documento API	Autorizzazione S3 Access Grants	Risorsa S3			
s3:DeleteObjectVersion	DeleteObject	WRITE	Oggetto			
s3:AbortMultipartUpload	AbortMultipartUpload	WRITE	Oggetto			
s3:ListBucket	HeadBucket , ListObjects V2, ListObjects	READ	Bucket			
s3:ListBucketVersions	ListObjectVersions	READ	Bucket			
s3:ListBucketMultipartUploads	ListMultipartUploads	READ	Bucket			

Elenco dei permessi di accesso del chiamante

I proprietari dei dati S3 possono utilizzare S3 Access Grants per creare autorizzazioni di accesso per le identità AWS Identity and Access Management (IAM) o per le identità delle directory aziendali. Centro identità AWS IAM Le identità IAM e le identità della directory del Centro identità IAM possono a loro volta utilizzare l'API `ListCallerAccessGrants` per elencare tutti i bucket Amazon S3, i prefissi e gli oggetti a cui possono accedere, come definito dai rispettivi S3 Access Grants. Utilizza questa API per scoprire tutti i dati S3 a cui un'identità IAM o di directory può accedere tramite S3 Access Grants.

È possibile utilizzare questa funzionalità per creare applicazioni che mostrano i dati accessibili a utenti finali specifici. Ad esempio, AWS Storage Browser for S3, un componente dell'interfaccia utente open source utilizzato dai clienti per accedere ai bucket S3, utilizza questa funzionalità per

presentare agli utenti finali i dati a cui hanno accesso in Amazon S3, in base alle concessioni di accesso S3. Un altro esempio è la creazione di un'applicazione per la navigazione, il caricamento o il download di dati in Amazon S3: è possibile utilizzare questa funzione per costruire una struttura ad albero nell'applicazione che l'utente finale può poi sfogliare.

Note

Per le identità delle directory aziendali, quando si elencano le concessioni di accesso del chiamante, S3 Access Grants restituisce le concessioni dell'identità IAM utilizzata per la sessione con riconoscimento dell'identità. Per ulteriori informazioni sulle sessioni con riconoscimento dell'identità, consulta [Concessione delle autorizzazioni per l'utilizzo di sessioni di console con riconoscimento dell'identità](#) nella Guida per l'utente di AWS Identity and Access Management .

Il beneficiario, che si tratti di un'identità IAM o di una directory aziendale, può ottenere un elenco delle proprie autorizzazioni di accesso utilizzando AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e AWS gli SDK.

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di nella Guida per l'utente AWS CLI](#). AWS Command Line Interface

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example Elenca i permessi di accesso di un chiamante

Richiesta:

```
aws s3control list-caller-access-grants \  
--account-id 111122223333 \  
--region us-east-2 \  
--max-results 5
```

Risposta:

```
{
```

```

"NextToken": "6J9S...",
"CallerAccessGrantsList": [
  {
    "Permission": "READWRITE",
    "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix1/*",
    "ApplicationArn": "NA"
  },
  {
    "Permission": "READWRITE",
    "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix2/*",
    "ApplicationArn": "ALL"
  },
  {
    "Permission": "READWRITE",
    "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix3/*",
    "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
  }
]
}

```

Example Elenca i permessi di accesso di un chiamante per un bucket

È possibile restringere l'ambito dei risultati utilizzando il parametro `grantscope`.

Richiesta:

```

aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--grant-scope "s3://amzn-s3-demo-bucket*"
--max-results 1000

```

Risposta:

```

{
  "NextToken": "6J9S...",
  "CallerAccessGrantsList": [
    {
      "Permission": "READ",
      "GrantScope": "s3://amzn-s3-demo-bucket*",

```

```
"ApplicationArn": "ALL"
},
{
  "Permission": "READ",
  "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/*",
  "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
}
]
}
```

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per ottenere un elenco delle autorizzazioni di accesso del chiamante dell'API, consulta [ListCallerAccessGrants](#) Amazon Simple Storage Service API Reference.

Utilizzo di AWS SDK

Questa sezione fornisce un esempio di come i beneficiari richiedono credenziali temporanee da S3 Access Grants utilizzando gli SDK. AWS

Java

Il seguente esempio di codice restituisce le concessioni di accesso del chiamante dell'API ai dati S3 di un particolare Account AWS. Per utilizzare questo esempio di codice, sostituisci *user input placeholders* con le tue informazioni.

Example Elenca i permessi di accesso di un chiamante

Richiesta:

```
Public void ListCallerAccessGrants() {
  ListCallerAccessGrantsRequest listRequest = ListCallerAccessGrantsRequest.builder()
    .withMaxResults(1000)
    .withGrantScope("s3://")
    .accountId("111122223333");
  ListCallerAccessGrantsResponse listResponse =
    s3control.listCallerAccessGrants(listRequest);
  LOGGER.info("ListCallerAccessGrantsResponse: " + listResponse);
}
```

Risposta:

```
ListCallerAccessGrantsResponse(  
  CallerAccessGrantsList=[  
    ListCallerAccessGrantsEntry(  
      S3Prefix=s3://amzn-s3-demo-bucket/prefix1/,  
      Permission=READ,  
      ApplicationArn=ALL  
    )  
  ]  
)
```

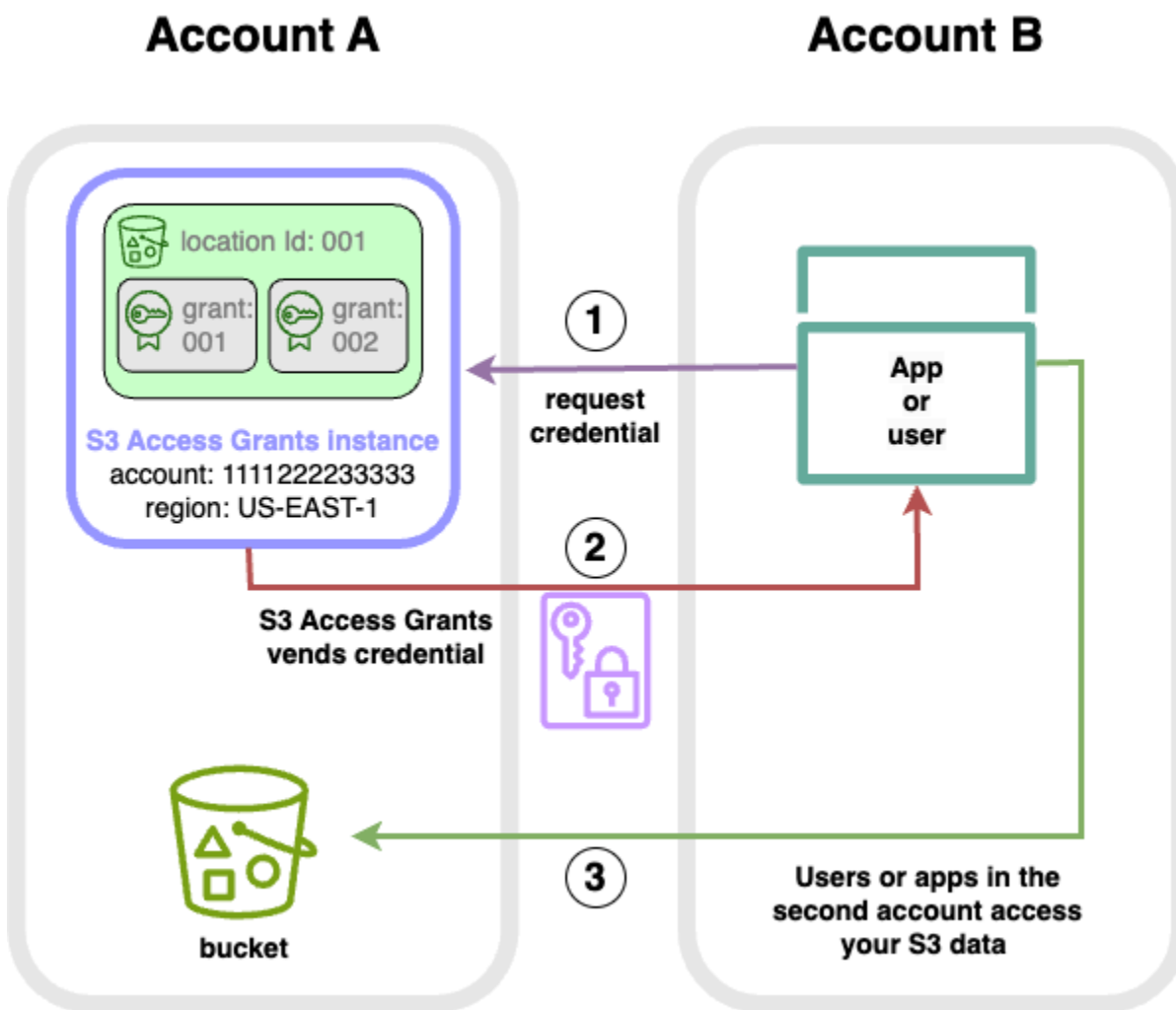
Accesso multi-account S3 Access Grants

Con S3 Access Grants, è possibile concedere l'accesso ai dati di Amazon S3 a quanto segue:

- AWS Identity and Access Management identità (IAM) all'interno del tuo account
- Identità IAM in altri account AWS
- Elenco di utenti o gruppi nella tua istanza Centro identità AWS IAM

Innanzitutto, configurare l'accesso multi-account per l'altro account. Ciò include la concessione dell'accesso all'istanza S3 Access Grants utilizzando una policy di risorse. Quindi, concedere l'accesso ai dati S3 (bucket, prefissi o oggetti) utilizzando le concessioni.

Dopo aver configurato l'accesso multi-account, l'altro account può richiedere credenziali di accesso temporanee ai dati Amazon S3 da S3 Access Grants. L'immagine seguente mostra il flusso di utenti per l'accesso S3 multi-account tramite S3 Access Grants:



1. Gli utenti o le applicazioni di un secondo account (B) richiedono le credenziali all'istanza S3 Access Grants del tuo account (A), dove sono memorizzati i dati Amazon S3. Per ulteriori informazioni, consulta [Richiedi l'accesso ai dati di Amazon S3 tramite S3 Access Grants](#).
2. L'istanza S3 Access Grants dell'account (A) restituisce le credenziali temporanee se esiste una concessione che dà al secondo account l'accesso ai dati Amazon S3. Per ulteriori informazioni sulle concessioni di accesso, consulta [Operazioni con le concessioni in S3 Access Grants](#).
3. Gli utenti o le applicazioni del secondo account (B) utilizzano le Grants-vended credenziali S3 Access per accedere ai dati S3 nel tuo account (A).

Configurazione dell'accesso multi-account a S3 Access Grants

Per concedere l'accesso S3 multi-account tramite S3 Access Grants, procedere come segue:

- Fase 1: Configurare un'istanza S3 Access Grants nel proprio account, ad esempio l'account ID 111122223333, dove vengono archiviati i dati S3.
- Fase 2: configurare la policy delle risorse per l'istanza S3 Access Grants nell'account 111122223333 per consentire l'accesso al secondo account, ad esempio l'ID account 444455556666.
- Fase 3: Configurare le autorizzazioni IAM per il Principale IAM nel secondo account 444455556666 per richiedere le credenziali dall'istanza S3 Access Grants nell'account 111122223333.
- Fase 4: creare una concessione nell'account 111122223333 che dia al principale IAM del secondo account 444455556666 l'accesso ad alcuni dei dati S3 dell'account 111122223333.

Fase 1: Configurare un'istanza S3 Access Grants nel proprio account

Innanzitutto, è necessario disporre di un'istanza S3 Access Grants nel proprio account 111122223333 per gestire l'accesso ai dati Amazon S3. È necessario creare un'istanza di S3 Access Grants in ciascuna Regione AWS in cui sono memorizzati i dati S3 che si desidera condividere. Se condividi i dati in più di una Regione AWS, ripeti ciascuno di questi passaggi di configurazione per ciascuno. Regione AWS Se disponi già di un'istanza S3 Access Grants in Regione AWS cui sono archiviati i dati S3, procedi al passaggio successivo. Se non è stata configurata un'istanza S3 Access Grants, consulta [Operazioni con le istanze S3 Access Grants](#) per completare questo passaggio.

Fase 2: Configurare la policy delle risorse per l'istanza S3 Access Grants in modo da concedere l'accesso multi-account

Dopo aver creato un'istanza S3 Access Grants nell'account 111122223333 per l'accesso multi-account, configurare la policy basata sulle risorse per l'istanza S3 Access Grants nell'account 111122223333 per concedere l'accesso multi-account. L'istanza S3 Access Grants supporta da sola le policy basate sulle risorse. Con la corretta policy basata sulle risorse, puoi concedere l'accesso a utenti o ruoli AWS Identity and Access Management (IAM) di altri utenti Account AWS alla tua istanza S3 Access Grants. Cross-account l'accesso concede solo queste autorizzazioni (azioni):

- `s3:GetAccessGrantsInstanceForPrefix` - l'utente, il ruolo o l'applicazione possono recuperare l'istanza S3 Access Grants che contiene un particolare prefisso.
- `s3:ListAccessGrants`
- `s3:ListAccessLocations`

- `s3:ListCallerAccessGrants`
- `s3:GetDataAccess` - l'utente, il ruolo o l'applicazione possono richiedere credenziali temporanee in base all'accesso concesso tramite S3 Access Grants. Usa queste credenziali per accedere ai dati S3 a cui ti è stato concesso l'accesso.

Puoi scegliere quali di queste autorizzazioni includere nella policy della risorsa. Questa policy di risorse sull'istanza S3 Access Grants è una normale policy basata sulle risorse e supporta tutto ciò che il [linguaggio delle policy IAM](#) supporta. Nella stessa policy, è possibile concedere l'accesso a identità IAM specifiche nell'account 111122223333, ad esempio, utilizzando la condizione `aws:PrincipalArn`, ma non è necessario farlo con S3 Access Grants. Invece, all'interno dell'istanza S3 Access Grants, è possibile creare concessioni per le singole identità IAM del proprio account e per l'altro account. Gestendo ogni concessione di accesso tramite S3 Access Grants, è possibile scalare le autorizzazioni.

Se si utilizza già [AWS Resource Access Manager](#) (AWS RAM), è possibile utilizzarlo per condividere le risorse `s3:AccessGrants` con altri account o all'interno dell'organizzazione. Per ulteriori informazioni, consulta [Lavorare con AWS risorse](#) condivise. Se non lo usi AWS RAM, puoi anche aggiungere la policy sulle risorse utilizzando le operazioni API S3 Access Grants o AWS Command Line Interface (AWS CLI).

Utilizzo della console S3

Ti consigliamo di utilizzare la AWS Resource Access Manager (AWS RAM) Console per condividere `s3:AccessGrants` le tue risorse con altri account o all'interno della tua organizzazione. Per condividere S3 Access Grants multi-account, procedi come segue:

Per configurare la policy delle risorse dell'istanza S3 Access Grants:

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Seleziona il Regione AWS dal Regione AWS selettore.
3. Dal riquadro di navigazione a sinistra, seleziona concessioni di accesso.
4. Nella pagina dell'istanza Access Grants, nella sezione Istanza in questo account, seleziona Condividi istanza. Questo ti reindirizzerà alla Console. AWS RAM
5. Seleziona Crea condivisione risorse.
6. Segui i AWS RAM passaggi per creare la condivisione delle risorse. Per ulteriori informazioni, consulta [Creazione di una condivisione di risorse in AWS RAM](#).

Utilizzo di AWS CLI

Per installarlo AWS CLI, vedere [Installazione di AWS CLI](#) nella Guida AWS Command Line Interface per l'utente.

È possibile aggiungere la policy delle risorse utilizzando il comando CLI `put-access-grants-instance-resource-policy`.

Se si vuole concedere l'accesso multi-account per l'istanza S3 Access Grants nell'account 111122223333 al secondo account 444455556666, la policy delle risorse per l'istanza S3 Access Grants nell'account 111122223333 deve dare al secondo account 444455556666 il permesso di eseguire le seguenti azioni:

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

Nella policy delle risorse dell'istanza S3 Access Grants, specificare l'ARN dell'istanza S3 Access Grants come `Resource`, e il secondo account 444455556666 come `Principal`. Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "444455556666"
      },
      "Action": [
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsLocations",
        "s3:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
  ]
}
```


Per aggiungere o aggiornare la policy delle risorse dell'istanza S3 Access Grants, utilizzare il comando seguente. Quando si utilizza il seguente esempio di comando, sostituisci *user input placeholders* con le tue informazioni.

Example Aggiungere o aggiornare la policy delle risorse dell'istanza S3 Access Grants

```
aws s3control put-access-grants-instance-resource-policy \
--account-id 111122223333 \
--policy file://resourcePolicy.json \
--region us-east-2
{
  "Policy": "{\n
    \"Version\": \"2012-10-17\",\n
    \"Statement\": [{\n
      \"Effect\": \"Allow\",\n
      \"Principal\": {\n
        \"AWS\": \"444455556666\"\n
      },\n
      \"Action\": [\n
        \"s3:ListAccessGrants\",\n
        \"s3:ListAccessGrantsLocations\",\n
        \"s3:GetDataAccess\",\n
        \"s3:GetAccessGrantsInstanceForPrefix\",\n
        \"s3:ListCallerAccessGrants\"\n
      ],\n
      \"Resource\": \"arn:aws:s3:us-east-2:111122223333:access-grants/default\"\n
    }]\n
  },\n
  \"CreatedAt\": \"2023-06-16T00:07:47.473000+00:00\"\n
}
```

Example Ottenere una policy per le risorse S3 Access Grants

È inoltre possibile utilizzare la CLI per ottenere o eliminare una policy di risorse per un'istanza S3 Access Grants.

Per ottenere una policy di risorse S3 Access Grants, utilizzare il seguente comando di esempio. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control get-access-grants-instance-resource-policy \
```

```
--account-id 111122223333 \  
--region us-east-2  
  
{  
  "Policy": "{\n\"Version\": \"2012-10-17\", \"Statement\": [\n{\n\"Effect\": \"Allow\", \"Principal\": {\n\"AWS\": {\n\"arn:aws:iam::111122223333:root\"}\n}, \"Action\": [\n\"s3:ListAccessGrants\", \"s3:ListAccessGrantsLocations\", \"s3:GetDataAccess\", \"s3:GetAccessGrantsInstanceForPrefix\", \"s3:ListCallerAccessGrants\"], \"Resource\": \"arn:aws:s3:us-east-2:111122223333:access-grants/default\"}]}\n\",  
  \"CreatedAt\": \"2023-06-16T00:07:47.473000+00:00\"  
}
```

Example Eliminare una policy di risorse S3 Access Grants

Per eliminare una policy di risorse S3 Access Grants, utilizzare il seguente esempio di comando. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control delete-access-grants-instance-resource-policy \  
--account-id 111122223333 \  
--region us-east-2  
  
// No response body
```

Utilizzo della REST API

È possibile aggiungere la politica delle risorse utilizzando l'[PutAccessGrantsInstanceResourcePolicy API](#).

Se si vuole concedere l'accesso multi-account per l'istanza S3 Access Grants nell'account 111122223333 al secondo account 444455556666, la policy delle risorse per l'istanza S3 Access Grants nell'account 111122223333 deve dare al secondo account 444455556666 il permesso di eseguire le seguenti azioni:

- s3:ListAccessGrants
- s3:ListAccessGrantsLocations
- s3:GetDataAccess
- s3:GetAccessGrantsInstanceForPrefix

Nella policy delle risorse dell'istanza S3 Access Grants, specificare l'ARN dell'istanza S3 Access Grants come Resource, e il secondo account 444455556666 come Principal. Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "444455556666"
      },
      "Action": [
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsLocations",
        "s3:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
  ]
}
```

È quindi possibile utilizzare l'[PutAccessGrantsInstanceResourcePolicy API](#) per configurare la policy.

Per informazioni sul supporto della REST API per aggiornare, ottenere o eliminare una policy di risorse per un'istanza S3 Access Grants, consulta le seguenti sezioni della guida di riferimento API di Amazon Simple Storage Service:

- [PutAccessGrantsInstanceResourcePolicy](#)
- [GetAccessGrantsInstanceResourcePolicy](#)
- [DeleteAccessGrantsInstanceResourcePolicy](#)

Utilizzo di AWS SDK

Questa sezione fornisce gli esempi dell' AWS SDK su come configurare la politica delle risorse di S3 Access Grants per concedere a un secondo AWS account l'accesso ad alcuni dei tuoi dati S3.

Java

Aggiungi, aggiorna, ottieni o elimina una policy della risorsa per gestire l'accesso multi-account alla tua istanza S3 Access Grants.

Example Aggiungere o aggiornare una policy per le risorse dell'istanza S3 Access Grants

Se si vuole concedere l'accesso multi-account per l'istanza S3 Access Grants nell'account 111122223333 al secondo account 444455556666, la policy delle risorse per l'istanza S3 Access Grants nell'account 111122223333 deve dare al secondo account 444455556666 il permesso di eseguire le seguenti azioni:

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

Nella policy delle risorse dell'istanza S3 Access Grants, specificare l'ARN dell'istanza S3 Access Grants come `Resource`, e il secondo account 444455556666 come `Principal`. Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "444455556666"
      },
      "Action": [
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsLocations",
        "s3:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
  ]
}
```

Per aggiungere o aggiornare una policy di risorse dell'istanza S3 Access Grants, utilizzare il seguente esempio di codice:

```
public void putAccessGrantsInstanceResourcePolicy() {
    PutAccessGrantsInstanceResourcePolicyRequest putRequest =
        PutAccessGrantsInstanceResourcePolicyRequest.builder()
```

```
.accountId(111122223333)
.policy(RESOURCE_POLICY)
.build();
PutAccessGrantsInstanceResourcePolicyResponse putResponse =
s3Control.putAccessGrantsInstanceResourcePolicy(putRequest);
LOGGER.info("PutAccessGrantsInstanceResourcePolicyResponse: " + putResponse);
}
```

Risposta:

```
PutAccessGrantsInstanceResourcePolicyResponse(
  Policy={
    "Version": "2012-10-17",
    "Statement": [{
      "Effect": "Allow",
      "Principal": {
        "AWS": "444455556666"
      },
      "Action": [
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsLocations",
        "s3:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:ListCallerAccessGrants"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    ]
  }
)
```

Example Ottenere una policy per le risorse S3 Access Grants

Per ottenere una policy di risorse S3 Access Grants, utilizzare il seguente esempio di codice. Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
public void getAccessGrantsInstanceResourcePolicy() {
  GetAccessGrantsInstanceResourcePolicyRequest getRequest =
  GetAccessGrantsInstanceResourcePolicyRequest.builder()
    .accountId(111122223333)
    .build();
  GetAccessGrantsInstanceResourcePolicyResponse getResponse =
  s3Control.getAccessGrantsInstanceResourcePolicy(getRequest);
}
```

```
LOGGER.info("GetAccessGrantsInstanceResourcePolicyResponse: " + getResponse);
}
```

Risposta:

```
GetAccessGrantsInstanceResourcePolicyResponse(
  Policy={"Version": "2012-10-17",      "Statement":
  [{"Effect":"Allow","Principal":{"AWS":"arn:aws:iam::444455556666:root"},"Action":
  ["s3:ListAccessGrants","s3:ListAccessGrantsLocations","s3:GetDataAccess","s3:GetAccessGrants
east-2:111122223333:access-grants/default"]]}],
  CreatedAt=2023-06-15T22:54:44.319Z
)
```

Example Eliminare una policy di risorse S3 Access Grants

Per eliminare una policy di risorse S3 Access Grants, utilizzare il seguente esempio di codice. Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
public void deleteAccessGrantsInstanceResourcePolicy() {
  DeleteAccessGrantsInstanceResourcePolicyRequest deleteRequest =
  DeleteAccessGrantsInstanceResourcePolicyRequest.builder()
    .accountId(111122223333)
    .build();
  DeleteAccessGrantsInstanceResourcePolicyResponse deleteResponse =
  s3Control.putAccessGrantsInstanceResourcePolicy(deleteRequest);
  LOGGER.info("DeleteAccessGrantsInstanceResourcePolicyResponse: " + deleteResponse);
}
```

Risposta:

```
DeleteAccessGrantsInstanceResourcePolicyResponse()
```

Fase 3: concedere alle identità IAM di un secondo account l'autorizzazione a chiamare l'istanza S3 Access Grants del proprio account

Dopo che il proprietario dei dati di Amazon S3 ha configurato la policy multi-account per l'istanza S3 Access Grants nell'account 111122223333, il proprietario del secondo account 444455556666 deve creare una policy basata sull'identità per i suoi utenti o ruoli IAM e deve concedere loro

l'accesso all'istanza S3 Access Grants. Nella policy basata sull'identità, includere una o più delle seguenti azioni, a seconda di quanto concesso nella policy delle risorse dell'istanza S3 Access Grants e delle autorizzazioni che si desidera concedere:

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`
- `s3:ListCallerAccessGrants`

Seguendo il [modello di accesso multi-account AWS](#), gli utenti o i ruoli IAM del secondo account 444455556666 devono avere esplicitamente una o più di queste autorizzazioni. Ad esempio, concedere l'autorizzazione `s3:GetDataAccess` in modo che l'utente o il ruolo IAM possa chiamare l'istanza S3 Access Grants nell'account 111122223333 per richiedere le credenziali.

Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
  ]
}
```

Per informazioni sulla modifica delle policy IAM basate sull'identità, consulta [Modifica delle policy IAM](#) nella Guida a AWS Identity and Access Management .

Fase 4: creare una concessione nell'istanza S3 Access Grants del proprio account, che dia all'identità IAM del secondo account l'accesso ad alcuni dei dati S3

Per l'ultima fase di configurazione, è possibile creare una concessione nell'istanza S3 Access Grants dell'account 111122223333 che dia accesso all'identità IAM del secondo account 444455556666 ad

alcuni dei dati S3 dell'account. È possibile farlo utilizzando la Console Amazon S3, la CLI, le API e gli SDK. Per ulteriori informazioni, consulta [Creazione di concessioni](#).

Nella concessione, specifica l' AWS ARN dell'identità IAM del secondo account e specifica a quale posizione nei tuoi dati S3 (un bucket, un prefisso o un oggetto) a cui stai concedendo l'accesso. Questa posizione deve essere già registrata con l'istanza S3 Access Grants. Per ulteriori informazioni, consulta [Registrazione di una posizione](#). È possibile specificare facoltativamente un sottoprefisso. Ad esempio, se la posizione a cui si concede l'accesso è un bucket e si vuole limitare ulteriormente l'accesso a un oggetto specifico di quel bucket, si deve passare il nome della chiave dell'oggetto nel campo `S3SubPrefix`. Oppure, se si vuole limitare l'accesso agli oggetti del bucket con nomi di chiavi che iniziano con un prefisso specifico, come `2024-03-research-results/`, trasmetti `S3SubPrefix=2024-03-research-results/`.

Di seguito è riportato un esempio di comando CLI per la creazione di una concessione di accesso per un'identità del secondo account. Per ulteriori informazioni, consulta [Creazione di concessioni](#). Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control create-access-grant \  
--account-id 111122223333 \  
--access-grants-location-id default \  
--access-grants-location-configuration S3SubPrefix=prefixA* \  
--permission READ \  
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::444455556666:role/data-  
consumer-1
```

Dopo aver configurato l'accesso multi-account, l'utente o il ruolo del secondo account può eseguire le seguenti operazioni:

- Chiama `ListAccessGrantsInstances` per elencare le istanze S3 Access Grants condivise con esso attraverso AWS RAM. Per ulteriori informazioni, consulta [Ottenimento dei dettagli di un'istanza S3 Access Grants](#).
- Richiede credenziali temporanee da S3 Access Grants. Per ulteriori informazioni su come effettuare queste richieste, consulta [Richiedi l'accesso ai dati di Amazon S3 tramite S3 Access Grants](#).

Gestione dei tag per S3 Access Grants

I tag in Amazon S3 Access Grants hanno caratteristiche simili ai [tag degli oggetti](#) in Amazon S3. Ogni tag è una coppia chiave-valore. Le risorse in S3 Access Grants alle quali puoi aggiungere tag sono [istanze](#), [posizioni](#) e [concessioni](#) di S3 Access Grants.

Note

L'assegnazione di tag in S3 Access Grants utilizza operazioni API diverse rispetto all'assegnazione di tag agli oggetti. S3 Access Grants utilizza le operazioni API [TagResource](#), [UntagResource](#) e [ListTagsForResource](#) in cui una risorsa può essere una posizione registrata, una concessione di accesso o un'istanza S3 Access Grants.

Analogamente ai [tag degli oggetti](#), si applicano le seguenti limitazioni:

- Puoi aggiungere tag alle nuove risorse S3 Access Grants al momento della loro creazione oppure puoi aggiungere tag alle risorse esistenti.
- Puoi associare fino a un massimo di 10 tag a ciascuna risorsa. Se alla stessa risorsa sono associati più tag, questi devono avere chiavi di tag univoche.
- Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori dei tag possono contenere fino a 256 caratteri Unicode. I tag sono rappresentati internamente in UTF-16. In UTF-16, i caratteri occupano 1 o 2 posizioni di caratteri.
- Per chiavi e valori viene fatta distinzione tra maiuscole e minuscole.

Per ulteriori informazioni sulle restrizioni relative ai tag, consulta le restrizioni relative ai [User-defined tag](#) nella Guida AWS Billing per l'utente.

Puoi etichettare le risorse in S3 Access Grants utilizzando AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 o gli SDK. AWS

Utilizzo di AWS CLI

Per installarlo AWS CLI, consulta [Installazione di AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Puoi aggiungere tag a una risorsa S3 Access Grants quando la crei o dopo averla creata. Di seguito sono riportati esempi che mostrano come aggiungere tag a un'istanza S3 Access Grants o rimuoverli da essa. Puoi eseguire operazioni simili per le posizioni registrate e le concessioni di accesso.

Per utilizzare i seguenti comandi di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example– Crea un'istanza S3 Access Grants con tag

```
aws s3control create-access-grants-instance \  
  --account-id 111122223333 \  
  --profile access-grants-profile \  
  --region us-east-2 \  
  --tags Key=tagKey1,Value=tagValue1
```

Risposta:

```
{  
  "CreatedAt": "2023-10-25T01:09:46.719000+00:00",  
  "AccessGrantsInstanceId": "default",  
  "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/  
default"  
}
```

Example– Aggiungi un tag a un'istanza S3 Access Grants già creata

```
aws s3control tag-resource \  
  --account-id 111122223333 \  
  --resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \  
  --profile access-grants-profile \  
  --region us-east-2 \  
  --tags Key=tagKey2,Value=tagValue2
```

Example– Elenca i tag per l'istanza S3 Access Grants

```
aws s3control list-tags-for-resource \  
  --account-id 111122223333 \  
  --resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \  
  --profile access-grants-profile \  
  --region us-east-2
```

Risposta:

```
{
  "Tags": [
    {
      "Key": "tagKey1",
      "Value": "tagValue1"
    },
    {
      "Key": "tagKey2",
      "Value": "tagValue2"
    }
  ]
}
```

Example– Rimuovi tag dall'istanza S3 Access Grants

```
aws s3control untag-resource \
  --account-id 111122223333 \
  --resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
  --profile access-grants-profile \
  --region us-east-2 \
  --tag-keys "tagKey2"
```

Utilizzo della REST API

Puoi utilizzare l'API Amazon S3 per aggiungere o rimuovere i tag oppure per elencare i tag per una posizione registrata, una concessione di accesso o un'istanza S3 Access Grants. Per informazioni sul supporto REST API di Amazon S3 per la gestione dei tag S3 Access Grants, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [TagResource](#)
- [UntagResource](#)
- [ListTagsForResource](#)

Limitazioni di S3 Access Grants

[S3 Access Grants](#) presenta le seguenti limitazioni:

 Note

Se il tuo caso d'uso supera queste limitazioni, [contatta l' AWS assistenza](#) per richiedere limiti più elevati.

Istanza S3 Access Grants

Puoi creare 1 istanza S3 Access Grants per account. Regione AWS Consulta [Creazione di un'istanza S3 Access Grants](#).

Posizione di S3 Access Grants

Puoi registrare 1.000 posizioni S3 Access Grants per istanza S3 Access Grants. Consulta [Operazioni con le posizioni S3 Access Grants](#).

Grant

Puoi creare solo 100.000 concessioni per istanza S3 Access Grants. Consulta [Creazione di una concessione](#).

S3 Access Grants Regioni AWS

S3 Access Grants è attualmente disponibile nei seguenti modi: Regioni AWS

Regione AWS codice	Regione AWS nome
us-east-1	Stati Uniti orientali (Virginia settentrionale)
us-east-2	Stati Uniti orientali (Ohio)
us-west-1	Stati Uniti occidentali (California settentrionale)
us-west-2	Stati Uniti occidentali (Oregon)
af-south-1	Africa (Città del Capo)
ap-east-1	Asia Pacifico (Hong Kong)
ap-east-2	Asia Pacifico (Taipei)

Regione AWS codice	Regione AWS nome
ap-northeast-1	Asia Pacifico (Tokyo)
ap-northeast-2	Asia Pacifico (Seoul)
ap-northeast-3	Asia Pacifico (Osaka)
ap-south-1	Asia Pacifico (Mumbai)
ap-south-2	Asia Pacifico (Hyderabad)
ap-southeast-1	Asia Pacifico (Singapore)
ap-southeast-2	Asia Pacifico (Sydney)
ap-southeast-3	Asia Pacifico (Giacarta)
ap-southeast-4	Asia Pacifico (Melbourne)
ap-southeast-6	Asia Pacifico (Nuova Zelanda)
ap-southeast-7	Asia Pacifico (Thailandia)
ca-central-1	Canada (Centrale)
ca-west-1	Canada occidentale (Calgary)
eu-central-1	Europa (Francoforte)
eu-central-2	Europa (Zurigo)
eu-north-1	Europa (Stoccolma)
eu-south-1	Europa (Milano)
eu-south-2	Europa (Spagna)
eu-west-1	Europa (Irlanda)
eu-west-2	Europa (Londra)

Regione AWS codice	Regione AWS nome
eu-west-3	Europa (Parigi)
eusc-de-east-1	AWS European Sovereign Cloud (Germania)
il-central-1	Israele (Tel Aviv)
me-central-1	Medio Oriente (Emirati Arabi Uniti)
me-south-1	Medio Oriente (Bahrein)
mx-central-1	Messico (centrale)
sa-east-1	Sud America (San Paolo)
us-gov-east-1	AWS GovCloud (US-East)
us-gov-west-1	AWS GovCloud (US-West)

Integrazioni con S3 Access Grants

S3 Access Grants può essere utilizzato con i seguenti AWS servizi e funzionalità. Questa pagina verrà aggiornata non appena saranno disponibili nuove integrazioni.

Tip

Questo [AWS workshop per S3 Access Grants](#) illustra come utilizzare S3 Access Grants con utenti AWS Identity and Access Management (IAM), utenti IAM Identity Center, Amazon EMR e. AWS Transfer Family

Amazon Athena

[Utilizzo di gruppi di processo Athena con Centro identità IAM abilitato](#)

Amazon EMR

[Avvio di un cluster Amazon EMR con S3 Access Grants](#)

Amazon EMR su EKS

[Avvio di un cluster Amazon EMR su EKS con S3 Access Grants](#)

Applicazione Amazon EMR serverless

[Avvio di un'applicazione Amazon EMR serverless con S3 Access Grants](#)

Amazon Redshift

[Integrazione di Amazon Redshift con Amazon S3 Access Grants](#)

Amazon AI Studio SageMaker

[Aggiungere dati Amazon S3 ad Amazon SageMaker AI Unified Studio](#)

Utilizzando S3 Access Grants in Amazon SageMaker AI Unified Studio, puoi condividere i tuoi dati Amazon S3 in più progetti. Per consentire la concessione dell'accesso ai dati tramite S3 Access Grants, è necessaria un'istanza S3 Access Grants. Amazon SageMaker AI Unified Studio utilizzerà un'istanza S3 Access Grants se è già disponibile o può crearne una. Innanzitutto, si aggiungono i dati di Amazon S3 e poi si pubblicano nel catalogo o si condividono direttamente con i consumatori.

[Utilizzo di Amazon S3 Access Grants con Amazon SageMaker AI Studio e il plug-in SDK for Python \(Boto3\)](#)

L'utilizzo di S3 Access Grants nei notebook Amazon SageMaker AI Studio ora è più semplice utilizzando il plug-in SDK for Python (Boto3). Imposta in anticipo le concessioni di accesso per i principali IAM e gli utenti delle directory. Centro identità AWS IAM Sebbene Amazon SageMaker AI Studio non supporti in modo nativo gli utenti delle directory dei provider di identità, puoi scrivere codice Python personalizzato utilizzando il plug-in che consente a queste identità di accedere ai dati S3 tramite S3 Access Grants. L'accesso ai dati avviene con l'aiuto del plugin e non tramite Amazon AI. SageMaker

AWS Glue

[Amazon S3 Access Grants con AWS Glue](#)

Centro identità AWS IAM

[Propagazione delle identità attendibili tra le applicazioni](#)

AWS Transfer Family

[Configura Amazon S3 Access Grants per](#) AWS Transfer Family

Storage Browser per S3

[Gestione dell'accesso ai dati in scala](#) con Storage Browser per S3

Framework Python open source

[Amazon S3 Access Grants ora si integra con i framework Python open source](#)

Gestione degli accessi con le ACL

Le liste di controllo degli accessi (ACL) sono una delle opzioni basate sulle risorse che si possono usare per gestire l'accesso ai bucket e agli oggetti. Puoi utilizzare gli ACL per concedere read/write autorizzazioni di base ad altri. Account AWS Esistono dei limiti alla gestione delle autorizzazioni tramite le ACL.

Ad esempio, puoi concedere autorizzazioni solo ad altri utenti Account AWS; non puoi concedere autorizzazioni agli utenti del tuo account. Non si possono concedere autorizzazioni condizionali e non è possibile rifiutare le autorizzazioni in modo esplicito. Le ACL sono idonee per scenari specifici. Ad esempio, se il proprietario di un bucket consente Account AWS ad altri di caricare oggetti, le autorizzazioni per questi oggetti possono essere gestite utilizzando l'ACL dell'oggetto solo dal proprietario dell' Account AWS oggetto.

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le liste di controllo degli accessi (ACL) sono disabilite. Quando le ACL sono disabilite, il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ad essi in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilite, tranne nelle circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Con le ACL disabilite, puoi utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al

bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Per ulteriori informazioni sugli ACL, consulta i seguenti argomenti:

Argomenti

- [Panoramica delle liste di controllo accessi \(ACL\)](#)
- [Configurazione delle ACL](#)
- [Esempi di policy per le ACL](#)

Panoramica delle liste di controllo accessi (ACL)

Le liste di controllo accessi (ACL) di Amazon S3 permettono di gestire l'accesso ai bucket e agli oggetti. A ogni bucket e oggetto è associata una ACL come sottorisorsa. Definisce a quali Account AWS gruppi è concesso l'accesso e il tipo di accesso. Quando viene ricevuta una richiesta relativa a una risorsa, Amazon S3 controlla la lista ACL corrispondente per verificare che il richiedente disponga delle autorizzazioni di accesso necessarie.

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le liste di controllo degli accessi (ACL) sono disabilite. Quando le ACL sono disabilite, il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ad essi in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilite, tranne nelle circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Con le ACL disabilite, puoi utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

⚠ Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Quando crei un bucket o un oggetto, Amazon S3 crea una lista ACL predefinita che concede al proprietario della risorsa il controllo completo su di essa. Questa situazione è illustrata nella seguente ACL del bucket di esempio (l'oggetto ACL predefinito ha la medesima struttura):

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

L'ACL di esempio include un elemento `Owner` che identifica il proprietario tramite l'ID utente canonico dell' Account AWS. Per istruzioni sulla ricerca dell'ID utente canonico, consulta [Trovare un Account AWS ID utente canonico](#). L'Grantelemento identifica il beneficiario (uno Account AWS o un gruppo predefinito) e l'autorizzazione concessa. Questa ACL predefinita possiede un elemento `Grant` per il proprietario. Per concedere le autorizzazioni aggiungere elementi `Grant`; ognuno di questi elementi identifica l'assegnatario e l'autorizzazione.

 Note

Un ACL può avere fino a 100 di questi elementi.

Argomenti

- [Che cosa si intende per assegnatario?](#)
- [Quali autorizzazioni è possibile concedere?](#)
- [ACL Valori richiesti per le richieste Amazon S3 comuni](#)
- [ACL di esempio](#)
- [ACL predefinita](#)

Che cosa si intende per assegnatario?

Quando si concedono i diritti di accesso, si specifica ogni assegnatario come coppia *type*="value" in cui *type* è uno dei seguenti:

- *id*— Se il valore specificato è l'ID utente canonico di un Account AWS
- *uri*: se si concedono autorizzazioni a un gruppo predefinito

 Warning

Quando concedi ad altri Account AWS l'accesso alle tue risorse, tieni presente che Account AWS possono delegare le proprie autorizzazioni agli utenti con i loro account. Questa operazione è nota con il nome di accesso multiaccount. Per informazioni sull'utilizzo dell'accesso multiaccount, consulta [Creazione di un ruolo per delegare le autorizzazioni a un utente IAM](#) nella Guida per l'utente di IAM.

Trovare un Account AWS ID utente canonico

L'ID utente canonico è associato al tuo Account AWS. Questo ID è una stringa di caratteri lunga, ad esempio:

79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be

Per informazioni su come trovare l'ID utente canonico per l'account, consulta la sezione [Trovare l'ID utente canonico per Account AWS](#) nella Guida di riferimento per la gestione dell'account AWS .

Puoi anche cercare l'ID utente canonico di un Account AWS leggendo l'ACL di un bucket o di un oggetto a cui dispone delle autorizzazioni di accesso. Account AWS Quando a un individuo Account AWS vengono concesse le autorizzazioni tramite una richiesta di concessione, all'ACL viene aggiunta una voce di concessione con l'ID utente canonico dell'account.

Note

Se rendi pubblico il bucket (non consigliato) qualsiasi utente non autenticato può caricare oggetti nel bucket. Questi utenti anonimi non dispongono di un Account AWS. Quando un utente anonimo carica un oggetto nel tuo bucket Amazon S3 aggiunge un ID utente canonico speciale (65a011a29cdf8ec533ec3d1ccaae921c) in quanto proprietario dell'oggetto nell'ACL. Per ulteriori informazioni, consulta [Proprietà di bucket e oggetti di Amazon S3](#).

Gruppi predefiniti di Amazon S3

Amazon S3 include un set di gruppi predefiniti. Quando si concede l'accesso a un gruppo a livello di account, viene specificato uno degli URI Amazon S3 anziché un ID utente canonico. Amazon S3 fornisce i seguenti gruppi predefiniti:

- Gruppo Authenticated Users – Rappresentato da `http://acs.amazonaws.com/groups/global/AuthenticatedUsers`.

Questo gruppo rappresenta tutto. Account AWS L'autorizzazione di accesso a questo gruppo consente Account AWS a chiunque di accedere alla risorsa. Tuttavia, tutte le richieste devono essere firmate (autenticate).

Warning

Quando concedi l'accesso al gruppo Authenticated Users, qualsiasi utente AWS autenticato nel mondo può accedere alla tua risorsa.

- Gruppo All Users – Rappresentato da `http://acs.amazonaws.com/groups/global/AllUsers`.

L'autorizzazione di accesso per questo gruppo consente a qualsiasi persona al mondo di accedere alla risorsa. Le richieste possono essere firmate (autenticate) o non firmate (anonime). Le richieste non firmate mancano dell'intestazione di autenticazione.

 Warning

È vivamente consigliato non concedere mai al gruppo All Users autorizzazioni WRITE, WRITE_ACP o FULL_CONTROL. Ad esempio, sebbene le autorizzazioni WRITE non consentano ai non proprietari di sovrascrivere o eliminare oggetti esistenti, le autorizzazioni WRITE consentono comunque a chiunque di archiviare oggetti nel bucket, i quali vengono fatturati. Per ulteriori dettagli su queste autorizzazioni, consulta la sezione [Quali autorizzazioni è possibile concedere?](#).

- Gruppo Log Delivery – Rappresentato da `http://acs.amazonaws.com/groups/s3/LogDelivery`.

L'autorizzazione WRITE per un bucket consente a questo gruppo di scrivere log di credenziali d'accesso al server (consulta [Registrazione delle richieste con registrazione dell'accesso al server](#)) per il bucket.

 Note

Quando si utilizzano gli ACL, un beneficiario può essere uno Account AWS o uno dei gruppi Amazon S3 predefiniti. Tuttavia, l'assegnatario non può essere un utente IAM. Per ulteriori informazioni sugli utenti AWS e sulle autorizzazioni in IAM, consulta [Utilizzo di AWS Identity and Access Management](#).

Quali autorizzazioni è possibile concedere?

La seguente tabella elenca il set di autorizzazioni che Amazon S3 supporta in una lista ACL. L'insieme di autorizzazioni ACL è lo stesso per le ACL degli oggetti e dei bucket. Tuttavia, a seconda del contesto (bucket ACL o oggetto ACL), queste autorizzazioni si riferiscono a specifiche operazioni sui bucket o sugli oggetti. La tabella elenca le autorizzazioni e ne descrive il significato nel contesto degli oggetti e dei bucket.

Per ulteriori informazioni sulle autorizzazioni ACL nella console di Amazon S3, consulta [Configurazione delle ACL](#).

Autorizzazione	Concessione a livello di bucket	Concessione a livello di oggetto
READ	Consente all'assegnatario di elencare gli oggetti del bucket	Consente all'assegnatario di leggere i dati dell'oggetto e i relativi metadata
WRITE	Consente all'assegnatario di creare nuovi oggetti del bucket. Per i proprietari di bucket e oggetti di oggetti esistenti, consente anche di eliminare e sovrascrivere tali oggetti.	Non applicabile.
READ_ACP	Consente all'assegnatario di leggere l'ACL del bucket	Consente all'assegnatario di leggere l'ACL dell'oggetto
WRITE_ACP	Consente all'assegnatario di scrivere l'ACL del bucket interessato	Consente all'assegnatario di scrivere l'ACL dell'oggetto interessato
FULL_CONTROL	Consente al beneficiario le autorizzazioni READ, WRITE, READ_ACP e WRITE_A sul bucket	Consente al beneficiario le autorizzazioni READ, READ_ACP e WRITE_ACP sull'oggetto

Warning

Prestare attenzione a concedere le autorizzazioni di accesso ai bucket e agli oggetti S3. Ad esempio, la concessione dell'accesso WRITE a un bucket consente all'assegnatario di creare oggetti nel bucket. È vivamente consigliato di leggere tutta questa sezione [Panoramica delle liste di controllo accessi \(ACL\)](#) prima di concedere autorizzazioni.

Mappatura delle autorizzazioni ACL e delle autorizzazioni della policy di accesso

Come illustrato nella tabella precedente, un'ACL concede solo un insieme finito di autorizzazioni rispetto al numero di autorizzazioni che possono essere definite in una policy d'accesso predefinita

(consulta [Azioni di policy per Amazon S3](#)). Ognuna di queste autorizzazioni permette di eseguire una o più operazioni di Amazon S3.

La seguente tabella mostra come ogni autorizzazione ACL è mappata sulle autorizzazioni corrispondenti della policy d'accesso predefinita. Come si può vedere, la policy di accesso predefinita concede un numero maggiore di autorizzazioni rispetto all'ACL. Gli ACL vengono utilizzati principalmente per concedere autorizzazioni di base, analogamente alle read/write autorizzazioni del file system. Per ulteriori informazioni su quando utilizzare una lista ACL, consulta [Identity and Access Management per Amazon S3](#).

Per ulteriori informazioni sulle autorizzazioni ACL nella console di Amazon S3, consulta [Configurazione delle ACL](#).

Autorizzazione ACL	Autorizzazioni corrispondenti della policy d'accesso predefinita quando l'autorizzazione ACL viene concessa su un bucket	Autorizzazioni corrispondenti della policy d'accesso predefinita quando l'autorizzazione ACL viene concessa su un oggetto
READ	<code>s3:ListBucket</code> , <code>s3:ListBucketVersions</code> e <code>s3:ListBucketMultipartUploads</code>	<code>s3:GetObject</code> e <code>s3:GetObjectVersion</code>
WRITE	<p><code>s3:PutObject</code></p> <p>Il proprietario del bucket può creare, sovrascrivere ed eliminare qualsiasi oggetto nel bucket e il proprietario dell'oggetto ha FULL_CONTROL sull'oggetto.</p> <p>Inoltre, quando l'assegnatario è il proprietario del bucket, la concessione dell'autorizzazione WRITE nell'ACL di un bucket consente l'esecuzione dell'operazione <code>s3:DeleteObjectVersion</code> su qualsiasi versione del bucket.</p>	Non applicabile.

Autorizzazione ACL	Autorizzazioni corrispondenti della policy d'accesso predefinita quando l'autorizzazione ACL viene concessa su un bucket	Autorizzazioni corrispondenti della policy d'accesso predefinita quando l'autorizzazione ACL viene concessa su un oggetto
READ_ACP	s3:GetBucketAc1	s3:GetObjectAc1 e s3:GetObjectVersionAc1
WRITE_ACP	s3:PutBucketAc1	s3:PutObjectAc1 e s3:PutObjectVersionAc1
FULL_CONTROL	Equivale alla concessione delle autorizzazioni ACL READ, WRITE, READ_ACP e WRITE_ACP . Di conseguenza, questa autorizzazione ACL è mappata su una combinazione delle autorizzazioni corrispondenti della policy d'accesso predefinita.	Equivale alla concessione delle autorizzazioni ACL READ, READ_ACP e WRITE_ACP . Di conseguenza, questa autorizzazione ACL è mappata su una combinazione delle autorizzazioni corrispondenti della policy d'accesso predefinita.

Chiavi di condizione

Quando si concedono autorizzazioni per le policy di accesso, è possibile utilizzare le chiavi di condizione per limitare il valore dell'ACL su un oggetto utilizzando una policy del bucket. Le chiavi di contesto riportate di seguito corrispondono alle ACL. È possibile utilizzare queste chiavi di contesto per richiedere l'utilizzo di un'ACL specifica in una richiesta:

- s3:x-amz-grant-read – Richiedere l'accesso in lettura.
- s3:x-amz-grant-write – Richiedere l'accesso in scrittura.
- s3:x-amz-grant-read-acp – Richiedere l'accesso in lettura alla lista ACL del bucket.
- s3:x-amz-grant-write-acp – Richiedere l'accesso in scrittura alla lista ACL del bucket.
- s3:x-amz-grant-full-control – Richiedere il controllo completo.
- s3:x-amz-acl – Richiedere una lista [ACL predefinita](#).

Ad esempio, politiche che coinvolgono le ACL-specific intestazioni, vedere [Concessione di s3:PutObject autorizzazione con una condizione che richiede al proprietario del bucket di ottenere il pieno controllo](#). Per un elenco completo delle chiavi di condizione specifiche per Amazon S3,

consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) nella Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

ACL Valori richiesti per le richieste Amazon S3 comuni

Per identificare le richieste Amazon S3 che richiedono le ACL per l'autorizzazione, puoi utilizzare il valore `aclRequired` nei log degli accessi del server Amazon S3 oppure AWS CloudTrail. Il `aclRequired` valore visualizzato nei CloudTrail log di accesso al server Amazon S3 dipende dalle operazioni richiamate e da determinate informazioni sul richiedente, sul proprietario dell'oggetto e sul proprietario del bucket. Se non sono richiesti ACL, o se stai impostando l'ACL predefinito o `bucket-owner-full-control` se le richieste sono consentite dalla tua policy del bucket, la stringa del `aclRequired` valore è "-" nei log di accesso al server Amazon S3 ed è assente in CloudTrail.

Le tabelle seguenti elencano `aclRequired` i valori previsti nei CloudTrail log di accesso al server Amazon S3 per le varie operazioni dell'API Amazon S3. Puoi utilizzare queste informazioni per capire quali operazioni di Amazon S3 dipendono dagli ACL per l'autorizzazione. Nelle tabelle seguenti, A, B e C rappresentano i diversi account associati al richiedente, al proprietario dell'oggetto e al proprietario del bucket. Le voci con un asterisco (*) indicano uno degli account A, B o C.

Note

Le operazioni `PutObject` nella tabella seguente, se non diversamente specificato, indicano richieste che non impostano un'ACL, a meno che l'ACL non sia un'ACL `bucket-owner-full-control`. Un valore nullo per `aclRequired` indica che `aclRequired` è assente nei log. AWS CloudTrail

La tabella seguente mostra i `aclRequired` valori per CloudTrail

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
GetObject	A	A	A	Sì o No	null	Same-account accesso
GetObject	A	B	A	Sì o No	null	Same-account accesso con proprietario del bucket imposto
GetObject	A	A	B	Sì	null	Cross-account accesso concesso dalla politica del bucket
GetObject	A	A	B	No	Sì	Cross-account l'accesso si basa su ACL
GetObject	A	A	B	Sì	null	Cross-account accesso concesso dalla

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
						bucket policy
GetObject	A	B	B	No	Sì	Cross-account l'accesso si basa su ACL
GetObject	A	B	C	Sì	null	Cross-account accesso concesso dalla bucket policy
GetObject	A	B	C	No	Sì	Cross-account l'accesso si basa su ACL
PutObject	A	Non applicabile	A	Sì o No	null	Same-account accesso

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
PutObject	A	Non applicabile	B	Sì	null	Cross-account accesso concesso dalla bucket policy
PutObject	A	Non applicabile	B	No	Sì	Cross-account l'accesso si basa su ACL
PutObject con un ACL (ad eccezione di bucket-owner-full-control)	*	Non applicabile	*	Sì o No	Sì	Richiesta di autorizzazioni ACL
ListObjects	A	Non applicabile	A	Sì o No	null	Same-account accesso

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
ListObjects	A	Non applicabile	B	Sì	null	Cross-account accesso concesso dalla bucket policy
ListObjects	A	Non applicabile	B	No	Sì	Cross-account l'accesso si basa su ACL
DeleteObject	A	Non applicabile	A	Sì o No	null	Same-account accesso
DeleteObject	A	Non applicabile	B	Sì	null	Cross-account accesso concesso dalla bucket policy
DeleteObject	A	Non applicabile	B	No	Sì	Cross-account l'accesso si basa su ACL

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
PutObject Acl	*	*	*	Sì o No	Sì	Richiesta di autorizzazioni ACL
PutBucket Acl	*	Non applicabile	*	Sì o No	Sì	Richiesta di autorizzazioni ACL

Note

Le operazioni REST.PUT.OBJECT nella tabella seguente, se non diversamente specificato, indicano richieste che non impostano un ACL, a meno che l'ACL non sia un bucket-owner-full-control ACL. Una stringa di valori aclRequired di "-" indica un valore nullo nei log di accesso al server Amazon S3.

La tabella seguente mostra i valori di aclRequired per i log di accesso al server Amazon S3.

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
REST.GET.OBJECT	A	A	A	Sì o No	-	Same-account accesso
REST.GET.OBJECT	A	B	A	Sì o No	-	Same-account accesso con

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
						proprietario del bucket imposto
REST.GET.OBJECT	A	A	B	Sì	-	Cross-account accesso concesso dalla politica del bucket
REST.GET.OBJECT	A	A	B	No	Sì	Cross-account l'accesso si basa su ACL
REST.GET.OBJECT	A	B	B	Sì	-	Cross-account accesso concesso dalla bucket policy
REST.GET.OBJECT	A	B	B	No	Sì	Cross-account l'accesso si basa su ACL

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
REST.GET.OBJECT	A	B	C	Sì	-	Cross-account accesso concesso dalla bucket policy
REST.GET.OBJECT	A	B	C	No	Sì	Cross-account l'accesso si basa su ACL
REST.PUT.OBJECT	A	Non applicabile	A	Sì o No	-	Same-account accesso
REST.PUT.OBJECT	A	Non applicabile	B	Sì	-	Cross-account accesso concesso dalla bucket policy
REST.PUT.OBJECT	A	Non applicabile	B	No	Sì	Cross-account l'accesso si basa su ACL

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
REST.PUT.OBJECT con un ACL (ad eccezione di bucket-owner-full-control)	*	Non applicabile	*	Sì o No	Sì	Richiesta di autorizzazioni ACL
REST.GET.BUCKET	A	Non applicabile	A	Sì o No	-	Same-account accesso
REST.GET.BUCKET	A	Non applicabile	B	Sì	-	Cross-account accesso concesso dalla bucket policy
REST.GET.BUCKET	A	Non applicabile	B	No	Sì	Cross-account l'accesso si basa su ACL
REST.DELETE.OBJECT	A	Non applicabile	A	Sì o No	-	Same-account accesso

Nome operazione	Richiedente	Proprietario dell'oggetto.	Proprietario del bucket	La policy di bucket garantisce l'accesso	aclRequired value	Motivo
REST.DELETE.OBJECT	A	Non applicabile	B	Sì	-	Cross-account accesso concesso dalla bucket policy
REST.DELETE.OBJECT	A	Non applicabile	B	No	Sì	Cross-account l'accesso si basa su ACL
REST.PUT.ACL	*	*	*	Sì o No	Sì	Richiesta di autorizzazioni ACL

ACL di esempio

La seguente ACL di esempio su un bucket identifica il proprietario della risorsa e un insieme di concessioni. Il suo formato è la rappresentazione XML di una lista ACL in REST API di Amazon S3. Il proprietario del bucket ha il FULL_CONTROL della risorsa. Inoltre, l'ACL mostra come vengono concesse le autorizzazioni su una risorsa a due Account AWS, identificati da un ID utente canonico, e a due dei gruppi Amazon S3 predefiniti discussi nella sezione precedente.

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>Owner-canonical-user-ID</ID>
  </Owner>
```

```
<AccessControllist>
  <Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
      <ID>Owner-canonical-user-ID</ID>
    </Grantee>
    <Permission>FULL_CONTROL</Permission>
  </Grant>

  <Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
      <ID>user1-canonical-user-ID</ID>
    </Grantee>
    <Permission>WRITE</Permission>
  </Grant>

  <Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
      <ID>user2-canonical-user-ID</ID>
    </Grantee>
    <Permission>READ</Permission>
  </Grant>

  <Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
      <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
    </Grantee>
    <Permission>READ</Permission>
  </Grant>

  <Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
      <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>WRITE</Permission>
  </Grant>

</AccessControllist>
</AccessControlPolicy>
```

ACL predefinita

Amazon S3 supporta un set di concessioni predefinite, dette liste ACL predefinite. Ogni ACL predefinita ha un insieme predefinito di assegnatari e autorizzazioni. La seguente tabella elenca l'insieme di ACL predefinite e le concessioni predefinite associate.

ACL predefinita	Si applica a	Autorizzazioni aggiunte a un'ACL
<code>private</code>	Bucket e oggetto	Il proprietario ottiene il <code>FULL_CONTROL</code> . Nessun altro ha diritti di accesso (impostazione predefinita).
<code>public-read</code>	Bucket e oggetto	Il proprietario ottiene il <code>FULL_CONTROL</code> . Il gruppo <code>AllUsers</code> (consulta Che cosa si intende per assegnatario?) ottiene l'accesso <code>READ</code> .
<code>public-read-write</code>	Bucket e oggetto	Il proprietario ottiene il <code>FULL_CONTROL</code> . Il gruppo <code>AllUsers</code> ottiene l'accesso <code>READ</code> e <code>WRITE</code> . In genere la concessione di queste autorizzazioni su un bucket non è consigliata.
<code>aws-exec-read</code>	Bucket e oggetto	Il proprietario ottiene il <code>FULL_CONTROL</code> . Amazon EC2 ottiene l'accesso di tipo <code>READ</code> per la richiesta <code>GET</code> con cui ottenere un bundle Amazon Machine Image (AMI) da Amazon S3.
<code>authenticated-read</code>	Bucket e oggetto	Il proprietario ottiene il <code>FULL_CONTROL</code> . Il gruppo <code>AuthenticatedUsers</code> ottiene l'accesso <code>READ</code> .
<code>bucket-owner-read</code>	Oggetto	Il proprietario dell'oggetto ottiene il <code>FULL_CONTROL</code> . Il proprietario del bucket ottiene l'accesso <code>READ</code> . Se specifichi questa lista ACL predefinita durante la creazione di un bucket, Amazon S3 la ignora.
<code>bucket-owner-full-control</code>	Oggetto	Sia il proprietario dell'oggetto che il proprietario del bucket ottengono il <code>FULL_CONTROL</code> dell'oggetto. Se specifichi questa lista ACL predefinita durante la creazione di un bucket, Amazon S3 la ignora.

ACL predefinita	Si applica a	Autorizzazioni aggiunte a un'ACL
log-delivery-write	Bucket	Il gruppo LogDelivery ottiene le autorizzazioni WRITE e READ_ACP sul bucket. Per ulteriori informazioni sui log, consulta (Registrazione delle richieste con registrazione dell'accesso al server).

Note

È possibile specificare solo una di queste ACL predefinite nella richiesta.

Per specificare un'ACL predefinita nella richiesta si utilizza l'intestazione di richiesta `x-amz-acl`. Quando Amazon S3 riceve una richiesta contenente una lista ACL predefinita, aggiunge le concessioni predefinite alla lista ACL della risorsa.

Configurazione delle ACL

Questa sezione descrive come gestire le autorizzazioni di accesso per bucket e oggetti S3 tramite le liste di controllo accessi (ACL). Puoi aggiungere sovvenzioni all'ACL della tua risorsa utilizzando AWS Command Line Interface (CLI) Console di gestione AWS, REST API o SDK. AWS

Le autorizzazioni per il bucket e gli oggetti sono indipendenti l'una dall'altra. Un oggetto non eredita le autorizzazioni dal bucket a cui appartiene. Se ad esempio si crea un bucket e si concede l'accesso in scrittura a un utente, non sarà possibile accedere agli oggetti di tale utente a meno che questi non conceda esplicitamente l'accesso.

Puoi concedere autorizzazioni ad altri Account AWS utenti o a gruppi predefiniti. L'utente o il gruppo a cui si concedono le autorizzazioni è denominato assegnatario. Per impostazione predefinita, il proprietario, ovvero colui Account AWS che ha creato il bucket, dispone delle autorizzazioni complete.

Ogni autorizzazione concessa a un utente o a un gruppo aggiunge una voce all'ACL associata al bucket. Nell'ACL sono elencate le assegnazioni, che identificano l'assegnatario e l'autorizzazione concessa.

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le liste di controllo degli accessi (ACL) sono disabilitate. Quando le ACL sono disabilitate, il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ad essi in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne nelle circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Con le ACL disabilitate, puoi utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Warning

Non concedere l'accesso in scrittura ai gruppi `Everyone` (accesso pubblico) o `Authenticated Users` (tutti gli utenti AWS autenticati). Per maggiori informazioni sugli effetti della concessione dell'accesso in scrittura a questi gruppi, consulta [Gruppi predefiniti di Amazon S3](#).

Utilizzo della console S3 per impostare le autorizzazioni ACL per un bucket

La console mostra le concessioni di accesso combinate per gli assegnatari duplicati. Per visualizzare l'elenco completo degli ACL, utilizza l'API REST di Amazon S3 o gli SDK. AWS CLI AWS

Nella tabella seguente vengono illustrate le autorizzazioni ACL che è possibile configurare per i bucket nella console di Amazon S3.

Autorizzazioni ACL della console di Amazon S3 per i bucket

Autorizzazione console	Autorizzazione ACL	Accesso
Oggetti – Elenco	READ	Consente all'assegnatario di elencare gli oggetti del bucket.
Oggetti - Scrittura	WRITE	Consente all'assegnatario di creare nuovi oggetti del bucket. Per i proprietari di bucket e oggetti di oggetti esistenti, consente anche di eliminare e sovrascrivere tali oggetti.
ACL del bucket – Lettura	READ_ACP	Consente all'assegnatario di leggere l'ACL del bucket.
ACL del bucket – Scrittura	WRITE_ACP	Consente all'assegnatario di scrivere l'ACL del bucket interessato.
Everyone (Tutti) (accesso pubblico) : Oggetti - Elenco	READ	Concede l'accesso pubblico in lettura per gli oggetti nel bucket. Quando si concede l'accesso all'elenco a Everyone (Tutti) (accesso pubblico), chiunque al mondo può accedere agli oggetti nel bucket.
Everyone (Tutti) (accesso pubblico) : ACL del bucket - Lettura	READ_ACP	Concede l'accesso pubblico in lettura per l'ACL del bucket. Quando si concede l'accesso in lettura a Everyone (Tutti) (accesso pubblico), chiunque al mondo può accedere all'ACL del bucket.

Per ulteriori informazioni sulle autorizzazioni ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

⚠ Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Come impostare le autorizzazioni ACL per un bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco Buckets (Bucket) scegliere il nome del bucket per cui impostare le autorizzazioni.
4. Seleziona Autorizzazioni.
5. In Lista di controllo degli accessi (ACL), seleziona Modifica.

Puoi modificare le seguenti autorizzazioni ACL per il bucket:

Oggetti

- **List:** consente all'assegnatario di elencare gli oggetti nel bucket.
- **Scrittura** – Consente all'assegnatario di creare nuovi oggetti nel bucket. Per i proprietari di bucket e oggetti di oggetti esistenti, consente anche di eliminare e sovrascrivere tali oggetti.

Nella console S3, puoi concedere l'accesso in scrittura solo al gruppo di distribuzione dei log S3 e al proprietario del bucket (il tuo). Account AWS Non concedere l'accesso in scrittura ad altri beneficiari. Tuttavia, se devi concedere l'accesso in scrittura, puoi utilizzare gli AWS SDK o l' AWS CLI API REST.

ACL del bucket

- Read: consente all'assegnatario di leggere l'ACL del bucket.
 - Write: consente all'assegnatario di scrivere l'ACL del bucket interessato.
6. Per modificare le autorizzazioni del proprietario del bucket, accanto a **Bucket owner (your Account AWS)**, deselecta o seleziona una delle seguenti autorizzazioni ACL:
- Oggetti – Elenco o scrittura
 - ACL del bucket – Lettura o scrittura

Il proprietario si riferisce a Utente root dell'account AWS, non a un utente IAM. AWS Identity and Access Management Per ulteriori informazioni sull'utente root, consulta [Utente root dell'account AWS](#) nella Guida per l'utente di IAM.

7. Per concedere o annullare le autorizzazioni per il pubblico generale (tutti su Internet), accanto a **Tutti (accesso pubblico)**, deselecta o seleziona una delle seguenti autorizzazioni ACL:
- Oggetti – Elenco
 - ACL del bucket – Lettura

Warning

Prestare attenzione nel concedere l'accesso pubblico al bucket S3 al gruppo Everyone (Tutti). Quando si concede l'accesso a questo gruppo, qualsiasi persona al mondo può accedere al bucket. Non concedere mai alcun tipo di accesso pubblico in scrittura al tuo bucket S3.

8. Per concedere o annullare le autorizzazioni a chiunque disponga di un Account AWS, oltre al gruppo **Authenticated Users** (chiunque ne abbia uno Account AWS), deselecta o seleziona una delle seguenti autorizzazioni ACL:
- Oggetti – Elenco
 - ACL del bucket – Lettura
9. Per concedere o annullare le autorizzazioni per Amazon S3 a scrivere i log di accesso al server nel bucket, in gruppo di recapito log S3 deselecta o seleziona una delle seguenti autorizzazioni ACL:

- Oggetti – Elenco o scrittura
- ACL del bucket – Lettura o scrittura

Se un bucket è impostato come destinazione per ricevere i log di accesso, le autorizzazioni del bucket devono consentire l'accesso in scrittura al gruppo Log Delivery. Quando abiliti la registrazione degli accessi al server su un bucket, la console Amazon S3 concede l'accesso in scrittura al gruppo Log Delivery per il bucket di destinazione scelto. Per ulteriori informazioni sulla registrazione degli accessi al server, consulta [Abilitazione della registrazione degli accessi al server Amazon S3](#).

10. Per concedere l'accesso a un altro Account AWS utente, procedi come segue:

- Scegli Aggiungi assegnatario.
- Nella casella Assegnatario, inserisci l'ID canonico dell'altro Account AWS.
- Seleziona una delle seguenti autorizzazioni ACL:
 - Oggetti – Elenco o scrittura
 - ACL del bucket – Lettura o scrittura

 Warning

Quando concedi ad altri Account AWS l'accesso alle tue risorse, tieni presente che Account AWS possono delegare le proprie autorizzazioni agli utenti con i loro account. Questa operazione è nota con il nome di accesso multiaccount. Per informazioni sull'utilizzo dell'accesso multiaccount, consulta [Creazione di un ruolo per delegare le autorizzazioni a un utente IAM](#) nella Guida per l'utente di IAM.

11. Per rimuovere l'accesso a un altro utente Account AWS, in Accesso per altro Account AWS, scegli Rimuovi.
12. Per salvare le modifiche, scegliere Save changes (Salva modifiche).

Utilizzo della console S3 per impostare le autorizzazioni ACL per un oggetto

La console mostra le concessioni di accesso combinate per gli assegnatari duplicati. Per visualizzare l'elenco completo degli ACL, utilizza l'API REST di Amazon S3 o AWS gli AWS CLI SDK. Nella tabella seguente vengono illustrate le autorizzazioni ACL che è possibile configurare per gli oggetti nella console di Amazon S3.

Autorizzazioni ACL della console di Amazon S3 per gli oggetti

Autorizzazione console	Autorizzazione ACL	Accesso
Oggetto - Lettura	READ	Consente all'assegnatario di leggere i dati dell'oggetto e i relativi metadati.
ACL dell'oggetto - Lettura	READ_ACP	Consente all'assegnatario di leggere l'ACL dell'oggetto.
ACL dell'oggetto - Scrittura	WRITE_ACP	Consente all'assegnatario di scrivere l'ACL dell'oggetto interessato

Per ulteriori informazioni sulle autorizzazioni ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

 Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Come impostare le autorizzazioni ACL per un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti, scegli il nome dell'oggetto per il quale si desidera impostare le autorizzazioni.
4. Seleziona Autorizzazioni.
5. In Lista di controllo degli accessi (ACL), seleziona Modifica.

Puoi modificare le seguenti autorizzazioni ACL per l'oggetto:

Oggetto

- Read: consente all'assegnatario di leggere i dati dell'oggetto e i relativi metadati.

ACL dell'oggetto

- Read: consente all'assegnatario di leggere l'ACL dell'oggetto.
- Write: consente all'assegnatario di scrivere l'ACL per l'oggetto interessato. Nella console S3, puoi concedere l'accesso in scrittura solo al proprietario del bucket (il tuo). Account AWS Non concedere l'accesso in scrittura ad altri beneficiari. Tuttavia, se devi concedere l'accesso in scrittura, puoi utilizzare gli AWS SDK o l' AWS CLI API REST.

6. È possibile gestire le autorizzazioni di accesso all'oggetto per i seguenti tipi di accesso:

a. Accesso per il proprietario dell'oggetto

Il proprietario si riferisce a Utente root dell'account AWS, e non a un utente AWS Identity and Access Management IAM. Per ulteriori informazioni sull'utente root, consulta [Utente root dell'account AWS](#) nella Guida per l'utente di IAM.

Per modificare le autorizzazioni di accesso agli oggetti del proprietario, in Accesso per il proprietario dell'oggetto, scegli Il tuo AWS account (proprietario).

Selezionare le caselle di controllo per le autorizzazioni da modificare, quindi selezionare Save (Salva).

b. Accesso per altri Account AWS

Per concedere le autorizzazioni a un AWS utente di un altro utente Account AWS, in Accesso per altro Account AWS, scegli Aggiungi account. Nel campo Inserisci un ID, inserisci l'ID canonico dell' AWS utente a cui desideri concedere le autorizzazioni all'oggetto. Per informazioni sulla ricerca di un ID canonico, consulta [I tuoi identificatori in. Account AWS](#) Riferimenti generali di Amazon Web Services È possibile aggiungere fino a 99 utenti.

Selezionare le caselle di controllo relative alle autorizzazioni da concedere all'utente, quindi selezionare Save (Salva). Per visualizzare informazioni sulle autorizzazioni, scegliere le icone della Guida in linea.

c. Accesso pubblico

Per concedere al pubblico (chiunque al mondo) l'accesso all'oggetto, in Public access (Accesso pubblico) scegliere Everyone (Tutti). La concessione delle autorizzazioni di accesso pubblico consente a chiunque di accedere all'oggetto.

Selezionare le caselle di controllo per le autorizzazioni da concedere, quindi selezionare Save (Salva).

Warning

- Prestare attenzione quando si concede al gruppo Everyone (Tutti) l'accesso anonimo agli oggetti Amazon S3. Quando si concede l'accesso a questo gruppo, qualsiasi persona al mondo può accedere all'oggetto. Se è necessario concedere l'accesso a chiunque, è vivamente consigliato farlo solo per autorizzazioni di tipo Read objects (Leggi oggetti).
- Non concedere al gruppo Everyone i permessi di scrittura sugli oggetti, perché questo consentirebbe a chiunque di sovrascrivere le autorizzazioni ACL per l'oggetto.

Utilizzo di AWS SDK

Gli esempi seguenti mostrano come impostare le concessioni ACL (Access Control List) su bucket e oggetti.

Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Java

Gli esempi seguenti mostrano come impostare le concessioni ACL (Access Control List) su bucket e oggetti. Il primo esempio crea un bucket con un ACL predefinito (vedi [ACL predefinita](#)), crea un elenco di concessioni personalizzate e quindi sostituisce l'ACL predefinito con le concessioni personalizzate. Il secondo esempio mostra come modificare un'ACL utilizzando il metodo `AccessControlList.grantPermission()`.

Example Creare un bucket e specificare una ACL predefinita che concede l'autorizzazione al gruppo di recapito log S3

Questo esempio crea un bucket. Nella richiesta, l'esempio specifica un'ACL predefinita che concede al Gruppo Log Delivery l'autorizzazione di scrittura dei log sul bucket.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;

public class CreateBucketWithACL {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "**** Bucket name ****";
        String userEmailForReadPermission = "**** user@example.com ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .withRegion(clientRegion)
                .build();

            // Create a bucket with a canned ACL. This ACL will be replaced by the
            // setBucketAcl()
            // calls below. It is included here for demonstration purposes.
            CreateBucketRequest createBucketRequest = new
            CreateBucketRequest(bucketName, clientRegion.getName())
                .withCannedAcl(CannedAccessControlList.LogDeliveryWrite);
```

```

        s3Client.createBucket(createBucketRequest);

        // Create a collection of grants to add to the bucket.
        ArrayList<Grant> grantCollection = new ArrayList<Grant>();

        // Grant the account owner full control.
        Grant grant1 = new Grant(new
CanonicalGrantee(s3Client.getS3AccountOwner().getId()),
            Permission.FullControl);
        grantCollection.add(grant1);

        // Grant the LogDelivery group permission to write to the bucket.
        Grant grant2 = new Grant(GroupGrantee.LogDelivery, Permission.Write);
        grantCollection.add(grant2);

        // Save grants by replacing all current ACL grants with the two we just
created.
        AccessControlList bucketAcl = new AccessControlList();
        bucketAcl.grantAllPermissions(grantCollection.toArray(new Grant[0]));
        s3Client.setBucketAcl(bucketName, bucketAcl);

        // Retrieve the bucket's ACL, add another grant, and then save the new
ACL.
        AccessControlList newBucketAcl = s3Client.getBucketAcl(bucketName);
        Grant grant3 = new Grant(new
EmailAddressGrantee(userEmailForReadPermission), Permission.Read);
        newBucketAcl.grantAllPermissions(grant3);
        s3Client.setBucketAcl(bucketName, newBucketAcl);
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
// it and returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
// couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
}

```

Example Aggiornamento di un'ACL su un oggetto esistente

Questo esempio aggiorna l'ACL su un oggetto. L'esempio esegue le seguenti operazioni:

- Recupera l'ACL di un oggetto
- Elimina l'ACL rimuovendo tutte le autorizzazioni esistenti
- Aggiunge due autorizzazioni: accesso completo al proprietario e WRITE_ACP (consulta [Quali autorizzazioni è possibile concedere?](#)) per un utente identificato tramite un indirizzo email
- Salva l'ACL sull'oggetto

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.AccessControlList;
import com.amazonaws.services.s3.model.CanonicalGrantee;
import com.amazonaws.services.s3.model.EmailAddressGrantee;
import com.amazonaws.services.s3.model.Permission;

import java.io.IOException;

public class ModifyACLExistingObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "**** Bucket name ****";
        String keyName = "**** Key name ****";
        String emailGrantee = "**** user@example.com ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(clientRegion)
                .build();

            // Get the existing object ACL that we want to modify.
            AccessControlList acl = s3Client.getObjectAcl(bucketName, keyName);

            // Clear the existing list of grants.
            acl.getGrantsAsList().clear();
```



```

        // Grant a sample set of permissions, using the existing ACL owner for
Full
        // Control permissions.
        acl.grantPermission(new CanonicalGrantee(acl.getOwner().getId()),
Permission.FullControl);
        acl.grantPermission(new EmailAddressGrantee(emailGrantee),
Permission.WriteAcp);

        // Save the modified ACL back to the object.
        s3Client.setObjectAcl(bucketName, keyName, acl);
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
}
}

```

.NET

Example Creare un bucket e specificare una ACL predefinita che concede l'autorizzazione al gruppo di recapito log S3

Questo esempio C# crea un bucket. Nella richiesta, il codice specifica anche un'ACL predefinita che concede al Gruppo Log Delivery le autorizzazioni di scrittura dei log sul bucket.

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the SDK for .NET nella AWS SDK for .NET Developer Guide](#). AWS

```

using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingBucketACLTest
    {

```

```

private const string newBucketName = "*** bucket name ***";
// Specify your bucket region (an example region is shown).
private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
private static IAmazonS3 client;

public static void Main()
{
    client = new AmazonS3Client(bucketRegion);
    CreateBucketUseCannedACLAsync().Wait();
}

private static async Task CreateBucketUseCannedACLAsync()
{
    try
    {
        // Add bucket (specify canned ACL).
        PutBucketRequest putBucketRequest = new PutBucketRequest()
        {
            BucketName = newBucketName,
            BucketRegion = S3Region.EUW1, // S3Region.US,
                                           // Add canned ACL.
            CannedACL = S3CannedACL.LogDeliveryWrite
        };
        PutBucketResponse putBucketResponse = await
client.PutBucketAsync(putBucketRequest);

        // Retrieve bucket ACL.
        GetACLResponse getACLResponse = await client.GetACLAsync(new
GetACLRequest
        {
            BucketName = newBucketName
        });
    }
    catch (AmazonS3Exception amazonS3Exception)
    {
        Console.WriteLine("S3 error occurred. Exception: " +
amazonS3Exception.ToString());
    }
    catch (Exception e)
    {
        Console.WriteLine("Exception: " + e.ToString());
    }
}

```

```
}  
}
```

Example Aggiornamento di un'ACL su un oggetto esistente

Questo esempio C# aggiorna l'ACL su un oggetto esistente. L'esempio esegue le seguenti operazioni:

- Recupera l'ACL di un oggetto.
- Elimina l'ACL rimuovendo tutte le autorizzazioni esistenti.
- Aggiunge due autorizzazioni: accesso completo al proprietario e WRITE_ACP per un utente identificato tramite un indirizzo email.
- Salva l'ACL inviando una richiesta PutAc1.

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;  
using Amazon.S3;  
using Amazon.S3.Model;  
using System;  
using System.Collections.Generic;  
using System.Threading.Tasks;  
  
namespace Amazon.DocSamples.S3  
{  
    class ManagingObjectACLTest  
    {  
        private const string bucketName = "**** bucket name ****";  
        private const string keyName = "**** object key name ****";  
        private const string emailAddress = "**** email address ****";  
        // Specify your bucket region (an example region is shown).  
        private static readonly RegionEndpoint bucketRegion =  
        RegionEndpoint.USWest2;  
        private static IAmazonS3 client;  
        public static void Main()  
        {  
            client = new AmazonS3Client(bucketRegion);  
            TestObjectACLTestAsync().Wait();  
        }  
        private static async Task TestObjectACLTestAsync()
```

```
{
    try
    {
        // Retrieve the ACL for the object.
        GetACLResponse aclResponse = await client.GetACLAsync(new
GetACLRequest
        {
            BucketName = bucketName,
            Key = keyName
        });

        S3AccessControlList acl = aclResponse.AccessControlList;

        // Retrieve the owner (we use this to re-add permissions after
we clear the ACL).
        Owner owner = acl.Owner;

        // Clear existing grants.
        acl.Grants.Clear();

        // Add a grant to reset the owner's full permission (the
previous clear statement removed all permissions).
        S3Grant fullControlGrant = new S3Grant
        {
            Grantee = new S3Grantee { CanonicalUser = owner.Id },
            Permission = S3Permission.FULL_CONTROL
        };

        // Describe the grant for the permission using an email address.
        S3Grant grantUsingEmail = new S3Grant
        {
            Grantee = new S3Grantee { EmailAddress = emailAddress },
            Permission = S3Permission.WRITE_ACP
        };
        acl.Grants.AddRange(new List<S3Grant> { fullControlGrant,
grantUsingEmail });

        // Set a new ACL.
        PutACLResponse response = await client.PutACLAsync(new
PutACLRequest
        {
            BucketName = bucketName,
            Key = keyName,
```

```
        AccessControllList = acl
    });
}
catch (AmazonS3Exception amazonS3Exception)
{
    Console.WriteLine("An AmazonS3Exception was thrown. Exception: " +
amazonS3Exception.ToString());
}
catch (Exception e)
{
    Console.WriteLine("Exception: " + e.ToString());
}
}
}
```

Utilizzo della REST API

Le API Amazon S3 permettono di impostare una lista ACL durante la creazione di un bucket o di un oggetto. Amazon S3 fornisce anche un'API per impostare una lista ACL in un bucket o un oggetto esistente. Queste API forniscono i metodi seguenti per impostare un'ACL:

- Impostazione della lista ACL tramite le intestazioni della richiesta – Quando invii una richiesta per creare una risorsa (bucket o oggetto), imposti una lista ACL utilizzando le intestazioni della richiesta. Tramite queste intestazioni, si può specificare o un'ACL predefinita oppure si possono indicare esplicitamente le concessioni (identificando assegnatario e autorizzazioni in modo esplicito).
- Impostazione della lista ACL tramite il corpo della richiesta – Quando invii una richiesta per impostare una lista ACL per una risorsa esistente, puoi impostare la lista ACL o nell'intestazione o nel corpo della richiesta.

Per informazioni sul supporto di REST API per la gestione delle liste ACL, consulta le sezioni seguenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [GetBucketAcl](#)
- [PutBucketAcl](#)
- [GetObjectAcl](#)
- [PutObjectAcl](#)

- [PutObject](#)
- [CreateBucket](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)

 Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Intestazioni di richiesta specifiche della lista di controllo degli accessi (ACL)

È possibile utilizzare le intestazioni per concedere le autorizzazioni basate sulla lista di controllo degli accessi (ACL). Per impostazione predefinita, tutti gli oggetti sono privati. Solo il proprietario ha il controllo completo dell'accesso. Quando aggiungi un nuovo oggetto, puoi concedere autorizzazioni a singoli gruppi Account AWS o a gruppi predefiniti definiti da Amazon S3. Queste autorizzazioni vengono quindi aggiunte all'ACL sull'oggetto. Per ulteriori informazioni, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

Con questa operazione, puoi concedere le autorizzazioni di accesso utilizzando uno dei due metodi seguenti:

- **ACL predefinita (`x-amz-acl`)** - Amazon S3 supporta un set di ACL predefinite, note come ACL predefinite. Ogni ACL predefinita ha un insieme predefinito di assegnatari e autorizzazioni. Per ulteriori informazioni, consulta [ACL predefinita](#).
- **Autorizzazioni di accesso:** per concedere esplicitamente le autorizzazioni di accesso a specifici Account AWS o gruppi, utilizza le seguenti intestazioni. Ogni intestazione esegue il mapping di autorizzazioni specifiche supportate da Amazon S3 in un'ACL. Per ulteriori informazioni, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#). Nell'intestazione, specifica un elenco di assegnatari che ottengono l'autorizzazione specifica.

- x-amz-grant-read
- x-amz-grant-write
- x-amz-grant-read-acp
- x-amz-grant-write-acp
- x-amz-grant-full control

Utilizzo di AWS CLI

Per ulteriori informazioni sulla gestione degli ACL utilizzando il AWS CLI, vedere <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/put-bucket-acl.html> put-bucket-acl nel Command Reference. AWS CLI

Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Esempi di policy per le ACL

È possibile utilizzare le chiavi di condizione nelle policy dei bucket per controllare l'accesso ad Amazon S3.

Argomenti

- [Concessione di s3: PutObject autorizzazione con una condizione che richiede al proprietario del bucket di ottenere il pieno controllo](#)
- [Concessione dell'PutObject autorizzazione a s3: con una condizione nell'intestazione x-amz-acl](#)

Concessione di s3:PutObject autorizzazione con una condizione che richiede al proprietario del bucket di ottenere il pieno controllo

L'[operazione](#) PUT Object consente l'uso di intestazioni specifiche per gli elenchi di controllo degli accessi (ACL) che è possibile utilizzare per concedere le autorizzazioni. ACL-based Utilizzando queste chiavi, il proprietario del bucket può impostare una condizione per richiedere determinate autorizzazioni di accesso specifiche quando l'utente carica un oggetto.

Si supponga che l'Account A sia proprietario di un bucket e che l'amministratore dell'account voglia assegnare a Dave, un utente dell'Account B, le autorizzazioni per caricare oggetti. Per default, gli oggetti che carica Dave sono di proprietà dell'Account B e l'Account A non dispone di autorizzazioni su tali oggetti. Dato che il proprietario del bucket paga i conti, vuole avere le autorizzazioni complete sugli oggetti che carica Dave. L'amministratore dell'Account A può eseguire questa operazione concedendo l'`s3:PutObject` autorizzazione a Dave, a condizione che la richiesta includa ACL-specific intestazioni che concedono esplicitamente l'autorizzazione completa o utilizzano un ACL predefinito. Per ulteriori informazioni, consulta [PUT Object](#).

Richiesta dell'intestazione `x-amz-full-control`

È possibile richiedere l'intestazione `x-amz-full-control` nella richiesta con autorizzazione al controllo completo al proprietario del bucket. La seguente policy di bucket assegna l'autorizzazione `s3:PutObject` all'utente Dave con la condizione di utilizzare la chiave di condizione `s3:x-amz-grant-full-control` che prevede che la richiesta includa l'intestazione `x-amz-full-control`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Dave"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3::awsexamplebucket1/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
        }
      }
    }
  ]
}
```



```

    }
  }
}

```

Note

Questo esempio riguarda l'autorizzazione tra account. Tuttavia, se Dave (che sta ottenendo l'autorizzazione) appartiene al proprietario del bucket, Account AWS questa autorizzazione condizionale non è necessaria. Questo perché l'account padre a cui Dave appartiene è proprietario degli oggetti caricati dall'utente.

Aggiunta del rifiuto esplicito

La precedente politica del bucket concede l'autorizzazione condizionale all'utente Dave nell'Account B. Mentre questa politica è in vigore, è possibile per Dave ottenere la stessa autorizzazione senza alcuna condizione attraverso un'altra politica. Ad esempio, Dave può appartenere a un gruppo a cui viene assegnata l'autorizzazione `s3:PutObject` senza alcuna condizione. Per evitare questi espedienti riguardo alle autorizzazioni, è possibile scrivere una policy di accesso più rigida aggiungendo un rifiuto esplicito. In questo esempio, all'utente Dave viene esplicitamente rifiutata l'autorizzazione a eseguire caricamenti se non include le intestazioni necessarie nella richiesta che assegnano le autorizzazioni complete al proprietario del bucket. Il rifiuto esplicito sovrascrive sempre qualsiasi altra autorizzazione assegnata. Di seguito è illustrato un esempio della policy di accesso modificata con il rifiuto esplicito aggiunto.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/AccountBadmin"
      },
      "Action": "s3:PutObject",

```

```

    "Resource": "arn:aws:s3:::awsexamplebucket1/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
      }
    },
  },
  {
    "Sid": "statement2",
    "Effect": "Deny",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:user/AccountBadmin"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::awsexamplebucket1/*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
      }
    }
  }
]
}

```

Verifica la politica con il AWS CLI

Se ne hai due Account AWS, puoi testare la policy usando AWS Command Line Interface (AWS CLI). Allegate la policy e utilizzate le credenziali di Dave per testare l'autorizzazione utilizzando il seguente AWS CLI `put-object` comando. Le credenziali di Dave vengono fornite aggiungendo il parametro `--profile`. L'autorizzazione al controllo completo al proprietario del bucket viene assegnata aggiungendo il parametro `--grant-full-control`. Per ulteriori informazioni sulla configurazione e l'utilizzo di AWS CLI, consulta [Developing with Amazon S3 using the AWS CLI](#) nell'Amazon S3 API Reference.

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
--grant-full-control id="AccountA-CanonicalUserID" --profile AccountBUserProfile
```

Richiesta dell'intestazione x-amz-acl

È possibile richiedere l'intestazione `x-amz-acl` con una lista di controllo degli accessi predefinita che assegna l'autorizzazione al controllo completo al proprietario del bucket. Per richiedere

l'intestazione `x-amz-acl` nella richiesta, è possibile sostituire la coppia chiave-valore nel blocco `Condition` e specificare la chiave di condizione `s3:x-amz-acl` come mostrato nell'esempio seguente.

```
"Condition": {
  "StringEquals": {
    "s3:x-amz-acl": "bucket-owner-full-control"
  }
}
```

Per testare l'autorizzazione utilizzando il AWS CLI, è necessario specificare il parametro. `--acl` AWS CLI Quindi aggiunge l'`x-amz-acl` intestazione quando invia la richiesta.

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
--acl "bucket-owner-full-control" --profile AccountBadmin
```

Concessione dell'`PutObject` autorizzazione a `s3`: con una condizione nell'intestazione `x-amz-acl`

La seguente policy del bucket concede l'`s3:PutObject` autorizzazione per due persone Account AWS se la richiesta include l'intestazione che rende l'oggetto leggibile pubblicamente. `x-amz-acl` Il blocco `Condition` utilizza la condizione `StringEquals` ed è dotato di una coppia chiave-valore, `"s3:x-amz-acl":["public-read"]`, per la valutazione. Nella coppia chiave-valore, la `s3:x-amz-acl` è una chiave specifica di Amazon S3, come indicato dal prefisso `s3:`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddCannedAcl",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::111122223333:root"
        ]
      }
    }
  ],
}
```

```
    "Action": "s3:PutObject",
    "Resource": [
        "arn:aws:s3:::awsexamplebucket1/*"
    ],
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": [
                "public-read"
            ]
        }
    }
}
```

Important

Non tutte le condizioni hanno significato per tutte le operazioni. Ha senso, ad esempio, includere una condizione `s3:LocationConstraint` in una policy che concede l'autorizzazione `s3:CreateBucket` di Amazon S3. Non ha tuttavia senso includere questa condizione in una policy che concede l'autorizzazione `s3:GetObject`. Amazon S3 può verificare la presenza di errori semantici di questo tipo che riguardano condizioni specifiche di Amazon S3. Se tuttavia stai creando una policy per un utente o un ruolo IAM e includi una condizione di Amazon S3 che non è valida sotto il profilo semantico, non viene segnalato alcun errore perché IAM non può convalidare le condizioni di Amazon S3.

Blocco dell'accesso pubblico allo storage Amazon S3

La funzionalità Amazon S3 Block Public Access fornisce impostazioni per punti di accesso, bucket, account e aiuta AWS Organizations a gestire l'accesso pubblico alle risorse Amazon S3. Per impostazione predefinita, nuovi bucket, access point e oggetti non consentono l'accesso pubblico. Tuttavia, gli utenti possono modificare le policy di bucket, le policy di access point o le autorizzazioni degli oggetti per consentire l'accesso pubblico. Le impostazioni di blocco dell'accesso pubblico in S3 sostituiscono le policy e le autorizzazioni, in modo da limitare l'accesso pubblico a queste risorse.

Con S3 Block Public Access, gli amministratori dell'organizzazione, gli amministratori degli account e i proprietari di bucket possono facilmente configurare controlli centralizzati per limitare l'accesso

pubblico alle risorse Amazon S3 che vengono applicate indipendentemente da come le risorse vengono create.

Puoi gestire le impostazioni di Block Public Access a più livelli: livello di organizzazione (utilizzo AWS Organizations), livello di account e livello di bucket e punto di accesso. Per istruzioni sulla configurazione dell'accesso pubblico ai blocchi, consulta [Configurazione del blocco dell'accesso pubblico](#).

Quando Amazon S3 riceve una richiesta di accesso a un bucket o a un oggetto, determina se per il bucket o l'account del proprietario del bucket è applicata un'impostazione di blocco dell'accesso pubblico. Se l'account fa parte di una AWS Organizations policy di Block Public Access, Amazon S3 verifica anche le impostazioni a livello di organizzazione. Se la richiesta è stata effettuata tramite un punto di accesso, Amazon S3 controlla anche la presenza di impostazioni di blocco dell'accesso pubblico per il punto di accesso. Se è presente un'impostazione di blocco dell'accesso pubblico che vieta l'accesso richiesto, Amazon S3 rifiuta la richiesta.

Il blocco dell'accesso pubblico di Amazon S3 comprende quattro impostazioni. Queste impostazioni sono indipendenti e possono essere usate in qualunque combinazione. Ogni impostazione può essere applicata a un punto di accesso, a un bucket o a un intero Account AWS. A livello di organizzazione, tutte e quattro le impostazioni vengono applicate insieme come una policy unificata: non è possibile selezionare le singole impostazioni in modo granulare. Se le impostazioni di accesso pubblico del blocco per il punto di accesso, il bucket o l'account sono diverse, Amazon S3 applica la combinazione più restrittiva delle impostazioni del punto di accesso, del bucket e dell'account. Account-level le impostazioni ereditano automaticamente le politiche a livello di organizzazione quando sono presenti e S3 adotta la politica più restrittiva tra le impostazioni a livello di bucket ed effettive a livello di account. Ad esempio, se la tua organizzazione ha abilitato un criterio di blocco dell'accesso pubblico, ma un bucket specifico ha il blocco dell'accesso pubblico disabilitato a livello di bucket, il bucket sarà comunque protetto perché S3 applica le impostazioni a livello più restrittivo. organization/account Al contrario, se i criteri dell'organizzazione sono disattivati ma in un bucket è abilitato il blocco dell'accesso pubblico, quel bucket rimane protetto dalle impostazioni a livello di bucket.

Quando Amazon S3 valuta se un'operazione è vietata da un'impostazione di blocco di accesso pubblico, respinge qualsiasi richiesta che violi una politica organizzativa (che applica l'impostazione BPA dell'account) o un'impostazione del punto di accesso, di un bucket o di un account.

 Important

L'accesso pubblico viene concesso a bucket e oggetti tramite liste di controllo accessi (ACL), policy per access point, policy di bucket o tutti. Per garantire che l'accesso pubblico sia bloccato per tutti gli access point, i bucket e gli oggetti di Amazon S3, ti consigliamo di attivare tutte e quattro le impostazioni per bloccare l'accesso pubblico per l'account. Per le organizzazioni che gestiscono più account, prendi in considerazione l'utilizzo di politiche di blocco dell'accesso pubblico a livello di organizzazione per un controllo centralizzato. Inoltre, ti consigliamo di attivare anche tutte e quattro le impostazioni per ciascun bucket per conformarti al controllo Security Foundational Security Best Practices di AWS Security di Security. S3.8 Queste impostazioni bloccano l'accesso pubblico per tutti i bucket e access point correnti e futuri.

Prima di applicare queste impostazioni, verifica che le applicazioni funzionino correttamente senza accesso pubblico. Se è richiesto un certo livello di accesso pubblico ai bucket o agli oggetti, ad esempio per ospitare un sito Web statico come descritto in [Hosting di un sito Web statico tramite Amazon S3](#), puoi personalizzare le impostazioni individuali in funzione dei casi d'uso di storage.

L'abilitazione di Blocca accesso pubblico aiuta a proteggere le risorse, impedendo che l'accesso pubblico sia concesso attraverso le policy delle risorse o le liste di controllo degli accessi (ACL) direttamente collegate alle risorse S3. Oltre ad abilitare l'opzione Blocca accesso pubblico, controlla attentamente le seguenti policy per verificare che non forniscano l'accesso pubblico:

- Identity-based politiche associate ai AWS principali associati (ad esempio, ruoli IAM)
- Resource-based politiche associate alle AWS risorse associate (ad esempio, chiavi AWS Key Management Service (KMS))

 Note

- È possibile abilitare le impostazioni di blocco dell'accesso pubblico solo per organizzazioni, punti di accesso, bucket e. Account AWS Amazon S3 non supporta le impostazioni di blocco dell'accesso pubblico per i singoli oggetti.
- Quando applichi le impostazioni di blocco dell'accesso pubblico a un account, le impostazioni si applicano a tutti a Regioni AWS livello globale. Le impostazioni possono

non diventare effettive in tutte le regioni immediatamente o allo stesso momento, ma vengono infine propagate in tutte le regioni.

- Quando applichi le politiche di blocco dell'accesso pubblico a livello di organizzazione, queste si propagano automaticamente agli account membri selezionati e sostituiscono le impostazioni a livello di account.

Argomenti

- [Impostazioni di blocco dell'accesso pubblico](#)
- [Gestione dei blocchi di accesso pubblico a livello di organizzazione](#)
- [Esecuzione di operazioni di accesso pubblico di blocco su un punto di accesso](#)
- [Significato di "pubblico"](#)
- [Utilizzo di IAM Access Analyzer per S3 per esaminare i bucket pubblici](#)
- [Permissions](#)
- [Configurazione del blocco dell'accesso pubblico](#)
- [Configurazione delle impostazioni di blocco dell'accesso pubblico per l'account](#)
- [Configurazione delle impostazioni di blocco dell'accesso pubblico per i bucket S3](#)

Impostazioni di blocco dell'accesso pubblico

Il blocco dell'accesso pubblico in S3 comprende quattro impostazioni. È possibile applicare queste impostazioni in qualsiasi combinazione a singoli access point, bucket o a interi account AWS. A livello di organizzazione, puoi abilitare o disabilitare tutte e quattro le impostazioni contemporaneamente utilizzando un approccio «tutte» o «nessuna»: il controllo granulare sulle singole impostazioni non è disponibile. Se applichi un'impostazione a un account, questa si applica a tutti i bucket e i punti di accesso di proprietà di quell'account. Account-level le impostazioni ereditano automaticamente dalle politiche dell'organizzazione quando presenti. Analogamente, se applichi un'impostazione a un bucket, questa si applica a tutti gli access point associati al bucket.

L'ereditarietà e l'applicazione delle politiche funzionano come segue:

- Organization-level le politiche si applicano automaticamente agli account dei membri, applicando tutte le impostazioni esistenti a livello di account
- Account-level le impostazioni ereditano dai criteri dell'organizzazione quando sono presenti o utilizzano le impostazioni configurate localmente quando non esistono criteri organizzativi

- Bucket-level le impostazioni funzionano in modo indipendente ma sono soggette a restrizioni di applicazione. S3 applica la combinazione più restrittiva a tutti i livelli applicabili: impostazioni a livello di organization/account livello e a livello di bucket. Ciò significa che un bucket eredita la protezione di base dal proprio account (che può essere gestito dall'organizzazione), ma S3 applicherà la configurazione più restrittiva tra le impostazioni del bucket e le impostazioni effettive dell'account.

La tabella seguente contiene le impostazioni disponibili.

Nome	Descrizione
BlockPublicAcls	<p>Se questa opzione è impostata su TRUE, produce il comportamento seguente:</p> <ul style="list-style-type: none">• <code>PutBucketAcl</code> e <code>PutObjectAcl</code> falliscono se la lista di controllo degli accessi (ACL) specificata è pubblica.• <code>PutObject</code> fallisce se la richiesta include una ACL pubblica.• Se questa impostazione viene applicata a un account, le chiamate <code>PUT Bucket</code> non riescono se la richiesta include una lista di controllo degli accessi pubblica. <p>Quando questa impostazione è impostata su TRUE, le operazioni specificate hanno esito negativo (sia che vengano eseguite tramite l'API REST o gli SDK). AWS CLI AWS Tuttavia, le policy e le liste di controllo degli accessi esistenti per bucket e oggetti non vengono modificate. Questa impostazione protegge l'ambiente dall'accesso pubblico, permettendo di controllare, perfezionare o modificare in altro modo le policy e le liste di controllo accessi per i bucket e gli oggetti.</p> <div><p> Note</p><p>I punti di accesso non hanno ACL associate. Se applicata a un punto di accesso, questa impostazione funge da passthrough al bucket sottostante. Se in un punto di accesso è attivata questa</p></div>

Nome	Descrizione
	<p>impostazione, le richieste effettuate tramite il punto di accesso si comportano come se il bucket sottostante avesse abilitato questa impostazione, indipendentemente dal fatto che il bucket abbia o meno effettivamente abilitato questa impostazione.</p>
IgnorePublicAcls	<p>Se questa opzione è impostata su TRUE, Amazon S3 ignora tutte le liste ACL pubbliche in un bucket e negli oggetti contenuti. Questa impostazione permette di bloccare in modo sicuro l'accesso pubblico concesso da liste di controllo degli accessi, permettendo comunque le chiamate <code>PutObject</code> che includono una lista di controllo degli accessi pubblica (diversamente da <code>BlockPublicAcls</code>, che rifiuta le chiamate <code>PutObject</code> che includono una lista di controllo degli accessi pubblica). L'abilitazione di questa impostazione non influisce sulla persistenza di qualsiasi lista di controllo accessi esistente e non impedisce l'impostazione di nuove liste di controllo accessi pubbliche.</p> <div data-bbox="430 976 1510 1434"><p> Note</p><p>Gli access point non hanno ACL associate. Se applicata a un punto di accesso, questa impostazione funge da passthrough al bucket sottostante. Se in un punto di accesso è attivata questa impostazione, le richieste effettuate tramite il punto di accesso si comportano come se il bucket sottostante avesse abilitato questa impostazione, indipendentemente dal fatto che il bucket abbia o meno effettivamente abilitato questa impostazione.</p></div>

Nome	Descrizione
BlockPublicPolicy	<p>L'impostazione di questa opzione su TRUE per un bucket fa sì che Amazon S3 rifiuti le chiamate a PutBucketPolicy se la policy di bucket specificata consente l'accesso pubblico. Impostando questa opzione su TRUE per un bucket, Amazon S3 rifiuta le chiamate a PutAccessPointPolicy per tutti i punti di accesso dello stesso account del bucket se la policy specificata consente l'accesso pubblico.</p> <p>Impostando questa opzione su TRUE per un punto di accesso, Amazon S3 rifiuta le chiamate a PutAccessPointPolicy e PutBucketPolicy effettuate attraverso il punto di accesso se la policy specificata (per il punto di accesso o il bucket sottostante) consente l'accesso pubblico.</p> <p>Puoi utilizzare questa impostazione per permettere agli utenti di gestire policy di bucket e punti di accesso impedendo loro di condividere pubblicamente il bucket o gli oggetti che contiene. L'abilitazione di questa impostazione non influisce sulle policy di access point o di bucket esistenti.</p> <div><p> Important</p><p>Per usare questa impostazione in modo efficace, consigliamo di applicarla a livello di account. Una policy del bucket può consentire e agli utenti di modificare le impostazioni di blocco dell'accesso pubblico di un bucket. Gli utenti autorizzati a modificare la policy del bucket potrebbero inserire una policy che permette loro di disabilitare le impostazioni di blocco dell'accesso pubblico per il bucket. Se questa impostazione è abilitata per l'intero account anziché per un bucket specifico, Amazon S3 blocca le policy pubbliche anche se un utente modifica la policy del bucket per disabilitare l'impostazione.</p></div>

Nome	Descrizione
<code>RestrictPublicBuckets</code>	<p>Se TRUE si imposta questa opzione in modo da limitare l'accesso a un access point o bucket con una policy pubblica solo ai responsabili del AWS servizio e agli utenti autorizzati all'interno dell'account del proprietario del bucket e dell'account del proprietario del punto di accesso. Questa impostazione blocca tutti gli accessi tra account all'access point o al bucket (ad eccezione dei responsabili del AWS servizio), pur consentendo agli utenti all'interno dell'account di gestire l'access point o il bucket.</p> <p>L'abilitazione di questa impostazione non influisce sulle policy dell'access point o del bucket esistenti, eccetto che per il fatto che Amazon S3 blocca l'accesso pubblico e multiaccount derivato da qualsiasi policy dell'access point o del bucket pubblica, inclusa la delega non pubblica ad account specifici.</p>

Important

- Le chiamate a `GetBucketAcl` e `GetObjectAcl` restituiscono sempre le autorizzazioni valide necessarie per il bucket o l'oggetto specificato. Ad esempio, supponiamo che un bucket sia associato a una lista di controllo accessi che concede l'accesso pubblico, ma che per il bucket sia anche abilitata l'impostazione `IgnorePublicAcls`. In questo caso, `GetBucketAcl` restituisce una lista ACL che riflette le autorizzazioni di accesso applicate da Amazon S3, anziché la lista ACL effettiva associata al bucket.
- Le impostazioni del blocco dell'accesso pubblico non modificano le policy o ACL esistenti. La rimozione di una di queste impostazioni fa sì che un bucket o un oggetto con una policy o una lista di controllo accessi pubblica torni pubblicamente accessibile.

Gestione dei blocchi di accesso pubblico a livello di organizzazione

Organization-level il blocco dell'accesso pubblico utilizza AWS Organizations politiche per gestire centralmente i controlli degli accessi pubblici di S3 in tutta l'organizzazione. Se abilitate, queste politiche si applicano automaticamente agli account selezionati e sostituiscono le singole impostazioni a livello di account.

Per ulteriori informazioni sul blocco dell'accesso pubblico a livello di organizzazione, consulta la politica [S3](#) nella guida per l'utente. AWS Organizations

Esecuzione di operazioni di accesso pubblico di blocco su un punto di accesso

Per eseguire operazioni di blocco dell'accesso pubblico su un punto di accesso, utilizza il AWS CLI `servicios3control`.

Important

Non è possibile modificare le impostazioni del blocco dell'accesso pubblico per un punto di accesso dopo la sua creazione. È possibile specificare le impostazioni di blocco dell'accesso pubblico per un punto di accesso solo durante la creazione del punto di accesso.

Significato di "pubblico"

Liste di controllo accessi

Amazon S3 considera pubblica una lista ACL di un bucket o di un oggetto se questa concede qualsiasi autorizzazione a membri dei gruppi predefiniti `AllUsers` e `AuthenticatedUsers`. Per ulteriori informazioni sui gruppi predefiniti, consulta [Gruppi predefiniti di Amazon S3](#).

Policy di bucket

Quando valuta la policy di un bucket, Amazon S3 inizia presumendo che la policy sia pubblica. Quindi valuta la policy per determinare se si qualifica come non pubblica. Per essere considerata non pubblica, una policy di bucket deve concedere l'accesso solo a valori fissi (valori che non contengono caratteri jolly o [una variabile di policy AWS Identity and Access Management](#)) di uno o più degli elementi seguenti:

- Un AWS principale, un utente, un ruolo o un responsabile del servizio (ad es. `aws:PrincipalOrgID`)
- Un set di blocchi Classless Inter-Domain Routings (CIDR), che utilizzano. `aws:SourceIp` Per ulteriori informazioni sui CIDR, consulta [RFC 4632](#) nel sito Web RFC Editor.

 Note

Policy bucket che concedono l'accesso condizionato alla chiave `aws:SourceIp` condizionale con intervalli IP molto ampi (ad esempio, `0.0.0.0/1`) sono valutati come «pubblici». Sono inclusi valori superiori a `/8` per IPv4 e `/32` per IPv6 (esclusi gli intervalli privati RFC1918). Il blocco dell'accesso pubblico rifiuta queste policy "pubbliche" e impedisce l'accesso multi-account ai bucket che già utilizzano queste policy "pubbliche".

- `aws:SourceArn`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:SourceOwner`
- `aws:SourceAccount`
- `aws:userid`, al di fuori del modello "AROLEID: *"
- `s3:DataAccessPointArn`

 Note

Se utilizzato in una policy di bucket, questo valore può contenere un carattere jolly per il nome del punto di accesso senza rendere pubblica la policy, purché l'ID dell'account sia corretto. Ad esempio, consentendo l'accesso a `arn:aws:s3:us-west-2:123456789012:accesspoint/*` si consente l'accesso a qualsiasi access point associato all'account 123456789012 nella regione us-west-2, senza rendere pubblica la policy di bucket. Questo comportamento è diverso per le policy del punto di accesso. Per ulteriori informazioni, consulta [Access point](#).

- `s3:DataAccessPointAccount`

Per ulteriori informazioni sulle policy di bucket, consulta [Policy dei bucket per Amazon S3](#).

 Note

Quando si utilizzano [chiavi di contesto multivalore](#), è necessario utilizzare gli operatori `ForAllValues` o `ForAnyValue`.

Example: policy di bucket pubbliche

In queste regole le policy di esempio seguenti sono considerate pubbliche.

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow"
}
```

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": { "StringLike": {"aws:SourceVpc": "vpc-*"}}
}
```

Queste policy possono essere modificate in non pubbliche includendo una delle chiavi di condizione elencate in precedenza, usando un valore fisso. Ad esempio, l'ultima policy indicata sopra può essere modificata in non pubblica impostando `aws:SourceVpc` su un valore fisso, come mostrato di seguito.

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": {"StringEquals": {"aws:SourceVpc": "vpc-91237329"}}
}
```

Questo esempio mostra in che modo Amazon S3 valuta una policy di bucket che contiene concessioni di accesso sia pubblico sia non pubblico.

Questo esempio mostra in che modo Amazon S3 valuta una policy del bucket che contiene concessioni di accesso sia pubblico sia non pubblico.

Supponiamo che un bucket sia associato a una policy che concede l'accesso a un set di entità principali fisse. In base alle regole descritte in precedenza, questa policy non è pubblica. Di

conseguenza, se abiliti l'impostazione `RestrictPublicBuckets`, la policy continua a essere valida come indicato, perché `RestrictPublicBuckets` si applica solo ai bucket associati a policy pubbliche. Tuttavia, se aggiungi un'istruzione pubblica alla policy, `RestrictPublicBuckets` ha effetto sul bucket. Consente solo agli amministratori del AWS servizio e agli utenti autorizzati dell'account del proprietario del bucket di accedere al bucket.

Ad esempio, supponiamo che un bucket di proprietà di "Account-1" abbia una politica che contiene quanto segue:

1. Una dichiarazione che concede l'accesso a AWS CloudTrail (che è un' AWS entità del servizio)
2. Una dichiarazione che concede l'accesso all'account "» Account-2
3. Un'istruzione che concede l'accesso al pubblico, ad esempio specificando `"Principal": "*"` senza `Condition` limitante

Questa policy viene qualificata come pubblica a causa della terza istruzione. Con questa politica in atto e `RestrictPublicBuckets` abilitata, Amazon S3 consente l'accesso solo da CloudTrail. Anche se la dichiarazione 2 non è pubblica, Amazon S3 disabilita l'accesso tramite "» Account-2. Questo perché la dichiarazione 3 rende pubblica l'intera politica, quindi si applica. `RestrictPublicBuckets`. Di conseguenza, Amazon S3 disabilita l'accesso tra account, anche se la policy delega l'accesso a un account specifico, "» Account-2. Ma se rimuovi la dichiarazione 3 dalla policy, la policy non è considerata pubblica e non si applica più. `RestrictPublicBuckets`. Pertanto, "Account-2" riottiene l'accesso al bucket, anche se lo lasci abilitato. `RestrictPublicBuckets`

Access point

Amazon S3 valuta le impostazioni di blocco dell'accesso pubblico in modo leggermente diverso per gli access point rispetto ai bucket. Le regole applicate da Amazon S3 per determinare quando una policy di un access point è pubblica sono generalmente le stesse per gli access point e per i bucket, ad eccezione delle seguenti situazioni:

- Un access point con un'origine di rete VPC è sempre considerato non pubblico, indipendentemente dal contenuto della policy di access point.
- Una policy di access point che concede l'accesso a un set di access point utilizzando `s3:DataAccessPointArn` è considerata pubblica. Tieni presente che questo comportamento è diverso rispetto alle policy di bucket. Ad esempio, una policy di bucket che concede l'accesso ai valori di `s3:DataAccessPointArn` che corrispondono a `arn:aws:s3:us-`

`west-2:123456789012:accesspoint/*` è considerata pubblica. Tuttavia, la stessa istruzione in una policy di access point renderebbe pubblico l'access point.

Utilizzo di IAM Access Analyzer per S3 per esaminare i bucket pubblici

È possibile utilizzare IAM Access Analyzer per S3 per esaminare i bucket con ACL bucket, policy di bucket o policy del punto di accesso che concedono l'accesso pubblico. IAM Access Analyzer for S3 ti avvisa dei bucket configurati per consentire l'accesso a chiunque su Internet o altro Account AWS, anche all'esterno della tua organizzazione. Account AWS Per ogni bucket pubblico o condiviso, vengono visualizzati risultati che riportano l'origine e il livello di accesso pubblico o condiviso.

In IAM Access Analyzer per S3, è possibile bloccare tutti gli accessi pubblici a un bucket con un solo clic. Inoltre, puoi eseguire il drill-down nelle impostazioni relative alle autorizzazioni a livello di bucket per configurare i livelli di accesso granulari. Per casi d'uso specifici e verificati che richiedono l'accesso pubblico o condiviso, puoi confermare e registrare l'intenzione del bucket di rimanere pubblico o condiviso archiviando i risultati per il bucket.

In rari casi, la valutazione dello strumento di analisi degli accessi IAM per S3 e del blocco dell'accesso pubblico Amazon S3 potrebbe differire a seconda che un bucket sia pubblico o meno. Questo comportamento si verifica perché il blocco dell'accesso pubblico Amazon S3 esegue la convalida dell'esistenza delle azioni oltre a valutare l'accesso pubblico. Supponi che la policy di bucket contenga un'istruzione `Action` che consenta l'accesso pubblico a un'azione non supportata da Amazon S3 (ad esempio, `s3:NotASupportedAction`). In questo caso, il blocco dell'accesso pubblico Amazon S3 valuta il bucket come pubblico perché una tale istruzione potrebbe potenzialmente renderlo pubblico se l'azione verrà successivamente supportata. Nei casi in cui il blocco dell'accesso pubblico Amazon S3 e lo strumento di analisi degli accessi AWS IAM per S3 differiscono nelle rispettive valutazioni, è consigliabile esaminare la policy di bucket e rimuovere eventuali azioni non supportate.

Per ulteriori informazioni su IAM Access Analyzer per S3, consultare [Revisione dell'accesso al bucket tramite IAM Access Analyzer per S3](#).

Permissions

Per utilizzare le caratteristiche di blocco dell'accesso pubblico di Amazon S3, sono necessarie le autorizzazioni seguenti.

Operazione	Autorizzazioni richieste
Operazione GET per lo stato della policy di bucket	s3:GetBucketPolicyStatus
Operazione GET per le impostazioni di blocco dell'accesso pubblico del bucket	s3:GetBucketPublicAccessBlock
Operazione PUT per le impostazioni di blocco dell'accesso pubblico del bucket	s3:PutBucketPublicAccessBlock
Operazione DELETE per le impostazioni di blocco dell'accesso pubblico del bucket	s3:PutBucketPublicAccessBlock
Operazione GET per le impostazioni di blocco dell'accesso pubblico dell'account	s3:GetAccountPublicAccessBlock
Operazione PUT per le impostazioni di blocco dell'accesso pubblico dell'account	s3:PutAccountPublicAccessBlock
Operazione DELETE per le impostazioni di blocco dell'accesso pubblico dell'account	s3:PutAccountPublicAccessBlock
Operazione PUT per le impostazioni di blocco dell'accesso pubblico del punto di accesso	s3:CreateAccessPoint

 Note

Per le operazioni DELETE sono necessarie le stesse autorizzazioni necessarie per le operazioni PUT. Non esistono autorizzazioni separate per le operazioni DELETE.

Configurazione del blocco dell'accesso pubblico

Per ulteriori informazioni sulla configurazione dei blocchi di accesso pubblico per i tuoi Account AWS bucket Amazon S3 e i tuoi access point, consulta i seguenti argomenti:

- [Configurazione delle impostazioni di blocco dell'accesso pubblico per l'account](#)

- [Configurazione delle impostazioni di blocco dell'accesso pubblico per i bucket S3](#)
- [Esecuzione di operazioni di accesso pubblico di blocco su un punto di accesso](#)

Configurazione delle impostazioni di blocco dell'accesso pubblico per l'account

Important

Se il tuo account è gestito da una politica di blocco dell'accesso pubblico a livello di organizzazione, non puoi modificare queste impostazioni a livello di account. Organization-level le politiche hanno la precedenza sulle configurazioni a livello di account. Per ulteriori informazioni sulle opzioni di gestione centralizzata, consulta la politica [S3 nella guida per l'utente](#). AWS Organizations

Amazon S3 Block Public Access fornisce impostazioni per punti di accesso, bucket, organizzazioni e account per aiutarti a gestire l'accesso pubblico alle risorse Amazon S3. Per impostazione predefinita, nuovi bucket, punti di accesso e oggetti non consentono l'accesso pubblico. Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Note

Le impostazioni a livello di account sostituiscono le impostazioni sui singoli oggetti. Se si configura l'account per bloccare l'accesso pubblico, le eventuali impostazioni di accesso pubblico effettuate su singoli oggetti all'interno dell'account verranno sovrascritte. Quando le policy a livello di organizzazione sono attive, le impostazioni a livello di account ereditano automaticamente dalla policy dell'organizzazione e non possono essere modificate direttamente.

Puoi utilizzare la console S3 AWS CLI, gli AWS SDK e l'API REST per configurare le impostazioni di blocco dell'accesso pubblico per tutti i bucket del tuo account quando non sono gestiti dalle politiche dell'organizzazione. Per ulteriori informazioni, consulta le sezioni seguenti.

Per configurare le impostazioni di accesso pubblico di blocco per i bucket, consulta [Configurazione delle impostazioni di blocco dell'accesso pubblico per i bucket S3](#). Per ulteriori informazioni sui punti di accesso, consulta [Esecuzione di operazioni di accesso pubblico di blocco su un punto di accesso](#).

Utilizzo della console S3

Il blocco dell'accesso pubblico di Amazon S3 impedisce l'applicazione di qualsiasi impostazione che consente l'accesso pubblico ai dati all'interno di bucket S3. In questa sezione viene descritto come modificare le impostazioni di blocco dell'accesso pubblico per tutti i bucket S3 nell' Account AWS. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Per modificare le impostazioni di accesso pubblico a blocchi per tutti i bucket S3 in un Account AWS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione, seleziona Impostazioni dell'account e dell'organizzazione.
3. In Blocca le impostazioni di accesso pubblico per questo account:
4. Scegli Modifica per modificare le impostazioni di blocco dell'accesso pubblico per tutti i bucket nell' Account AWS.
5. Scegliere le impostazione da modificare, quindi selezionare Save changes (Salva modifiche).
6. Quando viene richiesta la conferma, immettere **confirm**. Quindi scegli Confirm (Conferma) per salvare le modifiche.

Se ricevi un messaggio di errore che dice «Questo account non consente modifiche alle impostazioni di accesso pubblico di S3 Block Public Access a livello di account a causa di una politica organizzativa di blocco pubblico di S3 in vigore», il tuo account è gestito da politiche a livello di organizzazione. Contatta l'amministratore dell'organizzazione per modificare queste impostazioni.

Utilizzo di AWS CLI

È possibile utilizzare il blocco dell'accesso pubblico di Amazon S3 tramite la AWS CLI. Per ulteriori informazioni sulla configurazione e l'utilizzo di AWS CLI, vedi [What is the AWS Command Line Interface?](#)

Account

Per eseguire operazioni di blocco dell'accesso pubblico su un account, usa il servizio `s3control` di AWS CLI . Le operazioni a livello di account che usano questo servizio sono:

- `PutPublicAccessBlock` (per un account)
- `GetPublicAccessBlock` (per un account)

- DeletePublicAccessBlock (per un account)

Note

PutPublicAccessBlock e DeletePublicAccessBlock le operazioni restituiranno un errore di «Accesso negato» quando l'account è gestito da politiche a livello di organizzazione. Account-level GetPublicAccessBlock operations restituiranno la politica applicata a livello di organizzazione, se presente.

Per ulteriori informazioni ed esempi, consulta [put-public-access-block](#) nella Guida di riferimento della AWS CLI .

Utilizzo di AWS SDK

Java

Gli esempi seguenti mostrano come utilizzare Amazon S3 Block Public Access con AWS SDK per Java per inserire una configurazione di blocco di accesso pubblico su un account Amazon S3.

Note

PutPublicAccessBlock e DeletePublicAccessBlock le operazioni falliranno con un errore «Accesso negato» se l'account è gestito da policy a livello di organizzazione.

```
AWSS3ControlClientBuilder controlClientBuilder =
    AWSS3ControlClientBuilder.standard();
controlClientBuilder.setRegion(<region>);
controlClientBuilder.setCredentials(<credentials>);

AWSS3Control client = controlClientBuilder.build();
client.putPublicAccessBlock(new PutPublicAccessBlockRequest()
    .withAccountId(<account-id>)
    .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
        .withIgnorePublicAcls(<value>)
        .withBlockPublicAcls(<value>)
        .withBlockPublicPolicy(<value>)
        .withRestrictPublicBuckets(<value>)));
```

 Important

Questo esempio si applica solo alle operazioni a livello di account, che usano la classe client `AWSS3Control`. Per le operazioni a livello di bucket, consulta l'esempio precedente.

Other SDKs

Per informazioni sull'utilizzo degli altri AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Utilizzo della REST API

Per informazioni sull'uso di Blocco dell'accesso pubblico Amazon S3 attraverso le REST API, consulta i seguenti argomenti nel Riferimento API di Amazon Simple Storage Service.

- Account-level operazioni
 - [PutPublicAccessBlock](#)- Fallisce quando l'account è gestito dalle politiche dell'organizzazione
 - [GetPublicAccessBlock](#)- Restituisce una configurazione efficace, comprese le politiche dell'organizzazione.
 - [DeletePublicAccessBlock](#)- Non riesce quando l'account è gestito dalle politiche dell'organizzazione.

Verrà visualizzato il seguente messaggio di errore per le operazioni limitate: «Questo account non consente modifiche alle impostazioni di accesso pubblico di S3 Block Public Access a livello di account a causa di una politica organizzativa di S3 Block Public Access in vigore».

Configurazione delle impostazioni di blocco dell'accesso pubblico per i bucket S3

Amazon S3 Block Public Access fornisce impostazioni per punti di accesso, bucket, organizzazioni e account per aiutarti a gestire l'accesso pubblico alle risorse Amazon S3. Per impostazione predefinita, nuovi bucket, punti di accesso e oggetti non consentono l'accesso pubblico. Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

 Note

Bucket-level Le impostazioni Block Public Access funzionano insieme alle policy a livello di organizzazione e account. S3 applica l'impostazione più restrittiva tra le configurazioni a livello di bucket ed effettive a livello di account (che possono essere applicate dalle politiche dell'organizzazione, se presenti).

Puoi utilizzare la console S3, gli AWS SDK e l'API REST per AWS CLI concedere l'accesso pubblico a uno o più bucket. È anche possibile bloccare l'accesso pubblico a bucket che sono già pubblici. Per ulteriori informazioni, consulta le sezioni seguenti.

Per configurare le impostazioni Blocco dell'accesso pubblico per ogni bucket dell'account, consultare [Configurazione delle impostazioni di blocco dell'accesso pubblico per l'account](#). Per una gestione centralizzata a livello di organizzazione, consulta la policy S3 nella guida per l'utente [AWS Organizations](#)

Per informazioni sulla configurazione dell'accesso pubblico a blocchi per i punti di accesso, consulta [Esecuzione di operazioni di accesso pubblico di blocco su un punto di accesso](#).

Utilizzo della console S3

Il blocco dell'accesso pubblico Amazon S3 impedisce l'applicazione di qualsiasi impostazione che consente l'accesso pubblico ai dati all'interno dei bucket S3. In questa sezione viene descritto come modificare le impostazioni di blocco dell'accesso pubblico per uno o più bucket S3. Per informazioni sul blocco dell'accesso pubblico utilizzando gli AWS SDK e le AWS CLI API REST di Amazon S3, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#)

Puoi vedere se il bucket è accessibile pubblicamente nella colonna Analizzatore di accesso IAM dell'elenco Bucket. Per ulteriori informazioni, consulta [Revisione dell'accesso al bucket tramite IAM Access Analyzer per S3](#).

Se viene visualizzato un Error quando si elencano i bucket e le relative impostazioni di accesso pubblico, si potrebbe non disporre delle autorizzazioni richieste. Assicurarsi di disporre delle seguenti autorizzazioni aggiunte alla policy utente o del ruolo:

```
s3:GetAccountPublicAccessBlock
s3:GetBucketPublicAccessBlock
s3:GetBucketPolicyStatus
```

```
s3:GetBucketLocation  
s3:GetBucketAcl  
s3:ListAccessPoints  
s3:ListAllMyBuckets
```

In alcuni rari casi, le richieste possono anche non riuscire a causa di un'interruzione della Regione AWS .

Per modificare le impostazioni di blocco dell'accesso pubblico Amazon S3 per un singolo bucket S3

Segui questa procedura se è necessario modificare le impostazioni di accesso pubblico per un singolo bucket S3.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket name (Nome bucket), scegliere il nome del bucket desiderato.
3. Seleziona Autorizzazioni.
4. Scegli Modifica accanto a Blocco dell'accesso pubblico (impostazioni del bucket) per modificare le impostazioni di accesso pubblico per il bucket. Per maggiori informazioni sulle quattro impostazioni di blocco dell'accesso pubblico di Amazon S3, consulta [Impostazioni di blocco dell'accesso pubblico](#).
5. Scegli una delle impostazioni, quindi scegli Salva le modifiche.
6. Quando viene richiesta la conferma, immettere **confirm**. Quindi scegli Confirm (Conferma) per salvare le modifiche.

 Important

Anche se disabiliti le impostazioni di Block Public Access a livello di bucket, il bucket potrebbe comunque essere protetto da policy a livello di account o di organizzazione. S3 applica sempre la combinazione di impostazioni più restrittiva a tutti i livelli.

È possibile modificare le impostazioni di blocco dell'accesso pubblico Amazon S3 anche al momento della creazione di un bucket. Per ulteriori informazioni, consulta [Creazione di un bucket per uso generico](#).

Utilizzo di AWS CLI

Per bloccare l'accesso pubblico su un bucket o per eliminare il blocco di accesso pubblico, usa il servizio. AWS CLI s3api Le operazioni a livello di bucket che usano questo servizio sono:

- PutPublicAccessBlock (per un bucket)
- GetPublicAccessBlock (per un bucket)
- DeletePublicAccessBlock (per un bucket)
- GetBucketPolicyStatus

Per ulteriori informazioni ed esempi, consulta l'esempio [put-public-access-block](#) in Riferimento ai comandi della AWS CLI .

Note

Queste operazioni a livello di bucket non sono limitate dalle politiche a livello di organizzazione. Tuttavia, l'effettivo comportamento di accesso pubblico sarà comunque regolato dalla combinazione più restrittiva di impostazioni relative a bucket, account e organizzazione. Per ulteriori informazioni sulla gerarchia e sulle interazioni tra policy, vedere. [the section called “Modifica delle impostazioni di accesso pubblico del bucket”](#)

Utilizzo di AWS SDK

Java

```
AmazonS3 client = AmazonS3ClientBuilder.standard()
    .withCredentials(<credentials>)
    .build();

client.setPublicAccessBlock(new SetPublicAccessBlockRequest()
    .withBucketName(<bucket-name>)
    .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
        .withBlockPublicAcls(<value>)
        .withIgnorePublicAcls(<value>)
        .withBlockPublicPolicy(<value>)
        .withRestrictPublicBuckets(<value>)));
```


 Important

Questo esempio si applica solo alle operazioni a livello di bucket, che usano la classe client AmazonS3. Per le operazioni a livello di account, consulta l'esempio seguente.

Other SDKs

Per informazioni sull'utilizzo degli altri AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Utilizzo della REST API

Per informazioni sull'uso di Blocco dell'accesso pubblico Amazon S3 attraverso le REST API, consulta i seguenti argomenti nel Riferimento API di Amazon Simple Storage Service.

- Bucket-level operazioni
 - [PutPublicAccessBlock](#)
 - [GetPublicAccessBlock](#)
 - [DeletePublicAccessBlock](#)
 - [GetBucketPolicyStatus](#)

Revisione dell'accesso al bucket tramite IAM Access Analyzer per S3

IAM Access Analyzer for S3 fornisce risultati di accesso esterni per i bucket S3 generici configurati per consentire l'accesso a chiunque su Internet (pubblico) o altro Account AWS, anche Account AWS all'esterno dell'organizzazione. Per ogni bucket condiviso pubblicamente o con altri Account AWS, ricevi informazioni sulla fonte e sul livello di accesso condiviso. Ad esempio, IAM Access Analyzer for S3 potrebbe mostrare che un bucket dispone di un accesso in lettura o scrittura fornito tramite un bucket access control list (ACL), un bucket policy, un access point policy o un Multi-Region access point policy. Con questi risultati puoi intraprendere azioni correttive immediate e precise per ripristinare l'accesso del bucket desiderato.

La console Amazon S3 presenta un riepilogo degli accessi esterni nella console S3 accanto all'elenco dei bucket per uso generico. Nel riepilogo, puoi scegliere i risultati attivi per ciascuno per

Regione AWS visualizzarne i dettagli nella pagina IAM Access Analyzer for S3. Gli esiti degli accessi esterni nel riepilogo degli accessi esterni vengono aggiornati automaticamente ogni 24 ore.

Quando si esamina un bucket che consente l'accesso pubblico, nella pagina Strumento di analisi degli accessi IAM per S3 è possibile bloccare tutti gli accessi pubblici al bucket con un solo clic. È consigliabile bloccare l'accesso pubblico ai bucket, a meno che non sia necessario per supportare un caso d'uso specifico. Prima di bloccare tutti gli accessi pubblici, assicurati che le applicazioni continuino a funzionare correttamente senza accesso pubblico. Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Inoltre, puoi eseguire il drill-down nelle impostazioni relative alle autorizzazioni a livello di bucket per configurare i livelli di accesso granulari. Per casi d'uso specifici e verificati che richiedono l'accesso pubblico, ad esempio host di siti Web, download pubblici, condivisione tra account, puoi confermare e registrare l'intenzione del bucket di rimanere pubblico o condiviso archiviando i risultati per il bucket. Puoi consultare e modificare le configurazioni relative al bucket in qualsiasi momento. È inoltre possibile scaricare i risultati in un report CSV per scopi di verifica.

IAM Access Analyzer per S3 è disponibile senza costi aggiuntivi nella console di Amazon S3. IAM Access Analyzer per S3 è basato su AWS Identity and Access Management (IAM) IAM Access Analyzer. Per utilizzare lo strumento di analisi degli accessi IAM per S3 nella console Amazon S3, è necessario accedere alla console IAM e abilitare lo strumento di analisi degli accessi IAM su base regionale.

Per ulteriori informazioni su IAM Access Analyzer, consulta [Cos'è IAM Access Analyzer?](#) nella Guida all'utente IAM. Per ulteriori informazioni su IAM Access Analyzer per S3, rivedi le sezioni seguenti.

Important

- IAM Access Analyzer for S3 richiede un analizzatore a livello di account in ogni area in cui sono presenti dei bucket. Regione AWS Per utilizzare IAM Access Analyzer per S3, è necessario visitare IAM Access Analyzer e creare un analizzatore che abbia un account come zona di attendibilità. Per ulteriori informazioni, consultare [Abilitazione di IAM Access Analyzer](#) nella Guida per l'utente di IAM.
- IAM Access Analyzer per S3 non analizza la policy dei punti di accesso associata ai punti di accesso multi-account. Questo comportamento si verifica perché il punto di accesso e la relativa policy sono al di fuori della zona di attendibilità, ovvero l'account. I bucket che delegano l'accesso a un punto di accesso multi-account sono elencati in Buckets with public access (Bucket con accesso pubblico) se non hai applicato l'impostazione

`RestrictPublicBuckets` di Blocco dell'accesso pubblico Amazon S3 al bucket o all'account. Quando applichi l'impostazione di `RestrictPublicBuckets` blocco dell'accesso pubblico, il bucket viene segnalato in Bucket con accesso da altri, incluse terze parti. Account AWS Account AWS

- Quando una policy del bucket o un'ACL bucket viene aggiunta o modificata, IAM Access Analyzer genera e aggiorna i risultati in base alla modifica entro 30 minuti. I risultati relativi alle impostazioni di Blocco dell'accesso pubblico Amazon S3 a livello di account potrebbero non essere generati o aggiornati per un massimo di 6 ore dopo la modifica delle impostazioni. I risultati relativi agli Multi-Region access point potrebbero non essere generati o aggiornati per un massimo di sei ore dopo la creazione, l'eliminazione dell' Multi-Region Access Point o la modifica della sua politica.

Argomenti

- [Revisione del riepilogo globale delle policy che forniscono l'accesso esterno ai bucket](#)
- [Informazioni fornite dallo strumento di analisi degli accessi IAM per S3](#)
- [Blocco di tutti gli accessi pubblici](#)
- [Revisione e modifica dell'accesso al bucket](#)
- [Archiviazione dei risultati del bucket](#)
- [Attivazione di un risultato di bucket archiviato](#)
- [Visualizzazione dei dettagli del risultato](#)
- [Download di un report IAM Access Analyzer per S3](#)

Revisione del riepilogo globale delle policy che forniscono l'accesso esterno ai bucket

È possibile utilizzare il riepilogo degli accessi esterni per visualizzare un riepilogo globale delle policy che forniscono l'accesso esterno ai bucket dell' Account AWS direttamente dalla console S3. Questo riepilogo ti aiuta a identificare i bucket generici di Amazon S3 in quella Regione AWS che consentono l'accesso pubblico o l'accesso da altri utenti Account AWS senza dover esaminare le politiche di ciascuno singolarmente. Regione AWS

Abilitazione del riepilogo degli accessi esterni e dello strumento di analisi degli accessi IAM per S3

Per utilizzare il riepilogo degli accessi esterni e lo strumento di analisi degli accessi IAM per S3, è necessario completare le seguenti fasi.

1. Concedere le autorizzazioni richieste. Per ulteriori informazioni, consultare [Autorizzazioni necessarie per utilizzare IAM Access Analyzer](#) nella Guida per l'utente di IAM.
2. Visita IAM per creare un analizzatore a livello di account per ogni regione in cui desideri utilizzare IAM Access Analyzer.

Puoi farlo creando un analizzatore con un account come zona di fiducia nella console IAM o utilizzando gli SDK or. AWS CLI AWS Per ulteriori informazioni, consultare [Abilitazione di IAM Access Analyzer](#) nella Guida per l'utente di IAM.

Visualizzazione dei bucket che consentono l'accesso esterno

Il riepilogo degli accessi esterni mostra gli esiti e gli errori relativi all'accesso esterno forniti dallo strumento di analisi degli accessi IAM per S3 per i bucket per uso generico. Gli esiti archiviati e quelli relativi agli accessi non utilizzati non sono inclusi nel riepilogo, ma possono essere visualizzati nella console IAM o nello strumenti di analisi degli accessi IAM per S3. Per ulteriori informazioni, consulta [Visualizza la dashboard degli esiti dello strumenti di analisi degli accessi IAM](#) nella Guida per l'utente IAM.

Note

Il riepilogo dell'accesso esterno include solo i risultati degli analizzatori di accesso esterni per ciascuna organizzazione Account AWS, non per la tua organizzazione. AWS

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Bucket per uso generico.
3. Espandi il riepilogo degli accessi esterni. La console mostra gli esiti degli accessi multi-account e pubblici attivi.

 Note

Se S3 riscontra un problema durante il caricamento dei dettagli dei bucket, aggiorna l'elenco dei bucket per uso generico o visualizza gli esiti nello strumento di analisi degli accessi IAM per S3. Per ulteriori informazioni, consulta [Revisione dell'accesso al bucket tramite IAM Access Analyzer per S3](#).

4. Per visualizzare un elenco di risultati o errori relativi a un Regione AWS, scegli il link alla regione. La pagina Strumento di analisi degli accessi IAM per S3 mostra i nomi dei bucket a cui è possibile accedere pubblicamente o da altri Account AWS. Per ulteriori informazioni, consulta [Informazioni fornite dallo strumento di analisi degli accessi IAM per S3](#).

Aggiornamento dei controlli degli accessi per i bucket che consentono l'accesso esterno

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Bucket per uso generico.
3. Espandi il riepilogo degli accessi esterni. La console mostra gli esiti attivi per i bucket a cui è possibile accedere pubblicamente o da altri Account AWS.

 Note

Se S3 riscontra un problema durante il caricamento dei dettagli dei bucket, aggiorna l'elenco dei bucket per uso generico o visualizza gli esiti nello strumento di analisi degli accessi IAM per S3. Per ulteriori informazioni, consulta [Revisione dell'accesso al bucket tramite IAM Access Analyzer per S3](#).

4. Per visualizzare un elenco di risultati o errori relativi a un Regione AWS, scegli il link alla regione. Lo strumento di analisi degli accessi IAM per S3 mostra gli esiti attivi per i bucket a cui è possibile accedere pubblicamente o da altri Account AWS.

 Note

Gli esiti degli accessi esterni nel riepilogo degli accessi esterni vengono aggiornati automaticamente ogni 24 ore.

5. Per bloccare tutti gli accessi pubblici a un bucket, consulta [Blocco di tutti gli accessi pubblici](#). Per modificare l'accesso al bucket, consulta [Revisione e modifica dell'accesso al bucket](#).

Informazioni fornite dallo strumento di analisi degli accessi IAM per S3

IAM Access Analyzer per S3 fornisce risultati per i bucket a cui è possibile accedere al di fuori di Account AWS. I bucket elencati in Esiti degli accessi pubblici sono accessibili da chiunque su Internet. Se IAM Access Analyzer for S3 identifica i bucket pubblici, viene visualizzato anche un banner di avviso che mostra il numero di bucket pubblici nella tua regione. I bucket elencati nei risultati *Cross-account degli accessi* vengono condivisi condizionatamente con altri utenti Account AWS, inclusi account esterni all'organizzazione.

Per ogni bucket, IAM Access Analyzer for S3 fornisce le seguenti informazioni:

- Nome bucket
- Condiviso tramite - Come viene condiviso il bucket, tramite una policy bucket, un bucket ACL, una policy Access Point o una policy per un Multi-Region access point. Multi-Region I punti di accesso e i punti di accesso tra più account si riflettono nei punti di accesso. Un bucket può essere condiviso tramite policy e ACL. Per trovare e rivedere l'origine dell'accesso al bucket, puoi utilizzare le informazioni contenute in questa colonna come punto di partenza per intraprendere azioni correttive immediate e precise.
- Status (Stato) - Lo stato del rilevamento del bucket. IAM Access Analyzer per S3 visualizza i risultati per tutti i bucket pubblici e condivisi.
 - Active (Attivo)- Il risultato non è stato esaminato.
 - Archived (Archiviato) - Il risultato è stato esaminato e confermato come previsto.
 - Tutti - Tutti i risultati dei bucket pubblici o condivisi con altri Account AWS, anche Account AWS all'esterno dell'organizzazione.
- Access level (Livello di accesso) - Autorizzazioni di accesso concesse per il bucket:
 - List (Elenco) - Elencare le risorse.
 - Read (Lettura) - Leggere ma non modificare gli attributi e i contenuti delle risorse.
 - Write (Scrittura) - Creare, eliminare o modificare le risorse.
 - Permissions (Autorizzazioni) - Concedere o modificare le autorizzazioni a livello di risorsa.
 - Tagging (Tag) - Aggiornare i tag associati alla risorsa.
- Responsabile esterno - L' Account AWS esterno dell'organizzazione con accesso al bucket.

- **Restrizione della policy di controllo delle risorse (RCP)** - La policy di controllo delle risorse (RCP) collegata al bucket, se applicabile. Per ulteriori informazioni, consulta [Policy di controllo delle risorse \(RCP\)](#).

Blocco di tutti gli accessi pubblici

Per bloccare tutti gli accessi a un bucket con un solo clic, puoi utilizzare il pulsante **Blocca tutti gli accessi pubblici** in IAM Access Analyzer per S3. Quando blocchi tutti gli accessi pubblici a un bucket, non viene concesso alcun accesso pubblico. Ti consigliamo di bloccare tutti gli accessi pubblici ai bucket, a meno che non sia necessario l'accesso pubblico per supportare un caso d'uso specifico e verificato. Prima di bloccare tutti gli accessi pubblici, assicurati che le applicazioni continuino a funzionare correttamente senza accesso pubblico.

Se non desideri bloccare tutti gli accessi pubblici al bucket, puoi modificare le impostazioni di blocco dell'accesso pubblico sulla console di Amazon S3 per configurare livelli granulari di accesso ai bucket. Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

In rari casi, la valutazione dello strumento di analisi degli accessi IAM per S3 e del blocco dell'accesso pubblico Amazon S3 potrebbe differire a seconda che un bucket sia pubblico o meno. Questo comportamento si verifica perché il blocco dell'accesso pubblico Amazon S3 esegue la convalida dell'esistenza delle azioni oltre a valutare l'accesso pubblico. Supponi che la policy di bucket contenga un'istruzione `Action` che consenta l'accesso pubblico a un'azione non supportata da Amazon S3 (ad esempio, `s3:NotASupportedAction`). In questo caso, il blocco dell'accesso pubblico Amazon S3 valuta il bucket come pubblico perché una tale istruzione potrebbe potenzialmente renderlo pubblico se l'azione verrà successivamente supportata. Nei casi in cui il blocco dell'accesso pubblico Amazon S3 e lo strumento di analisi degli accessi AWS IAM per S3 differiscono nelle rispettive valutazioni, è consigliabile esaminare la policy di bucket e rimuovere eventuali azioni non supportate.

Per bloccare tutti gli accessi pubblici a un bucket utilizzando IAM Access Analyzer per S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, in Dashboards (Pannelli di controllo), scegliere **Access analyzer for S3** (Access Analyzer per S3).
3. In IAM Access Analyzer per S3, scegli un bucket.
4. Scegliere **Block all public access** (Blocca tutti gli accessi pubblici).

5. Per confermare l'intenzione di bloccare tutti gli accessi pubblici al bucket, in Block all public access (bucket settings) (Blocca tutti gli accessi pubblici (impostazioni bucket)), immettere **confirm**.

Amazon S3 blocca tutti gli accessi pubblici al bucket. Lo stato del risultato del bucket viene aggiornato in risolto e il bucket scompare dall'elenco di IAM Access Analyzer per S3. Se si desidera esaminare i bucket risolti, aprire IAM Access Analyzer nella [console IAM](#).

Revisione e modifica dell'accesso al bucket

Se non intendevi concedere l'accesso al pubblico o ad altri account Account AWS, compresi gli account esterni alla tua organizzazione, puoi modificare l'ACL del bucket, la policy del bucket, la policy dell' Multi-Region Access Point o la policy del punto di accesso per rimuovere l'accesso al bucket. La colonna Shared through mostra tutte le fonti di accesso al bucket: bucket policy, bucket ACL, access point policy. and/or Multi-Region I punti di accesso e i punti di accesso tra più account si trovano sotto i punti di accesso.

Per rivedere e modificare una policy bucket, un bucket ACL, un Access Point o una policy per un Multi-Region access point

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione scegliere Access analyzer for S3 (Access Analyzer per S3).
3. Per vedere se l'accesso pubblico o l'accesso condiviso è concesso tramite una policy bucket, un bucket ACL, una policy Multi-Region Access Point o una policy per un access point, consulta la colonna Shared through.
4. In Buckets, scegli il nome del bucket con la policy bucket, il bucket ACL, la policy Multi-Region Access Point o la policy del punto di accesso che desideri modificare o rivedere.
5. Se si desidera modificare o visualizzare una ACL di bucket:
 - a. Seleziona Autorizzazioni.
 - b. Scegliere Access Control List (Lista di controllo accessi).
 - c. Esaminare l'ACL di bucket e apportare le modifiche necessarie.

Per ulteriori informazioni, consulta [Configurazione delle ACL](#).

6. Se si desidera modificare o rivedere una policy di bucket:
 - a. Seleziona Autorizzazioni.

- b. Scegli Bucket Policy (Policy del bucket).
- c. Esaminare o modificare la policy di bucket come richiesto.

Per ulteriori informazioni, consulta [Aggiunta di una policy di bucket utilizzando la console di Amazon S3](#).

7. Se desideri modificare o visualizzare una politica di Access Point: Multi-Region
- a. Scegli Multi-Region Access Point.
 - b. Scegli il nome del punto di Multi-Region accesso.
 - c. Rivedi o modifica la politica dell' Multi-Region Access Point come richiesto.

Per ulteriori informazioni, consulta [Permissions](#).

8. Se si desidera rivedere o modificare una policy del punto di accesso:
- a. Scegli Punti di accesso per bucket per uso generico o Punti di accesso per bucket di directory.
 - b. Scegliere il nome del punto di accesso.
 - c. Esaminare o modificare l'accesso in base alle esigenze.

Per ulteriori informazioni, consulta [Gestione dei punti di accesso Amazon S3 per bucket per uso generico](#).

Se si modifica o si rimuove una ACL di bucket, una policy di bucket o una policy del punto di accesso per rimuovere l'accesso pubblico o condiviso, lo stato dei risultati del bucket viene aggiornato in resolved (risolto). I risultati dei bucket risolti scompaiono dall'elenco di IAM Access Analyzer for S3, ma è possibile visualizzarli in IAM Access Analyzer.

Archiviazione dei risultati del bucket

Se un bucket concede l'accesso al pubblico o ad altri utenti Account AWS, inclusi account esterni all'organizzazione, per supportare un caso d'uso specifico (ad esempio, un sito Web statico, download pubblici o condivisione tra account), puoi archiviare i risultati per il bucket. Quando archivi i risultati del bucket, confermi e registri l'intenzione che il bucket rimanga pubblico o condiviso. I risultati del bucket archiviati rimangono nell'elenco di IAM Access Analyzer per S3 in modo da sapere sempre quali bucket sono pubblici o condivisi.

Per archiviare i risultati del bucket in IAM Access Analyzer per S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione scegli Analizzatore di accesso IAM per S3.
3. In IAM Access Analyzer per S3, scegli un bucket attivo.
4. Per confermare la tua intenzione di consentire l'accesso a questo bucket da parte del pubblico o di altro tipo Account AWS, inclusi gli account esterni alla tua organizzazione, scegli Archive.
5. Immettere **confirm** e scegliere Archive (Archivia).

Attivazione di un risultato di bucket archiviato

Dopo aver archiviato i risultati, è sempre possibile esaminarli e modificarne lo stato attivo, indicando che il bucket richiede un'altra revisione.

Per attivare un risultato di bucket archiviato in IAM Access Analyzer per S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione scegliere Access analyzer for S3 (Access Analyzer per S3).
3. Scegliere i risultati del bucket archiviati.
4. Scegliere Mark as active (Contrassegna come attivo).

Visualizzazione dei dettagli del risultato

Se è necessario visualizzare ulteriori informazioni su un esito, è possibile aprire i dettagli dell'esito del bucket nello strumento di analisi degli accessi IAM sulla [console IAM](#).

Per visualizzare i dettagli dei risultati in IAM Access Analyzer per S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione scegliere Access analyzer for S3 (Access Analyzer per S3).
3. In IAM Access Analyzer per S3, scegli un bucket.
4. Seleziona View Details (Visualizza dettagli).

I dettagli della ricerca si aprono in IAM Access Analyzer sulla [console IAM](#).

Download di un report IAM Access Analyzer per S3

Puoi scaricare i risultati del bucket come report CSV che è possibile utilizzare per scopi di audit. Il report include le stesse informazioni visualizzate in IAM Access Analyzer per S3 sulla console di Amazon S3.

Per scaricare un report

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra scegliere Access analyzer for S3 (Access Analyzer per S3).
3. Nel filtro Region (Regione) scegliere Region (Regione).

IAM Access Analyzer per S3 viene aggiornato per mostrare i bucket per la regione scelta.

4. Scegliere Download report (Scarica report).

Un report CSV viene generato e salvato sul computer.

Verifica della proprietà del bucket con condizione del proprietario del bucket

La condizione di proprietario del bucket Amazon S3 garantisce che i bucket utilizzati nelle operazioni S3 appartengano a quelli previsti. Account AWS

La maggior parte delle operazioni S3 legge da o scrive in bucket S3 specifici. Queste operazioni includono il caricamento, la copia e il download di oggetti, il recupero o la modifica delle configurazioni dei bucket e il recupero o la modifica delle configurazioni degli oggetti. Quando esegui queste operazioni, specifichi il bucket da utilizzare includendo il suo nome nella richiesta. Ad esempio, per recuperare un oggetto da S3, effettui una richiesta che specifica il nome di un bucket e la chiave oggetto da recuperare da quel bucket.

Poiché Amazon S3 identifica i bucket in base ai loro nomi, un'applicazione che utilizza un nome bucket non corretto in una richiesta potrebbe accidentalmente eseguire operazioni su un bucket diverso da quello previsto. Per evitare interazioni del bucket involontarie in situazioni come questa, puoi utilizzare la condizione proprietario del bucket. La condizione proprietario del bucket consente di verificare che il bucket di destinazione sia di proprietà dell' Account AWS previsto, fornendo un ulteriore livello di garanzia sul fatto che le operazioni S3 avranno gli effetti desiderati.

Argomenti

- [Quando utilizzare la condizione proprietario del bucket](#)
- [Verifica del proprietario del bucket](#)
- [Esempi](#)
- [Restrizioni e limitazioni](#)

Quando utilizzare la condizione proprietario del bucket

È consigliabile utilizzare la condizione proprietario del bucket ogni volta che esegui un'operazione S3 supportata e conosci l'ID account del proprietario del bucket previsto. La condizione proprietario del bucket è disponibile per tutte le operazioni oggetto S3 e la maggior parte delle operazioni bucket S3. Per un elenco delle operazioni S3 che non supportano la condizione proprietario del bucket, consulta [Restrizioni e limitazioni](#).

Per vedere i vantaggi dell'utilizzo della condizione di proprietario del bucket, considera il seguente scenario che coinvolge il cliente Bea: AWS

1. Bea sviluppa un'applicazione che utilizza Amazon S3. Durante lo sviluppo, Bea utilizza solo i test Account AWS per creare un bucket denominato `bea-data-test` e configura la sua applicazione a cui effettuare richieste. `bea-data-test`
2. Bea distribuisce la sua applicazione, ma dimentica di riconfigurarla affinché utilizzi un bucket nel suo Account AWS di produzione.
3. In produzione, l'applicazione di Bea effettua richieste a `bea-data-test`, che hanno esito positivo. In questo modo i dati di produzione vengono scritti nel bucket nell'account di test di Bea.

Bea può prevenire situazioni come questa utilizzando la condizione proprietario del bucket. Con la condizione di proprietario del bucket, Bea può includere l' Account AWS ID del proprietario previsto del bucket nelle sue richieste. Amazon S3 controlla quindi l'ID account del proprietario del bucket prima di elaborare ogni richiesta. Se il proprietario del bucket effettivo non corrisponde al proprietario del bucket previsto, la richiesta ha esito negativo.

Se Bea utilizza la condizione proprietario del bucket, lo scenario descritto in precedenza non comporta la scrittura accidentale dell'applicazione di Bea in un bucket di test. Invece, le richieste effettuate dall'applicazione nella fase 3 avranno esito negativo con un messaggio di errore `Access Denied`. Utilizzando la condizione proprietario del bucket, Bea aiuta a eliminare il rischio di interagire accidentalmente con i bucket nell' Account AWS sbagliato.

Verifica del proprietario del bucket

Per utilizzare la condizione proprietario del bucket, includi nella richiesta un parametro che specifichi il proprietario del bucket previsto. La maggior parte delle operazioni S3 coinvolge solo un singolo bucket e richiede solo questo singolo parametro per utilizzare la condizione proprietario del bucket. Per le operazioni CopyObject, questo primo parametro specifica il proprietario previsto del bucket di destinazione e viene incluso un secondo parametro per specificare il proprietario previsto del bucket di origine.

Quando effettui una richiesta che include un parametro della condizione proprietario del bucket, S3 controlla l'ID account del proprietario del bucket rispetto al parametro specificato prima di elaborare la richiesta. Se il parametro corrisponde all'ID account del proprietario del bucket, S3 elabora la richiesta. Se il parametro non corrisponde all'ID account del proprietario del bucket, la richiesta ha esito negativo con un messaggio di errore Access Denied.

Puoi utilizzare la condizione di proprietario del bucket con AWS Command Line Interface (AWS CLI), AWS SDK e le API REST di Amazon S3. Quando usi la condizione bucket owner con le API REST di Amazon S3 AWS CLI e Amazon S3, utilizza i seguenti nomi di parametro.

Metodo di accesso	Parametro per operazioni di non copia	Parametro origine operazione di copia	Parametro destinazione operazione di copia
AWS CLI	--expected-bucket-owner	--expected-source-bucket-owner	--expected-bucket-owner
REST API di Amazon S3	x-amz-expected-bucket-owner Intestazione	x-amz-source-expected-bucket-owner Intestazione	x-amz-expected-bucket-owner Intestazione

I nomi dei parametri necessari per utilizzare la condizione proprietario del bucket con gli SDK AWS variano a seconda della lingua. Per determinare i parametri richiesti, consulta la documentazione SDK relativa alla lingua desiderata. È possibile trovare la documentazione SDK in [Strumenti per creare in AWS](#).

Esempi

Gli esempi seguenti mostrano come è possibile implementare la condizione di proprietario del bucket in Amazon S3 utilizzando o. AWS CLI AWS SDK for Java 2.x

Example

Esempio: caricare un oggetto

Nell'esempio seguente viene mostrato il caricamento di un oggetto nel bucket S3 *amzn-s3-demo-bucket1*, utilizzando la condizione di proprietario del bucket per assicurarsi che *amzn-s3-demo-bucket1* sia di proprietà dell' Account AWS 111122223333.

AWS CLI

```
aws s3api put-object \
    --bucket amzn-s3-demo-bucket1 --key exampleobject --
body example_file.txt \
    --expected-bucket-owner 111122223333
```

AWS SDK for Java 2.x

```
public void putObjectExample() {
    S3Client s3Client = S3Client.create();
    PutObjectRequest request = PutObjectRequest.builder()
        .bucket("amzn-s3-demo-bucket1")
        .key("exampleobject")
        .expectedBucketOwner("111122223333")
        .build();
    Path path = Paths.get("example_file.txt");
    s3Client.putObject(request, path);
}
```

Example

Esempio: copiare un oggetto

Nell'esempio seguente viene mostrata la copia di un oggetto *object1* dal bucket S3 *amzn-s3-demo-bucket1* nel bucket S3 *amzn-s3-demo-bucket2*. Utilizza la condizione proprietario del bucket per garantire che i bucket sono di proprietà degli account previsti secondo la tabella seguente.

Bucket	Proprietario previsto
<i>amzn-s3-demo-bucket1</i>	111122223333
<i>amzn-s3-demo-bucket2</i>	444455556666

AWS CLI

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/object1 \  
                        --bucket amzn-s3-demo-bucket2 --key object1copy \  
                        --expected-source-bucket-owner 111122223333 --expected-  
bucket-owner 444455556666
```

AWS SDK for Java 2.x

```
public void copyObjectExample() {  
    S3Client s3Client = S3Client.create();  
    CopyObjectRequest request = CopyObjectRequest.builder()  
        .copySource("amzn-s3-demo-bucket1/object1")  
        .destinationBucket("amzn-s3-demo-bucket2")  
        .destinationKey("object1copy")  
        .expectedSourceBucketOwner("111122223333")  
        .expectedBucketOwner("444455556666")  
        .build();  
    s3Client.copyObject(request);  
}
```

Example

Esempio: recuperare una policy del bucket

Nell'esempio seguente viene recuperata la policy di accesso per il bucket S3 *amzn-s3-demo-bucket1*, utilizzando la condizione proprietario del bucket per assicurarsi che *amzn-s3-demo-bucket1* sia di proprietà dell'account Account AWS 111122223333.

AWS CLI

```
aws s3api get-bucket-policy --bucket amzn-s3-demo-bucket1 --expected-bucket-  
owner 111122223333
```

AWS SDK for Java 2.x

```
public void getBucketPolicyExample() {
    S3Client s3Client = S3Client.create();
    GetBucketPolicyRequest request = GetBucketPolicyRequest.builder()
        .bucket("amzn-s3-demo-bucket1")
        .expectedBucketOwner("111122223333")
        .build();

    try {
        GetBucketPolicyResponse response = s3Client.getBucketPolicy(request);
    }
    catch (S3Exception e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    }
}
```

Restrizioni e limitazioni

La condizione proprietario del bucket Amazon S3 presenta le seguenti restrizioni e limitazioni:

- Il valore del parametro della condizione del proprietario del bucket deve essere un Account AWS ID (valore numerico a 12 cifre). I principali del servizio non sono supportati.
- La condizione di proprietario del bucket non è disponibile per [CreateBucket](#) nessuna delle operazioni incluse in S3 Control. [ListBuckets](#) [AWS](#) Amazon S3 ignora tutti i parametri delle condizioni proprietario del bucket inclusi nelle richieste a queste operazioni.
- La condizione proprietario del bucket verifica solo che l'account specificato nel parametro di verifica possieda il bucket. La condizione proprietario del bucket non controlla la configurazione del bucket. Inoltre, non garantisce che la configurazione del bucket soddisfi condizioni specifiche o corrisponda a qualsiasi stato passato.

Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le [liste di](#)

[controllo degli accessi \(ACL\)](#). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le ACL sono disabilitate. Quando le ACL sono disabilitate, il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte dei casi d'uso moderni in Amazon S3 non richiede più l'uso di ACL ed è consigliabile mantenere le ACL disabilitate tranne in circostanze in cui è necessario controllare l'accesso individualmente per ciascun oggetto. Con le ACL disabilitate, puoi utilizzare le policy per controllare più facilmente l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket.

Object Ownership ha tre impostazioni che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e disabilitare o abilitare le ACL:

ACL disabilitate

- Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket possiede automaticamente e ha il controllo completo di ogni oggetto nel bucket. Le ACL non influiscono più sulle autorizzazioni per i dati nel bucket S3. Il bucket utilizza le policy per definire il controllo degli accessi.

ACL abilitate

- Proprietario del bucket preferito - Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono sul bucket con l'ACL `bucket-owner-full-control` predefinita.
- Object writer – L' Account AWS che carica un oggetto lo possiede, ne ha il pieno controllo e può concedere ad altri utenti l'accesso tramite ACL.

Per la maggior parte dei casi d'uso moderni in S3, è consigliabile mantenere le ACL disabilitate applicando l'impostazione Proprietario del bucket applicato e utilizzando la policy del bucket per condividere i dati con utenti esterni all'account in base alle esigenze. Questo approccio semplifica la gestione delle autorizzazioni. È possibile disabilitare le ACL su bucket appena creati e già esistenti. Per i bucket appena creati, le ACL sono disabilitate per impostazione predefinita. Nel caso di un bucket esistente che contiene già oggetti, dopo aver disabilitato le ACL, le ACL oggetto e bucket non faranno più parte di una valutazione dell'accesso, che verrà concesso o negato sulla base delle policy. Per i bucket esistenti, è possibile riattivare le ACL in qualsiasi momento dopo averle disabilitate e le ACL bucket e oggetto preesistenti verranno ripristinate.

Prima di disabilitare le ACL, ti consigliamo di rivedere la policy del bucket per assicurarti che copra tutti i modi in cui intendi concedere l'accesso al tuo bucket al di fuori del tuo account. Dopo aver disabilitato le ACL, il bucket accetta solo le richieste PUT che non specificano una ACL o le richieste PUT con ACL di controllo completo del proprietario del bucket, ad esempio la ACL predefinita `bucket-owner-full-control` o forme equivalenti di questa ACL espresse in XML. Le applicazioni esistenti che supportano gli ACL con controllo completo da parte del proprietario del bucket non subiscono alcun impatto. PUT le richieste che contengono altri ACL (ad esempio, concessioni personalizzate a determinati ACL Account AWS) hanno esito negativo e restituiscono un 400 errore con il codice di errore. `AccessControlListNotSupported`

Al contrario, un bucket con l'impostazione `Bucket owner preferred` continua ad accettare e rispettare le ACL di bucket e oggetti. Con questa impostazione, nuovi oggetti scritti con l'ACL predefinita `bucket-owner-full-control` saranno automaticamente di proprietà del proprietario del bucket anziché dell'object writer. Tutti gli altri comportamenti ACL rimangono validi. Per richiedere a tutte le operazioni PUT di Amazon S3 di includere l'ACL predefinita `bucket-owner-full-control`, puoi [aggiungere una policy di bucket](#) che consenta solo il caricamento di oggetti utilizzando questa ACL.

Per vedere quali impostazioni di Object Ownership vengono applicate ai tuoi bucket, puoi utilizzare i parametri di Amazon S3 Storage Lens. S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti. Per ulteriori informazioni, consulta la sezione relativa all'[utilizzo di S3 Storage Lens per trovare le impostazioni di Object Ownership](#).

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Impostazioni di Object Ownership

Questa tabella mostra l'impatto di ogni impostazione Object Ownership su ACL, oggetti, proprietà di oggetti e caricamenti di oggetti.

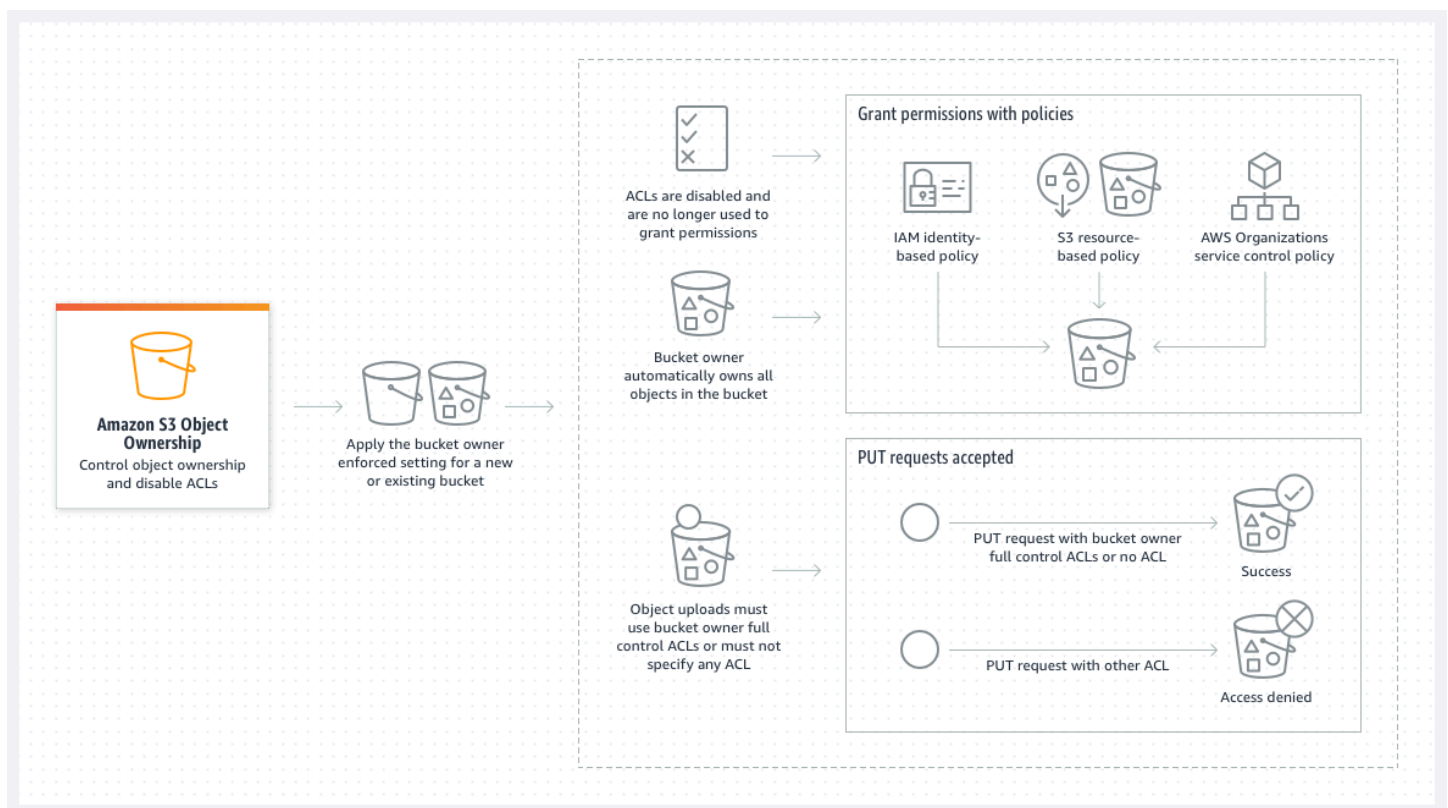
Impostazione	Si applica a	Effetto sulla proprietà degli oggetti	Effetto sulle ACL	Caricamenti accettati
Proprietario del bucket applicato (impostazione predefinita)	Tutti gli oggetti esistenti e nuovi	Il proprietario del bucket possiede ogni oggetto.	<p>Le ACL sono disabilite e non influiscono più sulle autorizzazioni di accesso al bucket. Le richieste di impostazione o aggiornamento delle ACL sono respinte. Tuttavia, sono supportate le richieste di lettura delle ACL.</p> <p>Il proprietario del bucket ha piena proprietà e controllo.</p> <p>L'object Writer non ha più piena proprietà e controllo.</p>	Caricamenti con ACL a controllo completo del proprietario del bucket o caricamenti che non specificano un'ACL
Proprietario del bucket preferito	Nuovi oggetti	Se un caricamento di oggetti include l'ACL preferita <code>bucket-owner-full-control</code> , il	Le ACL possono essere aggiornate e possono concedere autorizzazioni.	Tutti i caricamenti

Impostazione	Si applica a	Effetto sulla proprietà degli oggetti	Effetto sulle ACL	Caricamenti accettati
		<p>proprietario del bucket possiede l'oggetto.</p> <p>Gli oggetti caricati con altre ACL sono di proprietà dell'account di scrittura.</p>	<p>Se un caricamento di oggetti include l'ACL preferita <code>bucket-owner-full-control</code>, il proprietario del bucket ha completo controllo degli accessi mentre l'object writer non lo ha più.</p>	
Autore dell'oggetto	Nuovi oggetti	L'object writer è proprietario dell'oggetto.	<p>Le ACL possono essere aggiornate e possono concedere autorizzazioni.</p> <p>L'Object writer ha completo controllo degli accessi.</p>	Tutti i caricamenti

Modifiche introdotte disabilitando le ACL

Quando si applica l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, le ACL vengono disabilitate e l'utente dispone automaticamente e acquisisce il controllo completo di tutti gli oggetti nel bucket senza eseguire alcuna azione aggiuntiva. Proprietario del bucket applicato è l'impostazione predefinita per tutti i nuovi bucket creati. Dopo aver applicato l'impostazione Proprietario del bucket applicato, verranno visualizzate tre modifiche:

- Tutte le ACL dei bucket e le ACL degli oggetti sono disabilitate, il che ti dà pieno accesso in quanto proprietario del bucket. Quando esegui una richiesta ACL di lettura sul bucket o sull'oggetto, vedrai che l'accesso completo è dato solo al proprietario del bucket.
- In quanto proprietario del bucket possiedi automaticamente e hai il pieno controllo su ogni oggetto nel bucket.
- Le ACL non influiscono più sulle autorizzazioni di accesso al bucket. Di conseguenza, il controllo degli accessi ai dati si basa su policy, come le policy basate sull'[identità AWS Identity and Access Management \(IAM\)](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_rcps.html), le policy sui bucket di Amazon S3, le policy sugli endpoint VPC e le policy di controllo dei [servizi \(SCP\) delle organizzazioni](#) o le politiche di controllo delle risorse (RCP).
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_rcps.html



Se si utilizza il controllo delle versioni di S3, il proprietario del bucket possiede e ha il pieno controllo su tutte le versioni degli oggetti nel bucket. L'applicazione dell'impostazione Proprietario del bucket applicato non aggiunge una nuova versione di un oggetto.

I nuovi oggetti possono essere caricati nel bucket solo se utilizzano ACL a controllo completo del proprietario del bucket o non specificano un'ACL. I caricamenti di oggetti non riescono se specificano altre ACL. Per ulteriori informazioni, consulta [Risoluzione dei problemi](#).

Dal momento che la seguente operazione esemplificativa `PutObject` che utilizza la AWS Command Line Interface (AWS CLI) include l'ACL predefinita `bucket-owner-full-control`, l'oggetto può essere caricato in un bucket con ACL disabilitate.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file --acl bucket-owner-full-control
```

Dal momento che la seguente operazione `PutObject` non specifica un'ACL, avrà esito positivo anche per un bucket con ACL disabilitate.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file
```

Note

Se altri Account AWS hanno bisogno di accedere agli oggetti dopo il caricamento, devi concedere autorizzazioni aggiuntive a tali account tramite le politiche dei bucket. Per ulteriori informazioni, consulta [Passaggi che utilizzano le policy per gestire l'accesso alle risorse Amazon S3](#).

Re-enabling ACL

È possibile riabilitare le ACL passando dall'impostazione Proprietario del bucket applicato a un'altra impostazione di Proprietà dell'oggetto in qualsiasi momento. Se ACL oggetto sono state utilizzate per la gestione delle autorizzazioni prima di applicare l'impostazione Proprietario del bucket applicato e non è stata eseguita la migrazione delle autorizzazioni ACL dell'oggetto alla policy del bucket, dopo che le ACL vengono riabilite, queste autorizzazioni verranno ripristinate. Inoltre, gli oggetti scritti nel bucket mentre era applicata l'impostazione Proprietario del bucket applicato, appartengono ancora al proprietario del bucket.

Ad esempio, se passi dall'impostazione Proprietario del bucket applicato all'impostazione Autore dell'oggetto, in qualità di proprietario del bucket, non disporrai più della proprietà e del controllo completo sugli oggetti che appartenevano in precedenza ad altri Account AWS. Al contrario, gli account di caricamento possiederanno nuovamente questi oggetti. Gli oggetti di proprietà di altri account utilizzano le ACL per le autorizzazioni, quindi non è possibile utilizzare le policy per concedere autorizzazioni a questi oggetti. Tuttavia, in qualità di proprietario del bucket, sei ancora il proprietario di tutti gli oggetti che sono stati scritti nel bucket mentre era applicata l'impostazione

Proprietario del bucket applicato. Questi oggetti non sono di proprietà dell'object writer, anche se le ACL vengono riabilitate.

Per istruzioni su come abilitare e gestire gli ACL utilizzando Console di gestione AWS, AWS Command Line Interface (CLI), API REST o AWS SDK, consulta. [Configurazione delle ACL](#)

Prerequisiti per la disabilitazione delle ACL

Prima di disabilitare le ACL per un bucket esistente, è necessario soddisfare i seguenti prerequisiti.

- [Esamina le ACL di bucket e oggetti e migra le autorizzazioni ACL](#)
- [Identifica tutte le richieste che richiedono una ACL per l'autorizzazione](#)
- [Rivedi e aggiorna le policy dei bucket che utilizzano chiavi di condizione ACL-related](#)

Autorizzazioni di Object Ownership

Per applicare, aggiornare o eliminare un'impostazione di Object Ownership per un bucket, è necessaria l'autorizzazione `s3:PutBucketOwnershipControls`. Per restituire l'impostazione Object Ownership per un bucket, è necessaria l'autorizzazione `s3:GetBucketOwnershipControls`. Per ulteriori informazioni, consulta [Impostazione di Object Ownership quando si crea un bucket](#) e [Visualizzare l'impostazione di Object Ownership per un bucket S3](#).

Disabilitare le ACL per tutti i nuovi bucket

Per impostazione predefinita, tutti i nuovi bucket vengono creati con l'impostazione Proprietario del bucket applicato applicata e le ACL sono disabilite. È consigliabile mantenere le ACL disabilite. Come regola generale, è consigliabile utilizzare policy basate sulle risorse S3 (policy di bucket e policy dei punti di accesso) o policy IAM per il controllo degli accessi anziché ACL. Le policy sono un'opzione di controllo degli accessi semplificata e più flessibile. Con le policy dei bucket e le policy dei punti di accesso, puoi definire le regole applicabili globalmente a tutte le richieste alle risorse Amazon S3.

Replication e Object Ownership

Quando si utilizza la replica S3 e i bucket di origine e destinazione sono di proprietà diverse Account AWS, è possibile disabilitare gli ACL (impostando al proprietario del bucket l'impostazione Object Ownership) per modificare la proprietà della replica con quella proprietaria del bucket di destinazione. Account AWS Questa impostazione imita il comportamento di sovrascrittura del proprietario esistente senza la necessità di un'autorizzazione `s3:ObjectOwnerOverrideToBucketOwner`. Tutti gli oggetti replicati nel bucket di destinazione con l'impostazione Proprietario del bucket applicato sono di proprietà del proprietario del bucket di destinazione. Per ulteriori informazioni sull'opzione di sovrascrittura del proprietario per le configurazioni di replica, consulta [Modifica del proprietario della replica](#).

Impostazione di Object Ownership

Puoi applicare un'impostazione di Object Ownership utilizzando la console Amazon S3, gli AWS SDK AWS CLI, l'API REST di Amazon S3 o AWS CloudFormation L'API e i AWS CLI comandi REST seguenti supportano la proprietà degli oggetti:

REST API	AWS CLI	Description
PutBucketOwnershipControls	put-bucket-ownership-controls	Crea o modifica l'impostazione Object Ownership per un bucket S3 esistente.
CreateBucket	create-bucket	Crea un bucket tramite l'intestazione <code>x-amz-object-ownership</code> della richiesta per specificare l'impostazione Object Ownership.
GetBucketOwnershipControls	get-bucket-ownership-controls	Recupera l'impostazione Object Ownership per un bucket Amazon S3.
DeleteBucketOwnershipControls	delete-bucket-ownership-controls	Elimina l'impostazione Object Ownership per un bucket Amazon S3.

Per ulteriori informazioni sull'applicazione e l'utilizzo delle impostazioni di Object Ownership, consultare gli argomenti riportati di seguito.

Argomenti

- [Prerequisiti per la disabilitazione delle ACL](#)
- [Impostazione di Object Ownership quando si crea un bucket](#)
- [Impostazione di Object Ownership su un bucket esistente](#)
- [Visualizzare l'impostazione di Object Ownership per un bucket S3](#)
- [Disabilitare le ACL per tutti i nuovi bucket e applicare Object Ownership](#)
- [Risoluzione dei problemi](#)

Prerequisiti per la disabilitazione delle ACL

Un bucket access control list (ACL) in Amazon S3 è un meccanismo che consente di definire autorizzazioni granulari per singoli oggetti all'interno di un bucket S3, specificando quali AWS account o gruppi possono accedere e modificare tali oggetti. La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. Ti consigliamo di utilizzare le policy AWS Identity and Access Management (IAM) e bucket per gestire l'accesso e mantenere gli ACL disattivati, tranne nei casi in cui è necessario controllare l'accesso per ogni oggetto individualmente.

Se le ACL sono già abilitate nel bucket, prima di disabilitarle, verifica i seguenti prerequisiti:

Argomenti

- [Esamina le ACL di bucket e oggetti e migra le autorizzazioni ACL](#)
- [Identifica tutte le richieste che richiedono una ACL per l'autorizzazione](#)
- [Rivedi e aggiorna le policy dei bucket che utilizzano chiavi di condizione ACL-related](#)
- [Casi d'uso di esempio](#)

Esamina le ACL di bucket e oggetti e migra le autorizzazioni ACL

Quando si disattivano le ACL, le autorizzazioni concesse dalle ACL di bucket e oggetti non influiranno più sull'accesso. Prima di disabilitare le ACL, rivedere le ACL bucket e oggetto.

Ciascuna delle ACL di bucket e di oggetti esistenti ha un equivalente in una policy IAM. I seguenti esempi di policy di bucket mostrano come le autorizzazioni READ e WRITE per le ACL di bucket e di oggetti sono associate alle autorizzazioni IAM. Per ulteriori informazioni su come ogni ACL si traduce

in autorizzazioni IAM, consulta [Mappatura delle autorizzazioni ACL e delle autorizzazioni della policy di accesso](#).

Prima di disabilitare le ACL:

- Se l'ACL del bucket consente l'accesso al di fuori del tuo AWS account, devi innanzitutto migrare le autorizzazioni ACL del bucket alla tua policy del bucket.
- Quindi, ripristina l'ACL del bucket sull'ACL privata predefinita.
- È inoltre consigliabile rivedere le autorizzazioni ACL a livello di oggetto e di migrarle nella policy di bucket.

Se le ACL del bucket forniscono autorizzazioni di lettura o scrittura ad altri utenti esterni all'account, prima di poter disabilitare le ACL è necessario migrare tali autorizzazioni nella policy di bucket. Dopo aver migrato queste autorizzazioni, è possibile impostare Proprietà dell'oggetto sull'impostazione Proprietario del bucket applicato. Se non esegui la migrazione delle ACL del bucket che concedono l'accesso in lettura o scrittura al di fuori del tuo account, la richiesta di applicare l'impostazione Proprietario del bucket applicato non va a buon fine e restituisce il codice di errore [InvalidBucketAclWithObjectOwnership](#).

Se l'ACL del bucket concede l'accesso al di fuori del tuo Account AWS, prima di disabilitare gli ACL, devi migrare le autorizzazioni ACL del bucket alla tua policy del bucket e reimpostare l'ACL del bucket all'ACL privato predefinito. Se non si esegue la migrazione e il ripristino, la richiesta di applicare l'impostazione Proprietario del bucket applicato per disabilitare le ACL non riesce e restituisce il codice di errore [InvalidBucketAclWithObjectOwnership](#). Ti consigliamo inoltre di rivedere le autorizzazioni ACL dell'oggetto e di migrarle alla policy di bucket.

Per esaminare e migrare le autorizzazioni ACL alle policy di bucket, consultare i seguenti argomenti.

Argomenti

- [Esempi di policy di bucket](#)
- [Utilizzo della console S3 per esaminare e migrare le autorizzazioni ACL](#)
- [Utilizzo di AWS CLI per esaminare e migrare le autorizzazioni ACL](#)

Esempi di policy di bucket

Questi esempi di policy bucket mostrano come READ migrare le autorizzazioni ACL di una terza parte a una bucket policy. WRITE Account AWS READ_ACP e WRITE_ACP gli ACL sono meno

rilevanti per le policy perché concedono le ACL-related autorizzazioni (., e). s3:GetBucketAcl
s3:GetObjectAcl s3:PutBucketAcl s3:PutObjectAcl

Example— LEGGI ACL per un bucket

Se il tuo bucket ha un READ ACL che concede l' Account AWS **111122223333** autorizzazione per elencare i contenuti del tuo bucket, puoi scrivere una policy per il bucket che s3:ListBucket conceda,, le autorizzazioni per il tuo bucket. s3:ListBucketVersions
s3:ListBucketMultipartUploads

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Permission to list the objects in a bucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

Example— LEGGI gli ACL per ogni oggetto in un bucket

Se ogni oggetto del bucket ha un READ ACL che concede l'accesso a Account AWS **111122223333**, puoi scrivere una policy del bucket che conceda s3:GetObject e s3:GetObjectVersion autorizzazioni a questo account per ogni oggetto nel tuo bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Read permission for every object in a bucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}
```

Questo elemento di risorsa esemplificativo consente l'accesso a un oggetto specifico.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

Example— WRITE ACL che concede le autorizzazioni per scrivere oggetti in un bucket

Se il tuo bucket ha un WRITE ACL che concede Account AWS **111122223333** il permesso di scrivere oggetti nel tuo bucket, puoi scrivere una policy per il bucket che concede l'autorizzazione per il tuo bucket. `s3:PutObject`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Permission to write objects to a bucket",
      "Effect": "Allow",
```

```
"Principal": {
  "AWS": [
    "arn:aws:iam::111122223333:root"
  ],
  "Action": [
    "s3:PutObject"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
}
]
```

Utilizzo della console S3 per esaminare e migrare le autorizzazioni ACL

Per esaminare le autorizzazioni ACL di un bucket

1. Accedi e apri la console Amazon S3 all' Console di gestione AWS indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket, seleziona il nome del bucket.
3. Scegli la scheda Autorizzazioni.
4. Alla voce Lista di controllo accessi (ACL), controlla le autorizzazioni ACL del bucket.

Per esaminare le autorizzazioni ACL di un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket), scegli il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti scegli il nome dell'oggetto.
4. Scegli la scheda Autorizzazioni.
5. Alla voce Lista di controllo accessi (ACL), controlla le autorizzazioni ACL dell'oggetto.

Per migrare le autorizzazioni ACL e aggiornare l'ACL del bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket, seleziona il nome del bucket.

3. Nella sezione Autorizzazioni, alla voce Policy del bucket, scegliere Modifica.
4. Nella casella Policy, aggiungi o aggiorna la policy del bucket.

Per le policy di bucket di esempio, consulta [Esempi di policy di bucket](#) e [Casi d'uso di esempio](#).

5. Scegli Save changes (Salva modifiche).
6. [Aggiorna l'ACL del bucket](#) per rimuovere le autorizzazioni ACL ad altri gruppi o Account AWS.
7. [Applica l'impostazione Proprietario del bucket applicato](#) per Proprietà dell'oggetto.

Utilizzo di AWS CLI per esaminare e migrare le autorizzazioni ACL

1. Per restituire l'ACL del bucket per il tuo bucket, usa il comando: [get-bucket-acl](#) AWS CLI

```
aws s3api get-bucket-acl --bucket amzn-s3-demo-bucket
```

Ad esempio, questa ACL di bucket concede l'accesso WRITE e READ a un account di terze parti. In questa ACL, l'account di terze parti è identificato dall'[ID utente canonico](#). Per applicare l'impostazione Proprietario del bucket applicato e disabilitare le ACL, è necessario migrare queste autorizzazioni per l'account di terze parti a una policy del bucket.

```
{
  "Owner": {
    "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
  },
  "Grants": [
    {
      "Grantee": {
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
        "Type": "CanonicalUser"
      },
      "Permission": "FULL_CONTROL"
    },
    {
      "Grantee": {
        "ID": "72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
        "Type": "CanonicalUser"
      },
      "Permission": "READ"
    }
  ]
}
```

```

    "Grantee": {
      "ID":
        "72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
      "Type": "CanonicalUser"
    },
    "Permission": "WRITE"
  }
]
}

```

Per altre ACL di esempio, consultare [Casi d'uso di esempio](#).

2. Migrazione delle autorizzazioni ACL del bucket a una policy di bucket:

Questo esempio di policy di bucket concede autorizzazioni `s3:PutObject` e `s3:ListBucket` per un account di terze parti. Nella policy del bucket, l'account di terze parti è identificato dall'ID (). Account AWS **111122223333**

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://policy.json
```

```

policy.json:
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyForCrossAccountAllowUpload",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root"
        ]
      },
      "Action": [
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket",
        "arn:aws:s3::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}

```

Per ulteriori policy di bucket esemplificative, consulta [Esempi di policy di bucket](#) e [Casi d'uso di esempio](#).

3. Per restituire l'ACL per un oggetto specifico, usa il [get-object-acl](#) AWS CLI comando.

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket --key EXAMPLE-OBJECT-KEY
```

4. Se necessario, migrare le autorizzazioni ACL degli oggetti alla policy del bucket.

Questo elemento di risorsa esemplificativo concede l'accesso a un oggetto specifico in una policy di bucket.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-OBJECT-KEY"
```

5. Ripristina l'ACL per il bucket sull'ACL predefinito.

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

6. [Applica l'impostazione Proprietario del bucket applicato](#) per Proprietà dell'oggetto.

Identifica tutte le richieste che richiedono una ACL per l'autorizzazione

Per identificare le richieste Amazon S3 che richiedono le ACL per l'autorizzazione, puoi utilizzare il valore `aclRequired` nei log degli accessi del server Amazon S3 oppure AWS CloudTrail. Se la richiesta richiede un ACL per l'autorizzazione o se sono presenti richieste PUT che specificano un ACL, la stringa è `Yes`. Se non sono richiesti ACL, o se stai impostando un ACL predefinito o se le richieste sono consentite dalla tua policy del bucket, la stringa di `aclRequired` valore è `-` nei log di accesso al server Amazon S3 `bucket-owner-full-control` ed è assente in CloudTrail. Per ulteriori informazioni sui valori `aclRequired` attesi, consulta [ACLValori richiesti per le richieste Amazon S3 comuni](#).

Se hai `PutBucketAcl` o `PutObjectAcl` richiedi con intestazioni che concedono ACL-based autorizzazioni, ad eccezione dell'ACL predefinito, devi rimuovere tali intestazioni `bucket-owner-full-control` prima di poter disabilitare gli ACL. In caso contrario, le tue richieste non avranno esito positivo.

Per tutte le altre richieste che richiedevano un ACL per l'autorizzazione, migra tali autorizzazioni ACL alle policy dei bucket. Quindi, rimuovi tutti gli ACL del bucket prima di abilitare l'impostazione forzata del proprietario del bucket.

 Note

Non rimuovere gli ACL degli oggetti. In caso contrario, le applicazioni che si basano sugli ACL degli oggetti per le autorizzazioni perderanno l'accesso.

Se vedi che nessuna richiesta richiedeva un ACL per l'autorizzazione, puoi procedere alla disattivazione degli ACL. Per ulteriori informazioni sull'identificazione delle richieste, vedere [Utilizzo dei log degli accessi al server Amazon S3 per identificare le richieste](#) e [Identificazione delle richieste Amazon S3 utilizzando CloudTrail](#).

Rivedi e aggiorna le policy dei bucket che utilizzano chiavi di condizione ACL-related

Dopo aver applicato l'impostazione Proprietario del bucket applicato per disabilitare le ACL, i nuovi oggetti possono essere caricati nel bucket solo se la richiesta utilizza ACL di controllo completo del proprietario del bucket o se non specifica un'ACL. Prima di disabilitare gli ACL, rivedi la tua policy del bucket per le chiavi di condizione. ACL-related

Se la tua policy del bucket utilizza una chiave di ACL-related condizione per richiedere l'ACL bucket-owner-full-control predefinito (ad esempio, s3:x-amz-acl), non è necessario aggiornare la policy del bucket. La seguente policy di bucket utilizza il codice s3:x-amz-acl per richiedere l'ACL predefinita bucket-owner-full-control per le richieste PutObject di S3. Questa policy richiede ancora all'object writer di specificare l'ACL predefinita bucket-owner-full-control. Tuttavia, i bucket con ACL disabilitate accettano ancora questa ACL, quindi le richieste continuano ad avere successo senza bisogno di modifiche sul lato client.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OnlyAllowWritesToMyBucketWithBucketOwnerFullControl",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:user/ExampleUser"
        ]
      }
    }
  ],
}
```

```

    "Action": [
      "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control"
      }
    }
  }
]
}

```

Tuttavia, se la tua policy bucket utilizza una chiave di ACL-related condizione che richiede un ACL diverso, devi rimuovere questa chiave di condizione. Questo esempio di policy di bucket richiede l'ACL `public-read` per le richieste `PutObject` di S3 e quindi deve essere aggiornata prima di disabilitare le ACL.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Only allow writes to my bucket with public read access",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:user/ExampleUser"
        ]
      },
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "public-read"
        }
      }
    }
  ]
}

```

```
}
```

Casi d'uso di esempio

Negli esempi seguenti viene illustrato come migrare le autorizzazioni ACL alle policy di bucket per casi d'uso specifici.

Argomenti

- [Concedere l'accesso al gruppo di consegna di log S3 per la registrazione di log degli accessi al server](#)
- [Concedere l'accesso pubblico in lettura agli oggetti nel bucket](#)
- [Concedi ad Amazon ElastiCache \(Redis OSS\) l'accesso al tuo bucket S3](#)

Concedere l'accesso al gruppo di consegna di log S3 per la registrazione di log degli accessi al server

Se desideri applicare l'impostazione Proprietario del bucket applicato per disabilitare le ACL per un bucket di destinazione di registrazione di log degli accessi a un server (noto anche come bucket target), è necessario migrare le autorizzazioni ACL bucket per il gruppo di consegna di log S3 al principale del servizio di registrazione di log (`logging.s3.amazonaws.com`) in una policy del bucket. Per ulteriori informazioni sulle autorizzazioni della distribuzione dei registri, consultare [Autorizzazioni per la distribuzione dei registri](#).

Questa ACL del bucket concede l'accesso WRITE e READ_ACP al gruppo di distribuzione di registri S3:

```
{
  "Owner": {
    "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
  },
  "Grants": [
    {
      "Grantee": {
        "Type": "CanonicalUser",
        "ID":
"852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
      },
      "Permission": "FULL_CONTROL"
    },
  ],
}
```

```

    {
      "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
      },
      "Permission": "WRITE"
    },
    {
      "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
      },
      "Permission": "READ_ACP"
    }
  ]
}

```

Per migrare le autorizzazioni ACL del bucket per il gruppo di distribuzione di registri S3 al principale del servizio di registrazione in una policy di bucket

1. Aggiungi la seguente policy di bucket al bucket di destinazione, sostituendo i valori di esempio.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://policy.json
```

```

policy.json:    {
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "S3ServerAccessLogsPolicy",
        "Effect": "Allow",
        "Principal": {
          "Service": "logging.s3.amazonaws.com"
        },
        "Action": [
          "s3:PutObject"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-LOGGING-PREFIX",
        "Condition": {
          "ArnLike": {
            "aws:SourceArn": "arn:aws:s3:::SOURCE-BUCKET-NAME"
          }
        }
      }
    ]
  }
}

```

```

        "StringEquals": {
            "aws:SourceAccount": "SOURCE-AWS-ACCOUNT-ID"
        }
    }
}

```

2. Ripristina l'ACL per il bucket di destinazione all'ACL predefinita.

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. [Applica l'impostazione Proprietario del bucket applicato](#) per Proprietà dell'oggetto al bucket di destinazione.

Concedere l'accesso pubblico in lettura agli oggetti nel bucket

Se le ACL di oggetto consentono l'accesso pubblico in lettura a tutti gli oggetti del bucket, è possibile migrare queste autorizzazioni ACL a una policy di bucket.

Questa ACL di oggetto concede l'accesso pubblico in lettura a un oggetto in un bucket:

```

{
  "Owner": {
    "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
  },
  "Grants": [
    {
      "Grantee": {
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
        "Type": "CanonicalUser"
      },
      "Permission": "FULL_CONTROL"
    },
    {
      "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
      },
      "Permission": "READ"
    }
  ]
}

```

```
]
}
```

Per migrare le autorizzazioni ACL di lettura pubblica a una policy di bucket

1. Per concedere l'accesso in lettura pubblica a tutti gli oggetti nel bucket, aggiungere la seguente policy di bucket, sostituendo i valori di esempio.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
file:///policy.json
```

```
policy.json:
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}
```

Per concedere l'accesso pubblico a un oggetto specifico in una policy di bucket, utilizzare il seguente formato per l'elemento Resource.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

Per concedere l'accesso pubblico a tutti gli oggetti con un prefisso specifico, utilizzare il seguente formato per l'elemento Resource.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/PREFIX/*"
```

2. [Applica l'impostazione Proprietario del bucket applicato](#) per Proprietà dell'oggetto.

Concedi ad Amazon ElastiCache (Redis OSS) l'accesso al tuo bucket S3

Puoi [esportare il tuo backup ElastiCache](#) (Redis OSS) in un bucket S3, che ti consente di accedere al backup dall'esterno. ElastiCache Per esportare il backup in un bucket S3, devi concedere le ElastiCache autorizzazioni per copiare un'istantanea nel bucket. Se hai concesso le autorizzazioni ElastiCache a un bucket ACL, devi migrare queste autorizzazioni a una policy del bucket prima di applicare l'impostazione applicata dal proprietario del bucket per disabilitare gli ACL. Per ulteriori informazioni, consulta [Concedere l' ElastiCache accesso al tuo bucket Amazon S3 nella Amazon User Guide](#). ElastiCache

L'esempio seguente mostra le autorizzazioni ACL del bucket a cui concedono le autorizzazioni. ElastiCache

```
{
  "Owner": {
    "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
  },
  "Grants": [
    {
      "Grantee": {
        "ID":
"852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
        "Type": "CanonicalUser"
      },
      "Permission": "FULL_CONTROL"
    },
    {
      "Grantee": {
        "ID":
"540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
        "Type": "CanonicalUser"
      },
      "Permission": "READ"
    },
    {
      "Grantee": {
        "ID":
"540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
        "Type": "CanonicalUser"
      },
      "Permission": "WRITE"
    }
  ],
}
```

```

    {
      "Grantee": {
        "ID":
"540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
        "Type": "CanonicalUser"
      },
      "Permission": "READ_ACP"
    }
  ]
}

```

Per migrare le autorizzazioni ACL del bucket per ElastiCache (Redis OSS) a una policy del bucket

1. Aggiungere la seguente policy di bucket al bucket di destinazione, sostituendo i valori di esempio.

```

aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
file:///policy.json

policy.json:
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt15399483",
      "Effect": "Allow",
      "Principal": {
        "Service": "Region.elasticache-snapshot.amazonaws.com"
      },
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}

```



```
}
```

2. Resetare l'ACL per il bucket all'ACL di default:

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. [Applica l'impostazione Proprietario del bucket applicato](#) per Proprietà dell'oggetto.

Impostazione di Object Ownership quando si crea un bucket

Quando crei un bucket, puoi configurare S3 Object Ownership. Per impostare Object Ownership per un bucket esistente, consulta [Impostazione di Object Ownership su un bucket esistente](#).

S3 Object Ownership è un'impostazione a livello di bucket di Amazon S3 che può essere utilizzata per disabilitare le [liste di controllo degli accessi \(ACL\)](#) e assumere la proprietà di ogni oggetto nel bucket, semplificando la gestione degli accessi ai dati archiviati in Amazon S3. Per impostazione predefinita, Proprietà dell'oggetto S3 è impostata su Proprietario del bucket applicato e le ACL sono disabilitate per nuovi bucket. Con le ACL disabilitate, il proprietario del bucket possiede ogni oggetto nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy di gestione dell'accesso. È consigliabile mantenere le ACL disabilitate, tranne in circostanze insolite in cui è necessario controllare individualmente l'accesso per ciascun oggetto.

Object Ownership ha tre impostazioni che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e disabilitare o abilitare le ACL:

ACL disabilitate

- Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket possiede automaticamente e ha il controllo completo di ogni oggetto nel bucket. Le ACL non influiscono più sulle autorizzazioni per i dati nel bucket S3. Il bucket utilizza le policy per definire il controllo degli accessi.

ACL abilitate

- Proprietario del bucket preferito - Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono sul bucket con l'ACL `bucket-owner-full-control` predefinita.
- Autore di oggetti: chi carica un oggetto possiede l' Account AWS oggetto, ne ha il pieno controllo e può concedere ad altri utenti l'accesso ad esso tramite ACL.

Autorizzazioni: per applicare l'impostazione Bucket owner enforced (Applicata da proprietario bucket) oppure Bucket owner preferred (Preferita da proprietario bucket), devi disporre delle seguenti autorizzazioni: `s3:CreateBucket` e `s3:PutBucketOwnershipControls`. Non sono necessarie autorizzazioni aggiuntive quando si crea un bucket con l'impostazione Object writer applicata. Per ulteriori informazioni sulle autorizzazioni di Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Important

La maggior parte dei casi d'uso moderni in Amazon S3 non richiede più l'uso di ACL ed è consigliabile disabilitarle tranne in circostanze in cui è necessario controllare l'accesso individualmente per ciascun oggetto. Con Object Ownership, è possibile disabilitare le ACL e fare affidamento sulle policy per il controllo degli accessi. Quando si disattivano gli ACL, è possibile gestire facilmente un bucket con oggetti caricati da account diversi. AWS In qualità di proprietario del bucket, possiedi tutti gli oggetti nel bucket e puoi gestirne l'accesso utilizzando le policy.

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare un bucket.

Note

- Una volta creato, non è possibile modificarne la regione.
- Scegli una regione nelle tue vicinanze per ridurre al minimo la latenza e i costi o essere conforme ai requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione. Per un elenco di Amazon S3 Regioni AWS, consulta gli [Servizio AWS endpoint](#) in Riferimenti generali di Amazon Web Services

3. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
4. Scegliere Create bucket (Crea bucket). Viene visualizzata la pagina Create bucket (Crea bucket).
5. In Nome bucket, immettere il nome del bucket.

Il nome del bucket deve:

- Essere univoco all'interno di una partizione. Una partizione è un raggruppamento di regioni. AWS attualmente ha tre partizioni: aws (regioni commerciali), aws-cn (regioni cinesi) e aws-us-gov (AWS GovCloud (US) Regions).
- Deve contenere da 3 a 63 caratteri
- Essere costituito solo da lettere minuscole, numeri, punti (.) e trattini (-). Per una migliore compatibilità, è consigliabile evitare l'utilizzo di punti (.) nei nomi dei bucket, ad eccezione dei bucket utilizzati solo per l'hosting di siti web statici.
- Iniziare e finire con una lettera o un numero.
- Per l'elenco completo delle regole di denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#).

 Important

- Una volta creato il bucket, non è possibile modificarne il nome.
- Non includere informazioni sensibili nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

6. (Facoltativo) In Configurazione generale è possibile scegliere di copiare le impostazioni di un bucket esistente nel nuovo bucket. Se non desideri copiare le impostazioni di un bucket esistente, procedi al passaggio successivo.

 Note

Questa opzione:

- Non è disponibile nella AWS CLI ed è disponibile solo nella console Amazon S3
- Non copia la policy di bucket dal bucket esistente nel nuovo bucket

Per copiare le impostazioni di un bucket esistente, in Copia impostazioni da un bucket esistente, seleziona Scegli bucket. Viene visualizzata la finestra Scegli bucket. Individua il bucket con le impostazioni da copiare e seleziona Scegli bucket. La finestra Scegli bucket si chiude e si riapre la finestra Crea bucket.

In Copia impostazioni da un bucket esistente, ora viene visualizzato il nome del bucket selezionato. Le impostazioni del nuovo bucket ora corrispondono alle impostazioni del bucket selezionato. Se desideri rimuovere le impostazioni copiate, scegli Ripristina le impostazioni predefinite. Esamina le restanti impostazioni del bucket nella pagina Crea bucket. Se non desideri apportare modifiche, puoi passare alla fase finale.

7. Alla voce Proprietà oggetto, per disabilitare o abilitare le ACL e controllare la proprietà degli oggetti caricati nel bucket, scegliere una delle seguenti impostazioni:

ACL disabilitate

- Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket ha automaticamente il controllo completo di ogni oggetto di proprietà nel bucket per uso generico. Le liste di controllo degli accessi (ACL) non influiscono più sulle autorizzazioni di accesso ai dati nel bucket per uso generico S3. Il bucket utilizza esclusivamente le policy per definire il controllo degli accessi.

Per impostazione predefinita, le ACL sono disabilitate. La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne in circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

ACL abilitati

- Proprietario del bucket preferito - Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono sul bucket con l'ACL bucket-owner-full-control predefinita.

Se applichi l'impostazione Proprietario del bucket preferito, per richiedere che tutti i caricamenti di Amazon S3 includano l'ACL predefinita bucket-owner-full-control, puoi [aggiungere una policy del bucket](#) che consenta solo il caricamento di oggetti che utilizzano questa ACL.

- Autore di oggetti: chi carica un oggetto possiede l'oggetto, ne ha il pieno controllo e può concedere ad altri utenti l'accesso ad esso tramite ACL. Account AWS

Note

L'impostazione predefinita è Proprietario del bucket applicato. Per applicare l'impostazione predefinita e mantenere gli ACL disabilitati, è necessaria solo l'autorizzazione `s3:CreateBucket`. Per abilitare gli ACL, è necessario disporre dell'autorizzazione `s3:PutBucketOwnershipControls`.

8. In Impostazioni di blocco dell'accesso pubblico per questo bucket scegli le impostazioni di blocco dell'accesso pubblico che vuoi applicare al bucket.

Per impostazione predefinita, tutte e quattro le impostazioni Blocco dell'accesso pubblico sono abilitate. È consigliabile mantenere tutte le impostazioni abilitate, a meno che non sia necessario disattivarne una o più di una per il caso d'uso specifico. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Note

Per abilitare tutte le impostazioni Blocco dell'accesso pubblico, è richiesta solo l'autorizzazione `s3:CreateBucket`. Per disattivare le impostazioni Blocco dell'accesso pubblico, è necessario disporre dell'autorizzazione `s3:PutBucketPublicAccessBlock`.

9. (Facoltativo) Per impostazione predefinita, la funzionalità Controllo delle versioni del bucket è disabilitata. La funzione Controllo delle versioni è un modo per conservare più versioni di un oggetto nello stesso bucket. Si può utilizzare questa funzione per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket. Con il controllo delle versioni puoi eseguire facilmente il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Per abilitare il controllo delle versioni sul bucket, scegli Abilita.

10. (Facoltativo) In Tags (Tag), puoi scegliere di aggiungere tag al bucket. Con l'allocazione dei costi di AWS è possibile utilizzare i tag dei bucket per annotare nella fatturazione l'utilizzo di un

bucket. Un tag è una coppia chiave-valore che rappresenta un'etichetta assegnata a un bucket. Per ulteriori informazioni, consulta [the section called “Utilizzo dei tag per l'allocazione dei costi”](#).

Per aggiungere un tag al bucket, inserisci un valore in Key (Chiave) e facoltativamente un valore in Value (Valore), quindi scegli Add Tag (Aggiungi tag).

11. Per configurare Crittografia predefinita, in Tipo di crittografia scegli una delle seguenti opzioni:

- Server-side crittografia con chiavi gestite da Amazon S3 () SSE-S3
- Server-side crittografia con AWS Key Management Service chiavi () SSE-KMS
- Dual-layer crittografia lato server con chiavi AWS Key Management Service (AWS KMS) () DSSE-KMS

 Important

Se si utilizza l' DSSE-KMS opzione SSE-KMS or per la configurazione di crittografia predefinita, si è soggetti alla quota di richieste al secondo (RPS) di AWS KMS. Per ulteriori informazioni sulle AWS KMS quote e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli AWS Key Management Service sviluppatori.

I bucket e i nuovi oggetti sono crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) come livello base di configurazione della crittografia. Per ulteriori informazioni sulla crittografia predefinita, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#). Per ulteriori informazioni su SSE-S3, consultare [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).

Per ulteriori informazioni sull'utilizzo della crittografia lato server per crittografare i dati, consulta [the section called “Crittografia dei dati”](#).

12. Se hai scelto Server-side la crittografia con AWS Key Management Service chiavi (SSE-KMS) o la Dual-layer crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (DSSE-KMS), procedi come segue:

a. In Chiave AWS KMS specifica la tua chiave KMS in uno dei seguenti modi:

- Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS keys e scegli la tua chiave KMS dall'elenco delle chiavi disponibili.

Sia la chiave gestita da AWS (aws/s3) che quella gestita dal cliente vengono visualizzate in questo elenco. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per specificare l'ARN della chiave KMS, scegli Inserisci l'ARN della AWS KMS key e quindi specifica l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

⚠ Important

È possibile utilizzare solo le chiavi KMS disponibili nella Regione AWS stesso bucket. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, è necessario inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione richiesta per l'uso della chiave e quindi inserire l'ARN della chiave KMS. Per ulteriori informazioni sulle autorizzazioni multi-account per le chiavi KMS, consulta [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service . Per ulteriori informazioni su SSE-KMS, consulta [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#) Per ulteriori informazioni su DSSE-KMS, vedere [the section called “Dual-layer crittografia lato server \(\) DSSE-KMS”](#).

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- b. Quando configuri il bucket per utilizzare la crittografia predefinita con SSE-KMS, puoi anche utilizzare S3 Bucket Keys. Le chiavi S3 Bucket riducono il costo della crittografia diminuendo il traffico di richieste da Amazon S3 a AWS KMS Per ulteriori informazioni,

consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#). Le chiavi S3 Bucket non sono supportate per. DSSE-KMS

Per impostazione predefinita, le chiavi del bucket S3 sono abilitate nella console Amazon S3. È consigliabile lasciare abilitate le chiavi del bucket S3 per ridurre i costi. Per disabilitare le chiavi del bucket S3 per il bucket in uso, scegli Disabilita in Chiave del bucket.

13. (Facoltativo) Object Lock S3 aiuta a proteggere i nuovi oggetti dall'eliminazione o dalla sovrascrittura. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#). Se desideri abilitare Object Lock S3, procedi come segue:

- a. Scegli Impostazioni avanzate.

 Important

Abilitando Object Lock si abilita automaticamente il controllo delle versioni per il bucket. Dopo aver abilitato e creato il bucket, è necessario anche configurare le impostazioni predefinite di conservazione e blocco legale di Object Lock nella scheda Proprietà del bucket.

- b. Se desideri attivare Object Lock, scegli Abilita, leggi l'avviso che appare e confermallo.

 Note

Per creare un bucket abilitato per Object Lock, sono necessarie le seguenti autorizzazioni: `s3:CreateBucket`, `s3:PutBucketVersioning` e `s3:PutBucketObjectLockConfiguration`.

14. Seleziona Crea bucket.

Utilizzo di AWS CLI

Per impostare la proprietà dell'oggetto quando crei un nuovo bucket, usa il `create-bucket` AWS CLI comando con il parametro. `--object-ownership`

In questo esempio viene applicata l'impostazione Proprietario del bucket applicato per un nuovo bucket utilizzando la AWS CLI:


```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1 --object-ownership BucketOwnerEnforced
```

Important

Se non imposti la proprietà dell'oggetto quando crei un bucket utilizzando il AWS CLI, l'impostazione predefinita sarà `ObjectWriter` (ACL abilitati).

Utilizzo di AWS SDK per Java

In questo esempio viene definita l'impostazione Proprietario del bucket applicato per un nuovo bucket utilizzando AWS SDK per Java:

```
// Build the ObjectOwnership for CreateBucket
CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
    .bucket(bucketName)
    .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
    .build()

// Send the request to Amazon S3
s3client.createBucket(createBucketRequest);
```

Utilizzo CloudFormation

Per utilizzare la `AWS::S3::Bucket` CloudFormation risorsa per impostare la proprietà degli oggetti quando crei un nuovo bucket, consulta la Guida per l'utente [OwnershipControlsAWS::S3::Bucket](#) all'AWS CloudFormation interno.

Utilizzo della REST API

Per applicare l'impostazione Proprietario del bucket applicato per S3 Proprietà dell'oggetto, utilizza l'operazione API `CreateBucket` con l'intestazione della richiesta `x-amz-object-ownership` impostata su `BucketOwnerEnforced`. Per ulteriori informazioni, consulta [CreateBucket](#) nella Guida di riferimento per l'API di Amazon Simple Storage Service.

Fasi successive: dopo aver eseguito le impostazioni Proprietario del bucket applicato o Proprietario del bucket preferito per Proprietà dell'oggetto, è possibile compiere i seguenti passaggi:

- [Proprietario del bucket applicato](#) – Richiedi che tutti i nuovi bucket vengano creati con ACL disabilitate utilizzando le policy IAM o di Organizations.
- [Proprietario del bucket preferito](#) – Aggiungi una policy di bucket S3 per richiedere l'ACL predefinita `bucket-owner-full-control` per tutti gli oggetti caricati nel tuo bucket.

Impostazione di Object Ownership su un bucket esistente

È possibile configurare S3 Object Ownership su un bucket S3 esistente. Per applicare Object Ownership quando si crea un bucket, consulta [Impostazione di Object Ownership quando si crea un bucket](#).

S3 Object Ownership è un'impostazione a livello di bucket di Amazon S3 che può essere utilizzata per disabilitare le [liste di controllo degli accessi \(ACL\)](#) e assumere la proprietà di ogni oggetto nel bucket, semplificando la gestione degli accessi ai dati archiviati in Amazon S3. Per impostazione predefinita, Proprietà dell'oggetto S3 è impostata su Proprietario del bucket applicato e le ACL sono disabilitate per nuovi bucket. Con le ACL disabilitate, il proprietario del bucket possiede ogni oggetto nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy di gestione dell'accesso. È consigliabile mantenere le ACL disabilitate, tranne in circostanze insolite in cui è necessario controllare individualmente l'accesso per ciascun oggetto.

Object Ownership ha tre impostazioni che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e disabilitare o abilitare le ACL:

ACL disabilitate

- Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket possiede automaticamente e ha il controllo completo di ogni oggetto nel bucket. Le ACL non influiscono più sulle autorizzazioni per i dati nel bucket S3. Il bucket utilizza le policy per definire il controllo degli accessi.

ACL abilitate

- Proprietario del bucket preferito - Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono sul bucket con l'ACL `bucket-owner-full-control` predefinita.
- Autore di oggetti: chi carica un oggetto possiede l'oggetto, ne ha il pieno controllo e può concedere ad altri utenti l'accesso ad esso tramite ACL. Account AWS

Prerequisiti: prima di applicare l'impostazione Proprietario del bucket applicato per disabilitare le ACL, è necessario migrare le autorizzazioni ACL bucket alle policy del bucket e ripristinare le ACL bucket sull'ACL privata di default. Si consiglia inoltre di migrare le autorizzazioni ACL di oggetti alle policy di bucket e di modificare le policy di bucket che richiedono ACL diverse dalle ACL di controllo completo del proprietario del bucket. Per ulteriori informazioni, consulta [Prerequisiti per la disabilitazione delle ACL](#).

Autorizzazioni: Per utilizzare questa operazione, è necessario disporre dell'autorizzazione `s3:PutBucketOwnershipControls`. Per ulteriori informazioni sulle autorizzazioni di Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket scegliere il nome del bucket al quale applicare un'impostazione S3 Object Ownership.
3. Scegli la scheda Autorizzazioni.
4. Alla voce Proprietà Oggetto scegli Modifica.
5. Alla voce Proprietà oggetto, per disabilitare o abilitare le ACL e controllare la proprietà degli oggetti caricati nel bucket, scegliere una delle seguenti impostazioni:

ACL disabilitate

- Proprietario del bucket applicato – Le ACL sono disabilitate e il proprietario del bucket possiede automaticamente e ha il pieno controllo su ogni oggetto nel bucket. Le ACL non influiscono più sulle autorizzazioni per i dati nel bucket S3. Il bucket utilizza le policy per definire il controllo degli accessi.

Per richiedere che tutti i nuovi bucket vengano creati con gli ACL disattivati utilizzando IAM o AWS Organizations policy, consulta. [Disabilitazione degli ACL per tutti i nuovi bucket \(proprietario del bucket applicato\)](#)

ACL abilitati

- Proprietario del bucket scelto – Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono nel bucket con l'ACL predefinita `bucket-owner-full-control`.

Se applichi l'impostazione del proprietario del bucket preferito per richiedere che tutti i caricamenti di Amazon S3 includano l'ACL predefinita `bucket-owner-full-control`, puoi [aggiungere una policy del bucket](#) che consenta solo il caricamento di oggetti che utilizzano questo ACL.

- Autore di oggetti: chi carica un oggetto possiede l'oggetto, ne ha il pieno controllo e può concedere ad altri utenti l'accesso ad esso tramite ACL. Account AWS

6. Selezionare Salva.

Utilizzo di AWS CLI

Per applicare un'impostazione Object Ownership per un bucket esistente, utilizzare il comando `put-bucket-ownership-controls` con il parametro `--ownership-controls`. I valori validi per la proprietà sono `BucketOwnerEnforced`, `BucketOwnerPreferred` o `ObjectWriter`.

In questo esempio viene applicata l'impostazione Proprietario del bucket applicato per un bucket esistente utilizzando la AWS CLI:

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

Per ulteriori informazioni su `put-bucket-ownership-controls`, consulta [put-bucket-ownership-controls](#) nella Guida per l'utente di AWS Command Line Interface .

Utilizzo di AWS SDK per Java

In questo esempio viene eseguita l'impostazione `BucketOwnerEnforced` per Object Ownership su un bucket esistente utilizzando la AWS SDK per Java:

```
// Build the ObjectOwnership for BucketOwnerEnforced
OwnershipControlsRule rule = OwnershipControlsRule.builder()
    .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
```

```
        .build();

OwnershipControls ownershipControls = OwnershipControls.builder()
    .rules(rule)
    .build()

// Build the PutBucketOwnershipControlsRequest
PutBucketOwnershipControlsRequest putBucketOwnershipControlsRequest =
    PutBucketOwnershipControlsRequest.builder()
        .bucket(BUCKET_NAME)
        .ownershipControls(ownershipControls)
        .build();

// Send the request to Amazon S3
s3client.putBucketOwnershipControls(putBucketOwnershipControlsRequest);
```

Utilizzo CloudFormation

Per utilizzarlo CloudFormation per applicare un'impostazione di Object Ownership per un bucket esistente, consulta [AWS::S3::Bucket OwnershipControls](#) la Guida per l'AWS CloudFormation utente.

Utilizzo della REST API

Per utilizzare REST API per applicare un'impostazione Object Ownership a un bucket S3 esistente, utilizzare `PutBucketOwnershipControls`. Per ulteriori informazioni, consulta [PutBucketOwnershipControls](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Fasi successive: dopo aver eseguito le impostazioni Proprietario del bucket applicato o Proprietario del bucket preferito per Proprietà dell'oggetto, è possibile compiere i seguenti passaggi:

- [Proprietario del bucket applicato](#) – Richiedi che tutti i nuovi bucket vengano creati con ACL disabilitate utilizzando le policy IAM o di Organizations.
- [Proprietario del bucket preferito](#) – Aggiungi una policy di bucket S3 per richiedere l'ACL predefinita `bucket-owner-full-control` per tutti gli oggetti caricati nel tuo bucket.

Visualizzare l'impostazione di Object Ownership per un bucket S3

S3 Object Ownership è un'impostazione a livello di bucket di Amazon S3 che può essere utilizzata per disabilitare le [liste di controllo degli accessi \(ACL\)](#) e assumere la proprietà di ogni oggetto nel

bucket, semplificando la gestione degli accessi ai dati archiviati in Amazon S3. Per impostazione predefinita, Proprietà dell'oggetto S3 è impostata su Proprietario del bucket applicato e le ACL sono disabilitate per nuovi bucket. Con le ACL disabilitate, il proprietario del bucket possiede ogni oggetto nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy di gestione dell'accesso. È consigliabile mantenere le ACL disabilitate, tranne in circostanze insolite in cui è necessario controllare individualmente l'accesso per ciascun oggetto.

Object Ownership ha tre impostazioni che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e disabilitare o abilitare le ACL:

ACL disabilitate

- Proprietario del bucket applicato (impostazione predefinita): le ACL sono disabilitate e il proprietario del bucket possiede automaticamente e ha il controllo completo di ogni oggetto nel bucket. Le ACL non influiscono più sulle autorizzazioni per i dati nel bucket S3. Il bucket utilizza le policy per definire il controllo degli accessi.

ACL abilitate

- Proprietario del bucket preferito - Il proprietario del bucket possiede e ha il pieno controllo sui nuovi oggetti che altri account scrivono sul bucket con l'ACL `bucket-owner-full-control` predefinita.
- Autore di oggetti: chi carica un oggetto possiede l'oggetto, ne ha il pieno controllo e può concedere ad altri utenti l'accesso ad esso tramite ACL. Account AWS

È possibile visualizzare le impostazioni di S3 Object Ownership per un bucket Amazon S3. Per impostare Object Ownership per un nuovo bucket, consultare [Impostazione di Object Ownership quando si crea un bucket](#). Per impostare Object Ownership per un bucket esistente, consultare [Impostazione di Object Ownership su un bucket esistente](#).

Autorizzazioni: Per utilizzare questa operazione, è necessario disporre dell'autorizzazione `s3:GetBucketOwnershipControls`. Per ulteriori informazioni sulle autorizzazioni di Amazon S3, consulta [Azioni, risorse e chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket scegliere il nome del bucket al quale applicare un'impostazione di Object Ownership.
3. Scegli la scheda Autorizzazioni.
4. Alla voce Proprietà Oggetto, è possibile visualizzare le impostazioni di Object Ownership per il bucket.

Utilizzo di AWS CLI

Per recuperare l'impostazione S3 Object Ownership per un bucket S3, usa il comando. [get-bucket-ownership-controls](#) AWS CLI

```
aws s3api get-bucket-ownership-controls --bucket amzn-s3-demo-bucket
```

Utilizzo della REST API

Per recuperare l'impostazione di Object Ownership per un bucket S3, utilizzare l'operazione API `GetBucketOwnershipControls`. Per ulteriori informazioni, consulta [GetBucketOwnershipControls](#).

Disabilitare le ACL per tutti i nuovi bucket e applicare Object Ownership

Ti consigliamo di disabilitare le ACL sui bucket Amazon S3. È possibile farlo applicando l'impostazione Proprietario del bucket applicato per S3 Proprietà dell'oggetto. Una volta applicata questa impostazione, le ACL verranno disabilite e si possiederanno automaticamente e si avrà il pieno controllo su tutti gli oggetti del bucket. Per richiedere che tutti i nuovi bucket vengano creati con gli ACL disattivati, utilizza le politiche AWS Identity and Access Management (IAM) o le politiche di controllo dei AWS Organizations servizi (SCP), come descritto nella sezione successiva.

Per applicare la proprietà degli oggetti per i nuovi oggetti senza disabilitare le ACL, è possibile eseguire l'impostazione proprietario del bucket preferito. Una volta applicata questa impostazione, si consiglia fortemente di aggiornare la policy del bucket per richiedere l'ACL predefinita `bucket-owner-full-control` per tutte le richieste PUT sul tuo bucket. I client devono anch'essi essere aggiornati per inviare l'ACL predefinita `bucket-owner-full-control` al tuo bucket da altri account.

Argomenti

- [Disabilitazione degli ACL per tutti i nuovi bucket \(proprietario del bucket applicato\)](#)
- [Richiedere l'ACL predefinito con controllo completo dal proprietario del bucket per le operazioni PUT di Amazon S3 \(preferibilmente il proprietario del bucket\)](#)

Disabilitazione degli ACL per tutti i nuovi bucket (proprietario del bucket applicato)

La seguente policy IAM di esempio nega l'autorizzazione `s3:CreateBucket` per un utente IAM o un ruolo specifico a meno che non venga applicata l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto. La coppia chiave-valore nel blocco di `Condition` specifica `s3:x-amz-object-ownership` come chiave e l'impostazione `BucketOwnerEnforced` come valore corrispondente. In altre parole, l'utente IAM può creare bucket solo se imposta Proprietario del bucket applicato per Proprietà dell'oggetto e disabilita le ACL. Puoi anche utilizzare questa policy come SCP di confine per la tua organizzazione. AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireBucketOwnerFullControl",
      "Action": "s3:CreateBucket",
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-object-ownership": "BucketOwnerEnforced"
        }
      }
    }
  ]
}
```


Richiedere l'ACL predefinito con controllo completo dal proprietario del bucket per le operazioni PUT di Amazon S3 (**preferibilmente il proprietario del bucket**)

Con l'impostazione proprietario del bucket preferito per Object Ownership, in qualità di proprietario del bucket possiedi e hai il pieno controllo sui nuovi oggetti che gli altri account scrivono sul tuo bucket con l'ACL predefinita `bucket-owner-full-control`. Tuttavia, se altri account scrivono oggetti nel tuo bucket senza l'ACL predefinita `bucket-owner-full-control`, l'object writer mantiene il pieno controllo degli accessi. In qualità di proprietario del bucket, è possibile implementare una policy del bucket che consenta la scrittura solo se si specifica l'ACL predefinita `bucket-owner-full-control`.

Note

Se le ACL sono disabilitate con l'impostazione Proprietario del bucket applicato, in qualità di proprietario del bucket possiedi automaticamente e hai il controllo completo di tutti gli oggetti del bucket. Non è necessario utilizzare questa sezione per aggiornare la policy del bucket per applicare la proprietà degli oggetti per il proprietario del bucket.

La seguente policy del bucket specifica che l'account **111122223333** può caricare oggetti **amzn-s3-demo-bucket** solo quando l'ACL dell'oggetto è impostata su `bucket-owner-full-control`. Assicurati di sostituire **111122223333** con un account reale e **amzn-s3-demo-bucket** con il nome del tuo bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OnlyAllowWritesToMyBucketWithBucketOwnerFullControl",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:user/ExampleUser"
        ]
      },
      "Action": [
```

```
    "s3:PutObject"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "StringEquals": {
      "s3:x-amz-acl": "bucket-owner-full-control"
    }
  }
}
```

Di seguito è riportata un'operazione di copia di esempio che include l'ACL `bucket-owner-full-control` predefinito utilizzando AWS Command Line Interface (AWS CLI).

```
aws s3 cp file.txt s3://amzn-s3-demo-bucket --acl bucket-owner-full-control
```

Dopo che la policy del bucket è diventata efficace, se il client non include l'ACL predefinita `bucket-owner-full-control`, l'operazione non riuscirà e l'uploader riceverà il seguente errore:

Si è verificato un errore () `AccessDenied` durante la chiamata all'operazione: Accesso negato.
`PutObject`

Note

Se i client hanno bisogno di accedere agli oggetti dopo il caricamento, sarà necessario concedere autorizzazioni aggiuntive per l'account di caricamento. Per informazioni sulla concessione agli account dell'accesso alle risorse, consulta la sezione [Passaggi che utilizzano le policy per gestire l'accesso alle risorse Amazon S3](#).

Risoluzione dei problemi

Quando esegui l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, le liste di controllo degli accessi (ACL) vengono disabilitate e tu, in qualità di proprietario del bucket, possiedi automaticamente tutti gli oggetti nel bucket. Le ACL non influiscono più sulle autorizzazioni per gli oggetti nel bucket. Puoi utilizzare le policy per concedere autorizzazioni. Tutte le richieste PUT S3 devono specificare l'ACL predefinita `bucket-owner-full-control` o non specificare una ACL; in

caso contrario non andranno a buon fine. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Se viene specificato un'ACL non valida o le autorizzazioni ACL del bucket garantiscono l'accesso al di fuori del tuo Account AWS, potrebbero essere visualizzate le seguenti risposte di errore.

AccessControlListNotSupported

Dopo aver applicato l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, le ACL vengono disabilitate. Le richieste di impostazione degli ACL o di aggiornamento degli ACL hanno esito negativo e restituiscono il codice AccessControlListNotSupported di errore. 400 Le richieste di lettura delle ACL sono ancora supportate. Le richieste di lettura delle ACL restituiscono sempre una risposta che mostra il pieno controllo per il proprietario del bucket. Nelle operazioni PUT è necessario specificare le ACL di controllo completo del proprietario del bucket o non specificare un'ACL. Altrimenti, le tue operazioni PUT falliranno.

Il `put-object` AWS CLI comando di esempio seguente include l'`public-read` ACL predefinito.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object-key-name --body doc-example-body --acl public-read
```

Se il bucket utilizza l'impostazione Proprietario del bucket applicato per disabilitare le ACL, questa operazione non va a buon fine e l'uploader riceve il seguente messaggio di errore:

Si è verificato un errore (AccessControlListNotSupported) durante la chiamata all'`PutObject` operazione: il bucket non consente gli ACL

InvalidBucketAclWithObjectOwnership

Se desideri applicare l'impostazione Proprietario del bucket applicato per disabilitare le ACL, l'ACL bucket dovrà fornire il controllo completo solo al proprietario del bucket. L'ACL del bucket non può dare accesso a un gruppo esterno Account AWS o a un altro gruppo. Ad esempio, se la tua `CreateBucket` richiesta imposta il proprietario del bucket e specifica un ACL del bucket che fornisce l'accesso a un oggetto esterno Account AWS, la richiesta ha esito negativo con un 400 errore e restituisce il codice di errore. `InvalidBucketAclWithObjectOwnership` Allo stesso modo, se la tua richiesta `PutBucketOwnershipControls` imposta il proprietario del bucket applicato su un bucket con un ACL di bucket che concede autorizzazioni ad altri, la richiesta avrà esito negativo.

Example: l'ACL del bucket esistente concede l'accesso pubblico in lettura

Ad esempio, se un ACL bucket esistente concede l'accesso pubblico in lettura, non potrai applicare l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto finché queste autorizzazioni ACL non vengono migrate a una policy del bucket e l'ACL bucket non viene ripristinata sull'ACL privata di default. Per ulteriori informazioni, consulta [Prerequisiti per la disabilitazione delle ACL](#).

Questo esempio di ACL di bucket concede l'accesso pubblico in lettura:

```
{
  "Owner": {
    "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
  },
  "Grants": [
    {
      "Grantee": {
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
        "Type": "CanonicalUser"
      },
      "Permission": "FULL_CONTROL"
    },
    {
      "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
      },
      "Permission": "READ"
    }
  ]
}
```

Il `put-bucket-ownership-controls` AWS CLI comando di esempio seguente applica l'impostazione imposta dal proprietario del bucket per Object Ownership:

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls Rules=[{ObjectOwnership=BucketOwnerEnforced}]
```

Poiché l'ACL del bucket consente l'accesso pubblico in lettura, la richiesta sarà respinta e restituirà il seguente codice di errore:

Si è verificato un errore (InvalidBucketAclWithObjectOwnership) durante la chiamata all' PutBucketOwnershipControls operazione: Bucket non può avere ACL impostati con l'impostazione's ObjectOwnership BucketOwnerEnforced

Sicurezza in Amazon S3

Important

Amazon Simple Storage Service applica ora una nuova impostazione di sicurezza predefinita per i bucket che disabilita automaticamente la crittografia lato server con chiavi fornite dal cliente (SSE-C) per tutti i nuovi bucket generici. Nell'aprile 2026, Amazon S3 ha implementato un aggiornamento in modo che tutti i nuovi bucket generici abbiano la crittografia disabilitata per tutte le nuove richieste di scrittura. SSE-C Per i bucket esistenti senza oggetti SSE-C crittografati, Amazon S3 è disabilitato SSE-C anche per tutte le nuove richieste di scrittura. Account AWS Con questa modifica, le applicazioni che richiedono SSE-C la crittografia devono essere abilitate deliberatamente SSE-C utilizzando l'operazione [PutBucketEncryption](#) API dopo aver creato un nuovo bucket. Per ulteriori informazioni su questa modifica, vedere. [SSE-C Impostazione predefinita per i nuovi bucket \(domande frequenti\)](#)

La sicurezza del cloud AWS è la massima priorità. Come AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS voi. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

Sicurezza del cloud

AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei [programmi di conformitàAWS](#). Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon S3, consulta [AWS Servizi coperti dal programma di conformità](#).

Sicurezza nel cloud

La tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili. Per Amazon S3, la tua responsabilità include le seguenti aree:

- Gestione dei dati, inclusa la [proprietà degli oggetti](#) e la [crittografia](#).

- Classificazione delle tue risorse.
- [Gestione degli accessi](#) ai tuoi dati tramite [ruoli IAM](#) e altre configurazioni di servizio per applicare le autorizzazioni appropriate.
- Abilitazione di controlli investigativi come [Amazon AWS CloudTrail GuardDuty](#) per Amazon S3.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando utilizzi Amazon S3. Gli argomenti seguenti descrivono come configurare Amazon S3 per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che possono aiutarti a monitorare e proteggere le tue risorse Amazon S3.

Note

Per ulteriori informazioni sull'uso della classe di storage Amazon S3 Express One Zone con i bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Argomenti

- [Best practice di sicurezza per Amazon S3](#)
- [Protezione dei dati in Amazon S3](#)
- [Protezione dei dati con la crittografia](#)
- [Riservatezza del traffico Internet](#)
- [Convalida della conformità per Amazon S3](#)
- [Resilienza in Amazon S3](#)
- [Sicurezza dell'infrastruttura in Amazon S3](#)
- [Analisi della configurazione e delle vulnerabilità in Amazon S3](#)
- [Gestione degli accessi](#)
- [Inventario dei dati Amazon Simple Storage Service](#)

Best practice di sicurezza per Amazon S3

Important

Amazon Simple Storage Service applica ora una nuova impostazione di sicurezza predefinita per i bucket che disabilita automaticamente la crittografia lato server con chiavi fornite dal cliente (SSE-C) per tutti i nuovi bucket generici. Nell'aprile 2026, Amazon S3 ha implementato un aggiornamento in modo che tutti i nuovi bucket generici abbiano la crittografia disabilitata per tutte le nuove richieste di scrittura. SSE-C Per i bucket esistenti senza oggetti SSE-C crittografati, Amazon S3 è disabilitato SSE-C anche per tutte le nuove richieste di scrittura. Account AWS Con questa modifica, le applicazioni che richiedono SSE-C la crittografia devono essere abilitate deliberatamente SSE-C utilizzando l'operazione [PutBucketEncryption](#) API dopo aver creato un nuovo bucket. Per ulteriori informazioni su questa modifica, vedere. [SSE-C Impostazione predefinita per i nuovi bucket \(domande frequenti\)](#)

Amazon S3 fornisce una serie di caratteristiche di sicurezza che occorre valutare durante lo sviluppo e l'implementazione delle policy di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per il tuo ambiente, considerale come consigli utili più che prescrizioni.

Argomenti

- [Best practice di sicurezza per Amazon S3](#)
- [Best practice di monitoraggio e audit di Amazon S3](#)
- [Monitoraggio della sicurezza dei dati con managed AWS servizi di sicurezza](#)

Best practice di sicurezza per Amazon S3

Le seguenti best practice per Amazon S3 consentono di evitare incidenti di sicurezza.

Disabilitare le liste di controllo degli accessi (ACL)

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare ACL. Per impostazione predefinita, l'opzione Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le ACL sono disabilitate. Quando le ACL sono disabilitate, il proprietario

del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ai dati in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte dei casi d'uso moderno in Amazon S3 non richiede più l'uso di [liste di controllo degli accessi \(ACL\)](#). È consigliabile disabilitare le ACL, tranne in circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Per disabilitare le ACL e assumere la proprietà di ogni oggetto del tuo bucket, applica l'impostazione Bucket owner enforced (Applicata da proprietario bucket) per S3 Object Ownership. Quando si disabilitano le ACL, è possibile mantenere facilmente un bucket con oggetti caricati da diversi Account AWS.

Quando le ACL sono disabilitate, il controllo degli accessi per i dati è basato su policy, come quelle elencate di seguito:

- AWS Identity and Access Management politiche per gli utenti (IAM)
- Policy di bucket S3
- Policy di endpoint del cloud privato virtuale (VPC)
- AWS Organizations politiche di controllo dei servizi (SCP)
- AWS Organizations politiche di controllo delle risorse (RCP)

La disabilitazione delle ACL semplifica la gestione e il controllo delle autorizzazioni. Per impostazione predefinita, le ACL sono disabilitate per nuovi bucket. È anche possibile disabilitare le ACL per i bucket esistenti. Se hai un bucket esistente che contiene già oggetti, dopo aver disabilitato le ACL, l'oggetto e le ACL bucket non fanno più parte del processo di valutazione dell'accesso. L'accesso è invece concesso o negato in base alle policy.

Prima di disabilitare le ACL, assicurati di eseguire la seguente procedura:

- Esamina la policy del bucket per assicurarti che copra tutti i modi in cui intendi concedere l'accesso al bucket al di fuori del tuo account.
- Ripristina le impostazioni di default del bucket ACL (controllo completo per il proprietario del bucket).

Dopo aver disabilitato le ACL, si verificano i seguenti comportamenti:

- Il bucket accetta solo richieste PUT che non specificano un ACL o richieste PUT con ACL di controllo completo del proprietario del bucket. Queste ACL includono l'ACL predefinita bucket-owner-full-control o forme equivalenti di questa ACL espresse in XML.
- Le applicazioni esistenti che supportano le ACL di controllo completo del proprietario del bucket non subiranno alcun impatto.

- PUTLe richieste che contengono altri ACL (ad esempio, concessioni personalizzate a determinati utenti Account AWS) hanno esito negativo e restituiscono un codice di stato HTTP 400 (Bad Request) con il codice di errore. AccessControlListNotSupported

Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Verifica che i bucket Amazon S3 utilizzino le policy corrette e non siano accessibili pubblicamente

A meno che non venga richiesto in maniera esplicita che gli utenti su Internet siano in grado di leggere o scrivere nel bucket S3, assicurati che il bucket S3 non sia pubblico. Di seguito sono riportate alcune delle fasi che è possibile eseguire per bloccare l'accesso pubblico:

- Utilizza Blocco dell'accesso pubblico S3. Con il Blocco dell'accesso pubblico, è possibile configurare facilmente controlli centralizzati per limitare l'accesso pubblico alle risorse Amazon S3. Questi controlli centralizzati vengono applicati a prescindere da come vengono create le risorse. Per le organizzazioni che gestiscono più AWS account, è ora possibile utilizzare l'applicazione AWS Organizations a livello di organizzazione per gestire centralmente le impostazioni di S3 Block Public Access in tutta l'organizzazione con un'unica configurazione di policy.

Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

- Identifica le policy di bucket Amazon S3 che consentono l'uso di un'identità jolly, ad esempio "Principal": "*" (che significa di fatto "tutti"). Inoltre, cerca policy che consentono un'azione jolly "*" (che di fatto consente all'utente di eseguire qualsiasi azione nel bucket Amazon S3).
- Allo stesso modo, cerca gli elenchi di controllo degli accessi (ACL) di Amazon S3 che forniscano accesso in lettura, scrittura o completo a «Tutti» o «Qualsiasi utente autenticato». AWS
- Utilizza l'operazione API ListBuckets per eseguire la scansione di tutti i bucket Amazon S3. Quindi, utilizza GetBucketAcl, GetBucketWebsite e GetBucketPolicy per determinare se ciascun bucket dispone di controlli sugli accessi conformi e configurazione conforme.
- Utilizza [AWS Trusted Advisor](#) per ispezionare l'implementazione di Amazon S3.
- Valuta se implementare controlli di rilevamento continui utilizzando [s3-bucket-public-read-prohibited](#) e [s3-bucket-public-write-prohibited](#) gestito Regole di AWS Config.

Per le organizzazioni con più AWS account, valuta la possibilità di utilizzare la gestione Block Public Access a livello di organizzazione:

- Gestione centralizzata delle policy: consente di AWS Organizations creare un'unica policy S3 Block Public Access che si applica automaticamente a tutti gli account dei membri o alle unità organizzative (OU) selezionate.
- Ereditarietà automatica: quando si allega la policy a livello root o di unità organizzativa, i nuovi account membri ereditano automaticamente le impostazioni di blocco dell'accesso pubblico senza la configurazione di un singolo account.
- Conformità semplificata: Organization-level le policy eliminano la necessità di mantenere complesse Service Control Policy (SCP) per l'applicazione dei Block Public Access e riducono il sovraccarico operativo legato alla gestione delle configurazioni dei singoli account.
- Funzionalità di audit: utilizzate AWS CloudTrail per monitorare l'applicazione e l'applicazione delle policy negli account dei membri per il monitoraggio della conformità.

Per ulteriori informazioni, consulta [Identity and Access Management per Amazon S3](#).

Mantieni la crittografia lato server con le chiavi fornite dal cliente (SSE-C) disattivata a meno che il carico di lavoro non lo richieda

A partire da aprile 2026, Amazon S3 si disattiva automaticamente SSE-C per tutti i nuovi bucket generici e per i bucket esistenti negli account senza oggetti crittografati. SSE-C Ti consigliamo di mantenerlo SSE-C disabilitato a meno che il carico di lavoro non abbia un requisito specifico per questa offerta di crittografia.

SSE-C richiede di fornire la chiave di crittografia con ogni richiesta di lettura o scrittura di oggetti crittografati. Ciò rende poco pratico condividere l'accesso con altri utenti, ruoli o AWS servizi che operano sui tuoi dati. Gli oggetti crittografati con SSE-C non possono essere decrittografati in modo nativo dai servizi gestiti. AWS Per la maggior parte dei carichi di lavoro, la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) o chiavi AWS KMS () offre una protezione equivalente con maggiore flessibilità. SSE-KMS

Se disponi di bucket esistenti in cui SSE-C è ancora abilitato, verifica se è ancora necessario e bloccalo in caso contrario. Quando SSE-C è bloccata PutObject CopyObjectPostObject, qualsiasi richiesta di replica o caricamento in più parti che specifichi la SSE-C crittografia viene rifiutata con un errore HTTP 403. AccessDenied

Per ulteriori informazioni sul blocco, consulta. SSE-C [the section called “Blocco o sblocco SSE-C”](#)

Crea bucket nel namespace regionale del tuo account

Per impostazione predefinita, crei bucket globali per uso generico nello spazio dei nomi globale condiviso. Dopo aver creato un bucket generico nello spazio dei nomi globale condiviso, il nome

del bucket non può essere creato da nessun altro all'interno della partizione. Quando elimini un bucket globale per uso generico, il nome del bucket diventa nuovamente disponibile nello spazio dei nomi globale per essere ricreato da chiunque.

Sebbene i bucket generici di Amazon S3 esistano in uno spazio dei nomi globale condiviso, puoi facoltativamente creare bucket nello spazio dei nomi regionale del tuo account. Il namespace regionale dell'account è una suddivisione riservata dello spazio dei nomi dei bucket globale in cui solo il tuo account può creare bucket generici. Ti consigliamo di creare bucket nel namespace regionale del tuo account poiché questi bucket sono unici per il tuo account e non possono mai essere ricreati da un altro account. Per ulteriori informazioni, consulta [Namespace per bucket generici](#).

Ti consigliamo di non eliminare i bucket globali per uso generico nel namespace globale condiviso. Tutti gli AWS account ora hanno una quota predefinita di 10.000 bucket, il che riduce la necessità di eliminare i bucket vuoti dal tuo account. Se elimini un bucket nello spazio dei nomi globale condiviso, tieni presente che un altro AWS account nella stessa partizione può utilizzare lo stesso nome di bucket per un nuovo bucket e quindi può potenzialmente ricevere richieste destinate al bucket eliminato. Per evitare che ciò accada o continuare a utilizzare lo stesso nome del bucket, non eliminare il bucket. Ti consigliamo di eliminare solo il contenuto del bucket. Invece di eliminare il bucket, blocca tutte le richieste del bucket, se necessario. Per i bucket non più in uso, è consigliabile eliminare tutti gli oggetti del bucket per ridurre al minimo i costi e mantenere il bucket stesso. Per ulteriori informazioni, consulta [Eliminazione di un bucket per uso generico](#).

Applica l'accesso con privilegi minimi

Quando concedi le autorizzazioni, puoi decidere quali autorizzazioni assegnare, a chi e per quali risorse Amazon S3. Puoi abilitare operazioni specifiche che desideri consentire su tali risorse. Pertanto, è consigliabile concedere solo le autorizzazioni necessarie richieste per eseguire un'attività. L'implementazione dell'accesso con privilegi minimi è fondamentale per ridurre i rischi di sicurezza e l'impatto risultante da errori o intenzioni dannose.

Gli strumenti seguenti sono disponibili per implementare l'accesso con privilegi minimi:

- [Azioni di policy per Amazon S3](#) e [Limiti delle autorizzazioni per le entità IAM](#)
- [Come funziona Amazon S3 con IAM](#)
- [Panoramica delle liste di controllo accessi \(ACL\)](#)

Per indicazioni sugli aspetti da tenere in considerazione quando scegli uno o più dei meccanismi precedenti, consulta [Identity and Access Management per Amazon S3](#).

Usa i ruoli IAM per le applicazioni che richiedono l'accesso ad Amazon S3 Servizi AWS

Affinché le applicazioni in esecuzione su Amazon EC2 o altro possano accedere Servizi AWS alle risorse Amazon S3, devono includere AWS credenziali valide nelle loro richieste API. AWS Consigliamo di non archiviare AWS le credenziali direttamente nell'applicazione o nell'istanza Amazon EC2. Si tratta di credenziali a lungo termine che non vengono automaticamente ruotate e potrebbero avere un impatto aziendale significativo se vengono compromesse.

Utilizza invece un ruolo IAM per gestire credenziali temporanee per le applicazioni o i servizi che devono accedere ad Amazon S3. Quando si utilizza un ruolo, non è necessario distribuire credenziali a lungo termine (come nome utente e password o chiavi di accesso) a un'istanza Amazon EC2 o Servizio AWS, ad esempio, AWS Lambda Il ruolo fornisce autorizzazioni temporanee che le applicazioni possono utilizzare quando effettuano chiamate ad altre risorse. AWS

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente IAM:

- [Ruoli IAM](#)
- [Scenari comuni per ruoli: utenti, applicazioni e servizi](#)

Prendi in considerazione la crittografia dei dati inattivi

Per la protezione dei dati inattivi in Amazon S3 sono disponibili le opzioni seguenti:

- Server-side crittografia: tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita e tutti i nuovi oggetti caricati in un bucket S3 vengono crittografati automaticamente quando sono inattivi. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket in Amazon S3. Per utilizzare un diverso tipo di crittografia, puoi specificare il tipo di crittografia lato server da utilizzare nelle richieste PUT S3 oppure impostare la configurazione di crittografia predefinita nel bucket di destinazione.

Anche Amazon S3 offre queste opzioni di crittografia lato server:

- Server-side crittografia con chiavi AWS Key Management Service (AWS KMS) () SSE-KMS
- Dual-layer crittografia lato server con chiavi AWS Key Management Service (AWS KMS) () DSSE-KMS
- Server-side crittografia con chiavi fornite dal cliente () SSE-C

Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia lato server](#).

- Client-side crittografia: crittografa i dati lato client e carica i dati crittografati su Amazon S3. In questo caso, è l'utente a gestire la procedura di crittografia, nonché le chiavi e gli strumenti correlati. Come per la crittografia lato server, la crittografia lato client riduce i rischi crittografando i dati con una chiave che viene archiviata in un meccanismo diverso rispetto a quello utilizzato per archiviare i dati stessi.

Amazon S3 fornisce più opzioni di crittografia lato client. Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia lato client](#).

Applica la crittografia dei dati in transito

Puoi utilizzare HTTPS (TLS) per impedire a potenziali aggressori di intercettare o manipolare traffico di rete utilizzando attacchi di tipo person-in-the-middle o simili. Si consiglia di consentire solo connessioni crittografate su HTTPS (TLS) utilizzando la condizione [aws:SecureTransport](#) nelle policy di bucket Amazon S3. Per ulteriori informazioni, consulta l'esempio di policy di bucket S3 [Gestione dell'accesso in base a richieste HTTP o HTTPS](#). Oltre a rifiutare le richieste HTTP, ti consigliamo di impostare degli CloudWatch allarmi Amazon che ti avvisino se vengono effettuati tentativi di accesso HTTP ai tuoi contenuti. `tlsDetails.tlsVersion NOT EXISTS` Per ulteriori informazioni su come configurare gli CloudWatch allarmi di Amazon, consulta [Creazione di CloudWatch allarmi per CloudTrail eventi: esempi](#) e contenuti di [CloudTrail registrazione](#) nella Guida per l'utente. AWS CloudTrail

Important

Consigliamo che la tua applicazione non blocchi i certificati TLS di Amazon S3 in quanto AWS non supporta il blocco di certificati pubblicamente attendibili. S3 rinnova automaticamente i certificati e il rinnovo può avvenire in qualsiasi momento prima della scadenza del certificato. Il rinnovo di un certificato genera una nuova coppia di chiavi pubbliche e private. Se si è appuntato un certificato S3 che è stato recentemente rinnovato con una nuova chiave pubblica, non sarà possibile connettersi a S3 finché l'applicazione non utilizzerà il nuovo certificato.

Inoltre, valuta se implementare controlli di rilevamento continui utilizzando la regola [s3-bucket-ssl-requests-only](#) gestita da AWS Config .

Valutazione dell'utilizzo di S3 Object Lock

Con S3 Object Lock, puoi archiviare gli oggetti utilizzando il modello "Write Once Read Many" (WORM). Il blocco oggetti S3 può contribuire a evitare l'eliminazione accidentale o

inappropriata dei dati. Ad esempio, puoi utilizzare S3 Object Lock per proteggere i tuoi log. AWS CloudTrail

Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).

Abilitazione del controllo delle versioni S3

Il controllo delle versioni S3 è un modo per conservare più versioni di un oggetto nello stesso bucket. Si può utilizzare questa funzione per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket . Con la funzione Controllo delle versioni si può facilmente eseguire il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente.

Inoltre, valuta se implementare controlli di rilevamento continui utilizzando la regola [s3-bucket-versioning-enabled](#) gestita da AWS Config .

Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Prendi in considerazione l'utilizzo di S3 Replication Cross-Region

Sebbene Amazon S3 per impostazione predefinita archivi i dati in più zone di disponibilità geograficamente distanti, per soddisfare i requisiti di conformità potrebbe essere necessario archivarli a distanze ancora maggiori. Con S3 Cross-Region Replication (CRR), puoi replicare i dati tra distanti Regioni AWS per soddisfare questi requisiti. Il CRR consente la copia automatica e asincrona di oggetti tra bucket diversi. Regioni AWS Per ulteriori informazioni, consulta [Replica di oggetti all'interno e tra le Regioni](#).

Note

CRR richiede che il controllo delle versioni sia abilitato per i bucket S3 di origine e destinazione.

Inoltre, valuta se implementare controlli di rilevamento continui utilizzando la regola [s3-bucket-replication-enabled](#) gestita da AWS Config .

Valutazione dell'utilizzo degli endpoint VPC per l'accesso ad Amazon S3

Un endpoint Virtual Private Cloud (VPC) Amazon S3 è un'entità logica all'interno di un VPC che consente la connettività solo ad Amazon S3. Gli endpoint VPC impediscono al traffico di attraversare la rete Internet aperta.

Gli endpoint VPC per Amazon S3 offrono diversi modi per controllare l'accesso ai dati di Amazon S3:

- È possibile controllare le richieste, gli utenti o i gruppi autorizzati tramite un endpoint VPC specifico utilizzando policy del bucket S3.
- È possibile controllare quali VPC o endpoint VPC hanno accesso ai bucket S3 utilizzando le policy di bucket S3.
- Puoi impedire l'esfiltrazione di dati utilizzando un VPC che non dispone di un Internet gateway.

Per ulteriori informazioni, consulta [Controllo dell'accesso dagli endpoint VPC con policy di bucket](#).

Utilizza servizi di sicurezza gestiti AWS per monitorare la sicurezza dei dati

Diversi servizi AWS di sicurezza gestiti possono aiutarti a identificare, valutare e monitorare i rischi di sicurezza e conformità per i tuoi dati Amazon S3. Questi servizi consentono anche di proteggere i dati da tali rischi. Questi servizi includono funzionalità automatiche di rilevamento, monitoraggio e protezione progettate per scalare dalle risorse Amazon S3 per una singola risorsa Account AWS alle risorse per organizzazioni con migliaia di account.

Per ulteriori informazioni, consulta [Monitoraggio della sicurezza dei dati con managed AWS servizi di sicurezza](#).

Best practice di monitoraggio e audit di Amazon S3

Le best practice seguenti per Amazon S3 consentono di rilevare potenziali debolezze e incidenti di sicurezza.

Identificazione e audit di tutti i bucket Amazon S3

L'identificazione degli asset IT è un aspetto essenziale di governance e sicurezza. È richiesta la visibilità di tutte le risorse Amazon S3 per valutare il loro assetto di sicurezza e intervenire su aree di debolezza potenziali. Per eseguire l'audit delle risorse, procedi come segue:

- Utilizza Tag Editor per identificare e applicare tag a risorse sensibili alla sicurezza e risorse sensibili al controllo; quindi, utilizza questi tag quando devi cercare le risorse. Per ulteriori informazioni, consulta [Searching for Resources to Tagging](#) nella Tagging AWS Resources User Guide.
- Utilizza S3 Inventory per eseguire l'audit e creare report sullo stato di replica e crittografia degli oggetti per esigenze aziendali, di conformità e normative. Per ulteriori informazioni, consulta [Catalogazione e analisi dei dati con Inventario S3](#).

- Crea gruppi di risorse per le risorse Amazon S3. Per ulteriori informazioni, consulta [Che cosa sono i gruppi di risorse?](#) nella Guida per l'utente di AWS Resource Groups .

Implementa il monitoraggio utilizzando strumenti AWS di monitoraggio

Il monitoraggio è una parte importante per mantenere l'affidabilità, la sicurezza, la disponibilità e le prestazioni di Amazon S3 e delle tue AWS soluzioni. AWS fornisce diversi strumenti e servizi per aiutarti a monitorare Amazon S3 e gli altri. Servizi AWS Ad esempio, puoi monitorare le CloudWatch metriche di Amazon per Amazon S3, in particolare le metriche `PutRequests`, `GetRequests4xxErrors`, e `DeleteRequests` Per ulteriori informazioni, consulta [Metriche di monitoraggio con Amazon CloudWatch](#) e [Registrazione e monitoraggio in Amazon S3](#).

Per un secondo esempio, consulta [Esempio: attività del bucket Amazon S3](#). Questo esempio descrive come creare un CloudWatch allarme che viene attivato quando viene effettuata una chiamata all'API Amazon S3 a una bucket policy, a PUT DELETE un bucket lifecycle, a una configurazione di replica del bucket o a un bucket ACL. PUT

Abilita la registrazione degli accessi al server Amazon S3

La registrazione degli accessi al server fornisce record dettagliati delle richieste che sono effettuate a un bucket. I log di accesso al server possono essere utili durante gli audit di sicurezza e accesso, per conoscere la base clienti e comprendere la fattura Amazon S3. Per istruzioni sull'abilitazione della registrazione degli accessi al server, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

Considera anche l'implementazione di controlli investigativi continui utilizzando la regola gestita. [s3-bucket-logging-enabled](#) AWS Config

Utilizza AWS CloudTrail

AWS CloudTrail fornisce un registro delle azioni intraprese da un utente, da un ruolo o da un utente Servizio AWS in Amazon S3. Puoi utilizzare le informazioni raccolte da CloudTrail per determinare quanto segue:

- La richiesta effettuata ad Amazon S3
- L'indirizzo IP dal quale è stata effettuata la richiesta
- L'utente che ha effettuato la richiesta
- L'ora in cui è stata effettuata la richiesta
- Dettagli aggiuntivi relativi alla richiesta

Ad esempio, è possibile identificare le CloudTrail voci relative alle PUT azioni che influiscono sull'accesso ai dati `PutBucketAcl`, in particolare `PutObjectAcl`, `PutBucketPolicy`, e `PutBucketWebsite`.

Quando si configura Account AWS, CloudTrail è abilitato per impostazione predefinita. Puoi visualizzare gli eventi recenti nella CloudTrail console. Per creare un record continuo di attività ed eventi per i tuoi bucket Amazon S3, puoi creare un percorso nella CloudTrail console. Per ulteriori informazioni, consultare [Registrazione di eventi di dati](#) nella Guida per l'utente di AWS CloudTrail .

Quando crei un percorso, puoi configurare la registrazione degli eventi relativi CloudTrail ai dati. Gli eventi di dati sono le registrazioni delle operazioni eseguite per una risorsa o al suo interno. In Amazon S3, gli eventi di dati registrano l'attività API a livello di oggetto per singoli bucket. CloudTrail supporta un sottoinsieme di operazioni API a livello di oggetto di Amazon S3, come, e. `GetObject` `DeleteObject` `PutObject` Per ulteriori informazioni su come CloudTrail funziona con Amazon S3, consulta. [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#) Nella console di Amazon S3, puoi configurare i tuoi bucket S3 anche su [Abilitazione della registrazione CloudTrail degli eventi per bucket e oggetti S3](#).

AWS Config fornisce una regola gestita (`cloudtrail-s3-dataevents-enabled`) che puoi utilizzare per confermare che almeno un CloudTrail percorso stia registrando eventi di dati per i tuoi bucket S3. Per ulteriori informazioni, consulta la sezione [cloudtrail-s3-dataevents-enabled](#) nella Guida per gli sviluppatori di AWS Config .

Attiva AWS Config

Alcune delle best practice elencate in questo argomento suggeriscono la creazione di regole. AWS Config ti aiuta a valutare, controllare e valutare le configurazioni delle tue AWS risorse. AWS Config monitora le configurazioni delle risorse in modo da poter valutare le configurazioni registrate rispetto alle configurazioni sicure desiderate. Con AWS Config, puoi fare quanto segue:

- Rivedere le modifiche nelle configurazioni e nelle relazioni tra le risorse AWS
- Investigare le cronologie dettagliate della configurazione delle risorse
- Determinare la conformità complessiva rispetto alle configurazioni specificate nelle linee guida interne

L'utilizzo AWS Config può aiutarti a semplificare il controllo di conformità, l'analisi della sicurezza, la gestione delle modifiche e la risoluzione dei problemi operativi. Per ulteriori informazioni,

consulta [Configurazione AWS Config con la console](#) nella Guida per gli AWS Config sviluppatori. Durante la specifica dei tipi di risorse da registrare, assicurati di includere le risorse Amazon S3.

 Important

AWS Config managed rules supporta solo bucket generici nella valutazione delle risorse Amazon S3. AWS Config non registra le modifiche alla configurazione per i bucket di directory. Per ulteriori informazioni, consulta Regole [AWS Config gestite](#) e [Elenco delle regole AWS Config gestite](#) nella Guida per gli AWS Config sviluppatori.

Per un esempio di utilizzo AWS Config, consulta [How to Use to Monitor and Response AWS Config to Monitor and Response to Bucket di Amazon S3 che consentono l'accesso](#) pubblico nel AWS Security Blog.

Utilizzo di S3 Storage Lens

S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti. S3 Storage Lens analizza i parametri di archiviazione per fornire raccomandazioni contestuali che puoi usare per ottimizzare i costi di archiviazione e applicare le best practice sulla protezione dei dati.

Con S3 Storage Lens puoi usare i parametri per generare approfondimenti, ad esempio per scoprire la quantità di spazio di archiviazione disponibile nell'intera organizzazione o quali sono i bucket e i prefissi caratterizzati da una crescita più rapida. Puoi utilizzare i parametri di Amazon S3 Storage Lens anche per individuare le opportunità di ottimizzazione dei costi, implementare le best practice di protezione dei dati e gestione degli accessi e migliorare le prestazioni dei carichi di lavoro delle applicazioni.

Ad esempio, puoi identificare i bucket che non hanno regole del ciclo di vita S3 per interrompere i caricamenti in più parti incompleti che risalgono a più di 7 giorni. Puoi anche individuare i bucket non conformi alle best practice di protezione dei dati, come quelli che usano la replica S3 o il controllo delle versioni S3. Per maggiori informazioni, consulta [Informazioni su Amazon S3 Storage Lens](#).

Monitora i suggerimenti di sicurezza di AWS

È opportuno controllare regolarmente i consigli di sicurezza pubblicati in Trusted Advisor per il tuo Account AWS. In particolare, cerca gli avvisi relativi ai bucket Amazon S3 con "autorizzazioni

di accesso aperte". Puoi eseguire questa operazione a livello di codice o utilizzando [describe-trusted-advisor-checks](#).

Inoltre, monitora attivamente l'indirizzo email principale registrato da ciascuno dei tuoi Account AWS. AWS utilizza questo indirizzo email per contattarti in merito a problemi di sicurezza emergenti che potrebbero interessarti.

AWS i problemi operativi di ampio impatto sono pubblicati su [Dashboard AWS Health - Salute del servizio](#). I problemi operativi sono anche pubblicati sui singoli account tramite Dashboard AWS Health. Per ulteriori informazioni, consulta la [documentazione relativa ad AWS Health](#).

Monitoraggio della sicurezza dei dati con managed AWS servizi di sicurezza

Diversi servizi AWS di sicurezza gestiti possono aiutarti a identificare, valutare e monitorare i rischi di sicurezza e conformità per i tuoi dati Amazon S3. Consentono anche di proteggere i dati da tali rischi. Questi servizi includono funzionalità automatiche di rilevamento, monitoraggio e protezione progettate per scalare dalle risorse Amazon S3 per una singola risorsa Account AWS alle risorse per organizzazioni che coprono migliaia di persone. Account AWS

AWS i servizi di rilevamento e risposta possono aiutarti a identificare potenziali configurazioni errate di sicurezza, minacce o comportamenti imprevisti, in modo da poter rispondere rapidamente ad attività potenzialmente non autorizzate o dannose nel tuo ambiente. AWS i servizi di protezione dei dati possono aiutarti a monitorare e proteggere dati, account e carichi di lavoro da accessi non autorizzati. Inoltre, consentono di individuare dati sensibili, come informazioni di identificazione personale (PII), nel tuo patrimonio di dati Amazon S3.

Per semplificare l'identificazione e la valutazione dei rischi di sicurezza e conformità dei dati, i servizi di sicurezza AWS gestiti generano risultati per segnalare potenziali eventi o problemi di sicurezza con i dati Amazon S3. I risultati forniscono dettagli rilevanti che possono essere utilizzati per analizzare, valutare e agire su questi rischi in base ai flussi di lavoro e alle policy di risposta agli eventi imprevisti. È possibile accedere direttamente ai dati dei risultati utilizzando ciascun servizio. Inoltre, è possibile inviare i dati ad altre applicazioni, servizi e sistemi, ad esempio il sistema SIEM (Security Incident and Event Management).

Per monitorare la sicurezza dei tuoi dati Amazon S3, prendi in considerazione l'utilizzo di questi servizi di sicurezza gestiti AWS .

Amazon GuardDuty

Amazon GuardDuty è un servizio di rilevamento delle minacce che monitora continuamente i tuoi Account AWS carichi di lavoro per individuare eventuali attività dannose e fornisce risultati di sicurezza dettagliati per visibilità e risoluzione.

Con la funzionalità di protezione S3 GuardDuty, puoi configurare GuardDuty per analizzare la AWS CloudTrail gestione e gli eventi relativi ai dati per le tue risorse Amazon S3. GuardDuty quindi monitora tali eventi per individuare attività dannose e sospette. Per informare l'analisi e identificare i potenziali rischi per la sicurezza, GuardDuty utilizza feed di intelligence sulle minacce e apprendimento automatico.

GuardDuty è in grado di monitorare diversi tipi di attività per le tue risorse Amazon S3. Ad esempio, gli eventi di CloudTrail gestione per Amazon S3 includono operazioni a livello di bucket, come `ListBuckets`, e `DeleteBucket PutBucketReplication`. CloudTrail gli eventi di dati per Amazon S3 includono operazioni a livello di oggetto, come, e `GetObject ListObjects PutObject`. Se GuardDuty rileva attività anomale o potenzialmente dannose, genera un risultato per avvisarti.

Per ulteriori informazioni, consulta [Amazon S3 Protection in Amazon GuardDuty](#) nella Amazon User Guide. GuardDuty

Amazon Detective

Amazon Detective semplifica il processo di analisi e consente di condurre indagini sulla sicurezza più rapide ed efficaci. Detective fornisce aggregazioni di dati, riepiloghi e contesto predefiniti che facilitano l'analisi e la valutazione della natura e dell'estensione dei possibili problemi di sicurezza.

Detective estrae automaticamente gli eventi basati sul tempo, come le chiamate API AWS CloudTrail e i log di flusso di Amazon VPC per le tue risorse. AWS Inoltre, acquisisce i risultati generati da Amazon. GuardDuty Detective utilizza quindi machine learning, l'analisi statistica e la teoria dei grafi per generare visualizzazioni che consentono di condurre indagini sulla sicurezza efficaci più rapidamente.

Queste visualizzazioni forniscono una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni tra di esse nel tempo. È possibile esplorare questo grafico del comportamento per esaminare possibili azioni dannose, come tentativi di accesso non riusciti o chiamate API sospette. È anche possibile vedere in che modo queste azioni interessano le risorse, come bucket e oggetti S3.

Per ulteriori informazioni, consultare la [Guida di amministrazione di Amazon Detective](#).

Sistema di analisi degli accessi IAM

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) può aiutarti a identificare le risorse condivise con un'entità esterna. Puoi anche utilizzare IAM Access Analyzer per convalidare le policy IAM rispetto alla grammatica delle policy e alle best practice e generare policy IAM in base all'attività di accesso nei tuoi log. AWS CloudTrail

IAM Access Analyzer utilizza un ragionamento basato sulla logica per analizzare le politiche relative alle risorse nel tuo AWS ambiente, come le bucket policy. Con IAM Access Analyzer for S3, ricevi un avviso quando un bucket S3 è configurato per consentire l'accesso a chiunque su Internet o altro, compresi gli account esterni alla tua organizzazione. Account AWS Ad esempio, IAM Access Analyzer for S3 può segnalare che un bucket ha un accesso in lettura o scrittura fornito tramite una bucket access control list (ACL), una bucket policy, una policy Access Point o una policy di access point. Multi-Region Per ogni bucket pubblico o condiviso, vengono visualizzati risultati che indicano l'origine e il livello di accesso pubblico o condiviso. Con questi risultati puoi eseguire azioni correttive immediate e precise per ripristinare l'accesso del bucket desiderato.

Per ulteriori informazioni, consulta [Revisione dell'accesso al bucket tramite IAM Access Analyzer per S3](#).

Amazon Macie

Amazon Macie è un servizio di sicurezza che rileva dati sensibili utilizzando il machine learning e la corrispondenza del modello. Macie fornisce visibilità sui rischi legati alla sicurezza dei dati e consente una protezione automatizzata da tali rischi. Con Macie, puoi automatizzare l'individuazione e la creazione di report dei dati sensibili nel tuo patrimonio di dati Amazon S3 per una migliore comprensione dei dati archiviati dall'organizzazione in S3.

Per individuare dati sensibili con Macie, puoi utilizzare criteri e tecniche integrati progettati per rilevare un elenco ampio e in continua espansione di tipi di dati sensibili per molti Paesi e regioni. Questi tipi di dati sensibili includono diversi tipi di informazioni di identificazione personale (PII), dati finanziari e dati delle credenziali. Puoi anche utilizzare criteri personalizzati: espressioni regolari che definiscono modelli di testo da abbinare e, facoltativamente, sequenze di caratteri e regole di prossimità per perfezionare i risultati.

Se Macie rileva dati sensibili in un oggetto S3, genera un risultato relativo alla sicurezza per informare l'utente. Questo risultato fornisce informazioni sull'oggetto interessato, i tipi e il numero di occorrenze dei dati sensibili individuati da Macie e dettagli aggiuntivi per facilitare l'analisi del

bucket S3 e dell'oggetto interessati. Per ulteriori informazioni, consultare la [Guida per l'utente di Amazon Macie](#).

AWS Security Hub CSPM

AWS Security Hub CSPM è un servizio di gestione dello stato di sicurezza che esegue controlli delle migliori pratiche di sicurezza, aggrega avvisi e risultati provenienti da più fonti in un unico formato e consente la correzione automatica.

Security Hub CSPM raccoglie e fornisce dati sui risultati di sicurezza provenienti da soluzioni di AWS Partner Network sicurezza integrate Servizi AWS, tra cui Amazon Detective, Amazon IAM Access Analyzer e Amazon Macie. GuardDuty Genera inoltre i propri risultati eseguendo controlli di sicurezza continui e automatizzati basati sulle AWS migliori pratiche e sugli standard di settore supportati.

Security Hub CSPM quindi correla e consolida i risultati tra i fornitori per aiutarti a stabilire le priorità ed elaborare i risultati più significativi. Inoltre, fornisce supporto per azioni personalizzate, che possono essere utilizzate per richiamare risposte o azioni correttive per classi specifiche di risultati.

Con Security Hub CSPM, puoi valutare lo stato di sicurezza e conformità delle tue risorse Amazon S3 e puoi farlo come parte di un'analisi più ampia dello stato di sicurezza della tua organizzazione in singole e in più regioni. Regioni AWS Ciò include l'analisi delle tendenze di sicurezza e l'identificazione dei problemi di sicurezza con priorità massima. È anche possibile aggregare i risultati di più Regioni AWS e monitorare ed elaborare i dati dei risultati aggregati di una singola regione.

Per ulteriori informazioni, consultare la sezione relativa ai [controlli Amazon Simple Storage Service](#) nella Guida per l'utente di AWS Security Hub CSPM .

Protezione dei dati in Amazon S3

Amazon S3 offre un'infrastruttura di storage estremamente durevole, concepita per lo storage dei dati mission-critical e primari. S3 Standard, S3, S3 Intelligent-Tiering Standard-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive archiviano in modo ridondante gli oggetti su più dispositivi in un minimo di tre zone di disponibilità in un Regione AWS. Una zona di disponibilità consiste in uno o più data center separati con alimentazione, rete e connettività ridondanti in una Regione AWS. Le zone di disponibilità sono fisicamente separate da una distanza significativa, di diversi chilometri, da qualsiasi altra zona di disponibilità, anche se tutte si trovano

nel raggio di 100 km (60 miglia) l'una dall'altra. La classe di storage S3 One archivia i dati in modo ridondante su più dispositivi all'interno di un'unica zona di disponibilità. Zone-IA Questi servizi sono progettati per far fronte ai guasti simultanei dei dispositivi rilevando e riparando rapidamente eventuali perdite di ridondanza e controllano regolarmente l'integrità dei dati utilizzando checksum.

Lo storage standard Amazon S3 offre le seguenti caratteristiche:

- Sostenuto dall'[Accordo sul livello di servizio \(SLA\) Amazon S3](#).
- È progettato per garantire una durabilità pari al 99.999999999% e una disponibilità degli oggetti pari al 99.99% per un determinato anno.
- S3 Standard, S3, S3 Intelligent-Tiering, S3 Glacier Instant Retrieval Standard-IA, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive sono tutti progettati per supportare i dati in caso di perdita di un'intera zona di disponibilità di Amazon S3.

Amazon S3 protegge ulteriormente i dati tramite la funzione Controllo delle versioni, che può essere impiegata per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Con la funzione Controllo delle versioni si può facilmente eseguire il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Per default, le richieste recuperano la versione più recente scritta. È comunque possibile recuperare versioni meno recenti di un oggetto specificandone la versione in una richiesta.

Oltre alla funzionalità S3 di controllo delle versioni, puoi anche utilizzare funzionalità Blocco dell'accesso pubblico Amazon S3 e Replica S3 per proteggere i tuoi dati. Per ulteriori informazioni, consulta [Protezione dei dati in Amazon S3](#).

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare account utente individuali con, in modo che a ciascun utente vengano concesse solo le autorizzazioni necessarie per adempiere alle proprie mansioni AWS Identity and Access Management lavorative.

Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Le best practice di sicurezza seguenti gestiscono anche la protezione dei dati in Amazon S3:

- [Implement server-side encryption](#)
- [Enforce encryption of data in transit](#)

- [Consider using Macie with Amazon S3](#)
- [Identify and audit all your Amazon S3 buckets](#)
- [Monitor Amazon Web Services security advisories](#)

Protezione dei dati con la crittografia

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite da Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

La protezione dei dati ha lo scopo di proteggere i dati sia in transito (durante la trasmissione verso e da Amazon S3), sia quando sono a riposo (ovvero quando sono archiviati su disco nei data center Amazon S3). Puoi proteggere i dati in transito utilizzando Secure Socket Layer Layer/Transport Security (SSL/TLS), che include lo scambio ibrido di chiavi post-quantistiche o la crittografia lato client. Per la protezione dei dati a riposo in Amazon S3 sono disponibili le opzioni seguenti:

- Server-side crittografia: Amazon S3 crittografa gli oggetti prima di salvarli sui dischi AWS dei data center e quindi decrittografa gli oggetti quando li scarichi.

Tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita e tutti i nuovi oggetti caricati in un bucket S3 vengono crittografati automaticamente quando sono inattivi. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket in Amazon S3. Per utilizzare un diverso tipo di crittografia, puoi specificare il tipo di crittografia lato server da utilizzare nelle richieste PUT S3 oppure aggiornare la configurazione di crittografia predefinita nel bucket di destinazione.

Se desideri specificare un tipo di crittografia diverso nelle tue PUT richieste, puoi utilizzare la crittografia lato server con () chiavi AWS Key Management Service (AWS KMS), la crittografia

lato server a doppio livello con chiavi (SSE-KMS) o la crittografia lato server con AWS KMS chiavi fornite dal cliente (DSSE-KMS). SSE-C Se desideri impostare una diversa configurazione di crittografia predefinita nel bucket di destinazione, puoi utilizzare o. SSE-KMS DSSE-KMS

Per ulteriori informazioni su come modificare la configurazione di crittografia predefinita per i bucket per uso generico, consulta [Configurazione della crittografia predefinita](#).

Quando modifichi la configurazione di crittografia predefinita del bucket in SSE-KMS, il tipo di crittografia degli oggetti Amazon S3 esistenti nel bucket non viene modificato. Per modificare il tipo di crittografia degli oggetti preesistenti dopo aver aggiornato la configurazione di crittografia predefinita in SSE-KMS, puoi utilizzare Amazon S3 Batch Operations. Si fornisce a Operazioni in batch S3 un elenco di oggetti e Operazioni in batch richiama la rispettiva operazione API. Puoi utilizzare l'[Copia oggetti](#) operazione per copiare oggetti esistenti e riscriverli nello stesso bucket degli oggetti crittografati SSE-KMS. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch](#) e il post [Come crittografare retroattivamente gli oggetti esistenti in Amazon S3 utilizzando Inventario S3, Amazon Athena e Operazioni in batch S3](#) nel Blog dell'archiviazione AWS.

Per ulteriori informazioni su ogni opzione della crittografia lato server, consulta [Protezione dei dati con la crittografia lato server](#).

Per configurare la crittografia lato server, consulta:

- [Specificare la crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#)
 - [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#)
 - [the section called “Specificando DSSE-KMS”](#)
 - [Specificare la crittografia lato server con chiavi fornite dal cliente \(\) SSE-C](#)
- Client-side crittografia: crittografi i tuoi dati sul lato client e carichi i dati crittografati su Amazon S3. In questo caso, è l'utente a gestire il processo di crittografia, nonché le chiavi e gli strumenti correlati.

Per configurare la crittografia lato client, vedi [Protezione dei dati con la crittografia lato client](#).

Per vedere quale percentuale di byte di archiviazione crittografati, puoi utilizzare i parametri di Amazon S3 Storage Lens. S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle

attività relative all'archiviazione di oggetti. Per ulteriori informazioni, consulta [Valutazione dell'attività e dell'utilizzo dello storage con S3 Storage Lens](#). Per un elenco completo dei parametri, consulta [Glossario dei parametri di S3 Storage](#).

Per ulteriori informazioni sulla crittografia lato server, sulla crittografia lato client e sulla crittografia in transito, consulta i seguenti argomenti.

Argomenti

- [Protezione dei dati con la crittografia lato server](#)
- [Protezione dei dati con la crittografia lato client](#)
- [Protezione dei dati in transito con crittografia](#)

Protezione dei dati con la crittografia lato server

Important

Amazon Simple Storage Service applica ora una nuova impostazione di sicurezza predefinita per i bucket che disabilita automaticamente la crittografia lato server con chiavi fornite dal cliente (SSE-C) per tutti i nuovi bucket generici. Nell'aprile 2026, Amazon S3 ha implementato un aggiornamento in modo che tutti i nuovi bucket generici abbiano la crittografia disabilitata per tutte le nuove richieste di scrittura. SSE-C Per i bucket esistenti senza oggetti SSE-C crittografati, Amazon S3 è disabilitato SSE-C anche per tutte le nuove richieste di scrittura. Account AWS Con questa modifica, le applicazioni che richiedono SSE-C la crittografia devono essere abilitate deliberatamente SSE-C utilizzando l'operazione [PutBucketEncryption](#) API dopo aver creato un nuovo bucket. Per ulteriori informazioni su questa modifica, vedere. [SSE-C Impostazione predefinita per i nuovi bucket \(domande frequenti\)](#)

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon

S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS
Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

Server-side la crittografia è la crittografia dei dati a destinazione da parte dell'applicazione o del servizio che li riceve. Amazon S3 crittografa i tuoi dati a livello di oggetto mentre li scrive sui dischi AWS dei data center e li decrittografa automaticamente quando accedi ad essi. Se la richiesta è autenticata e sono disponibili le autorizzazioni per l'accesso, non c'è differenza nelle modalità di accesso agli oggetti, crittografati o meno. Ad esempio, se si condividono gli oggetti tramite un URL prefirmato, quest'ultimo funziona nello stesso modo, sia per i dati crittografati che per quelli non crittografati. Inoltre, quando si richiede un elenco degli oggetti nel bucket, le operazioni API restituisce l'elenco di tutti gli oggetti, crittografati o meno.

Tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita e tutti i nuovi oggetti caricati in un bucket S3 vengono crittografati automaticamente quando sono inattivi. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket in Amazon S3. Per utilizzare un diverso tipo di crittografia, puoi specificare il tipo di crittografia lato server da utilizzare nelle richieste PUT S3 oppure aggiornare la configurazione di crittografia predefinita nel bucket di destinazione.

Se desideri specificare un tipo di crittografia diverso nelle tue PUT richieste, puoi utilizzare la crittografia lato server con () chiavi AWS Key Management Service (AWS KMS), la crittografia lato server a doppio livello con chiavi (SSE-KMS) o la crittografia lato server con AWS KMS chiavi fornite dal cliente (DSSE-KMS). SSE-C Se desideri impostare una diversa configurazione di crittografia predefinita nel bucket di destinazione, puoi utilizzare o. SSE-KMS DSSE-KMS

Per ulteriori informazioni su come modificare la configurazione di crittografia predefinita per i bucket per uso generico, consulta [Configurazione della crittografia predefinita](#).

Quando modifichi la configurazione di crittografia predefinita del bucket in SSE-KMS, il tipo di crittografia degli oggetti Amazon S3 esistenti nel bucket non viene modificato. Per modificare il tipo di crittografia degli oggetti preesistenti dopo aver aggiornato la configurazione di crittografia predefinita in SSE-KMS, puoi utilizzare Amazon S3 Batch Operations. Si fornisce a Operazioni in batch S3 un elenco di oggetti e Operazioni in batch richiama la rispettiva operazione API. Puoi utilizzare l'[Copia oggetti](#) per copiare oggetti esistenti e riscriverli nello stesso bucket degli oggetti crittografati SSE-KMS . Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le](#)

[operazioni in batch](#) e il post [Come crittografare retroattivamente gli oggetti esistenti in Amazon S3 utilizzando Inventario S3, Amazon Athena e Operazioni in batch S3](#) nel Blog dell'archiviazione AWS .

Note

Non è possibile applicare contemporaneamente tipi diversi di crittografia lato server a uno stesso oggetto.

Se devi crittografare gli oggetti esistenti, usa Operazioni in batch S3 e S3 Inventory. Per ulteriori informazioni, consulta [Crittografia di oggetti con Operazioni in batch Amazon S3](#) e [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch](#).

Quando si archiviano dati in Amazon S3, sono disponibili quattro opzioni reciprocamente esclusive per la crittografia lato server, a seconda di come si sceglie di gestire le chiavi di crittografia e del numero di livelli di crittografia da applicare.

Server-side crittografia con chiavi gestite da Amazon S3 () SSE-S3

Tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita. L'opzione predefinita per la crittografia lato server è con le chiavi gestite di Amazon S3 (). SSE-S3 Ogni oggetto è crittografato con una chiave univoca. Come protezione aggiuntiva, SSE-S3 crittografa la chiave stessa con una chiave root che ruota regolarmente. SSE-S3 utilizza uno dei più potenti cifrari a blocchi disponibili, Advanced Encryption Standard () a 256 bit, per crittografare i dati. AES-256 Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).

Server-side crittografia con AWS Key Management Service (AWS KMS) chiavi (SSE-KMS)

Server-side la crittografia con AWS KMS keys (SSE-KMS) viene fornita tramite un'integrazione del AWS KMS servizio con Amazon S3. Con AWS KMS, hai un maggiore controllo sulle tue chiavi. Ad esempio, puoi visualizzare le chiavi separate, modificare le policy di controllo e seguire le chiavi in AWS CloudTrail. Inoltre, puoi creare e gestire chiavi gestite dal cliente oppure utilizzare chiavi Chiavi gestite da AWS create appositamente per te, il tuo servizio e la tua regione. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#).

Dual-layer crittografia lato server con AWS Key Management Service (AWS KMS) chiavi () DSSE-KMS

Dual-layer la crittografia lato server con AWS KMS keys (DSSE-KMS) è simile a SSE-KMS, ma DSSE-KMS applica due livelli di AES-256 crittografia indipendenti anziché un livello: prima utilizzando una chiave di crittografia AWS KMS dei dati, quindi utilizzando una chiave di S3-managed crittografia Amazon separata. Poiché entrambi i livelli di crittografia vengono applicati a un oggetto sul lato server, puoi utilizzare un'ampia gamma di Servizi AWS strumenti per analizzare i dati in S3 utilizzando un metodo di crittografia in grado di soddisfare i requisiti di conformità per la crittografia multistrato. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server a doppio livello con AWS KMS chiavi DSSE-KMS \(\)](#).

Server-side crittografia con chiavi fornite dal cliente () SSE-C

Con la crittografia lato server con chiavi fornite dal cliente (SSE-C), tu gestisci le chiavi di crittografia e Amazon S3 gestisce la crittografia durante la scrittura sui dischi e la decrittografia quando accedi ai tuoi oggetti. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi fornite dal cliente \(\) SSE-C](#).

Note

Gli oggetti crittografati con non supportano le annotazioni. SSE-C Il tentativo di aggiungere un'annotazione a un oggetto SSE-C crittografato restituisce un errore. Per tutti gli altri tipi di crittografia, le annotazioni ereditano la configurazione di crittografia dell'oggetto padre. Le chiavi S3 Bucket sono supportate per le annotazioni su oggetti crittografati. SSE-KMS

Note

Quando si utilizzano punti di accesso per i file system Amazon FSx che utilizzano punti di accesso S3, è disponibile un'opzione per la crittografia lato server.

Server-side crittografia con Amazon FSx () SSE-FSX

Tutti i file system Amazon FSx hanno la crittografia configurata per impostazione predefinita e sono crittografati a riposo con chiavi gestite tramite AWS Key Management Service I dati vengono automaticamente crittografati e decrittografati sul file system durante la scrittura e la lettura nel file system. Questi processi vengono gestiti in modo trasparente da Amazon FSx.

Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS. Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

Tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita e gli oggetti vengono crittografati automaticamente utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Questa impostazione di crittografia si applica a tutti gli oggetti nei bucket Amazon S3.

Se hai bisogno di un maggiore controllo sulle tue chiavi, ad esempio gestendo la rotazione delle chiavi e la concessione delle policy di accesso, puoi scegliere di utilizzare la crittografia lato server con () keys AWS Key Management Service (AWS KMS) o la crittografia lato server a doppio livello con chiavi (SSE-KMS). AWS KMS DSSE-KMS Per ulteriori informazioni sulla modifica delle chiavi KMS, consulta [Modifica delle chiavi](#) nella Guida per gli sviluppatori di AWS Key Management Service.

Note

Abbiamo modificato i bucket per crittografare automaticamente i caricamenti di nuovi oggetti. Se in precedenza hai creato un bucket senza crittografia predefinita, Amazon S3 abiliterà la crittografia per impostazione predefinita per il bucket che utilizza. SSE-S3 Non verranno apportate modifiche alla configurazione di crittografia predefinita per un bucket esistente già esistente o configurato. SSE-S3 SSE-KMS Se desideri crittografare i tuoi oggetti con SSE-KMS, devi modificare il tipo di crittografia nelle impostazioni del bucket. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#).

Quando configuri il bucket per utilizzare la crittografia predefinita con SSE-KMS, puoi anche abilitare S3 Bucket Keys per ridurre il traffico di richieste da Amazon S3 AWS KMS e ridurre il costo della crittografia. Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

Per identificare i bucket che hanno SSE-KMS abilitato la crittografia predefinita, puoi utilizzare le metriche di Amazon S3 Storage Lens. S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti. Per ulteriori informazioni, consulta [Utilizzo di S3 Storage Lens per proteggere i dati](#).

Quando utilizzi la crittografia lato server, Amazon S3 esegue la crittografia di un oggetto prima di salvarlo su disco e lo decrittografa al momento del download. Per ulteriori informazioni sulla protezione dei dati mediante la crittografia lato server e la gestione delle chiavi di crittografia, consulta [Protezione dei dati con la crittografia lato server](#).

Per ulteriori informazioni sulle autorizzazioni richieste per la crittografia predefinita, consulta [PutBucketEncryption](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Puoi configurare il comportamento di crittografia predefinito di Amazon S3 per un bucket S3 utilizzando la console Amazon S3, gli AWS SDK, l'API REST di Amazon S3 e l'interfaccia a riga di comando (). AWS CLI

Crittografia di oggetti esistenti

Per crittografare gli oggetti Amazon S3 non crittografati esistenti, puoi utilizzare la funzionalità Operazioni in batch Amazon S3. Si fornisce a Operazioni in batch S3 un elenco di oggetti su cui operare e Operazioni in batch chiama le rispettive API per eseguire l'operazione specificata. È possibile utilizzare l'operazione di [copia delle operazioni in batch](#) per copiare gli oggetti non crittografati esistenti e scrivere i nuovi oggetti crittografati nello stesso bucket. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch](#) e il post del Blog sull'archiviazione di AWS [Crittografia di oggetti Amazon S3 esistenti con le operazioni in batch di Amazon S3](#).

Puoi anche crittografare oggetti esistenti utilizzando l'operazione API o il comando. CopyObject copy-object AWS CLI Per ulteriori informazioni, consulta il post del Blog sull'archiviazione di AWS [Crittografia di oggetti Amazon S3 esistenti con AWS CLI](#).

 Important

Se il bucket è una destinazione di destinazione per la distribuzione dei log di accesso al server, il bucket deve utilizzare le chiavi gestite di Amazon S3 (). SSE-S3 Se il bucket di destinazione utilizza la crittografia SSE-KMS predefinita, gli oggetti di log potrebbero essere creati ma crittografati con una chiave a cui non puoi accedere.

Utilizzo della SSE-KMS crittografia per le operazioni tra account

Quando si utilizza la crittografia per operazioni multi-account, tieni presente quanto segue:

- Se non viene fornito un AWS KMS key Amazon Resource Name (ARN) o un alias al momento della richiesta o tramite la configurazione di crittografia predefinita del bucket, viene utilizzato Chiave gestita da AWS ()aws/s3.
- Se stai caricando o accedendo a oggetti S3 utilizzando i principali AWS Identity and Access Management (IAM) che si trovano nella Account AWS stessa chiave KMS, puoi utilizzare (). Chiave gestita da AWS aws/s3
- Se desideri concedere l'accesso multi-account agli oggetti S3, utilizza una chiave gestita dal cliente. È possibile configurare la policy di una chiave gestita dal cliente per consentire l'accesso da un altro account.
- Se si specifica una chiave KMS gestita dal cliente, si consiglia di utilizzare un ARN della chiave KMS completamente qualificato. Se invece utilizzi un alias di chiave KMS, AWS KMS risolve la chiave all'interno dell'account del richiedente. Ciò potrebbe comportare la crittografia dei dati con una chiave KMS di proprietà del richiedente e non del proprietario del bucket.
- È necessario specificare una chiave per cui il richiedente ha ottenuto l'autorizzazione Encrypt. Per ulteriori informazioni, consulta l'argomento relativo all'[autorizzazione concessa agli utenti delle chiavi di utilizzare una chiave KMS per le operazioni di crittografia](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni su quando utilizzare le chiavi gestite dal cliente e le chiavi KMS AWS gestite, consulta [Devo usare una Chiave gestita da AWS o una chiave gestita dal cliente per crittografare i miei oggetti in Amazon S3?](#)

Utilizzo della codifica predefinita con la replica

Una volta abilitata la crittografia predefinita per un bucket di destinazione della replica, si applica il seguente comportamento di crittografia:

- Se gli oggetti nel bucket di origine non sono crittografati, gli oggetti replicati nel bucket di destinazione vengono crittografati in base alle impostazioni di crittografia predefinita del bucket di destinazione. Di conseguenza, i tag di entità (ETag) degli oggetti di origine differiscono dagli ETag degli oggetti di replica. Se disponi di applicazioni che utilizzano ETag, devi aggiornarle per tenere conto di questa differenza.
- Se gli oggetti nel bucket di origine sono crittografati utilizzando la crittografia lato server con chiavi gestite Amazon S3 (SSE-S3), la crittografia lato server con chiavi AWS Key Management Service (AWS KMS) () o la crittografia lato server a doppio livello con AWS KMS chiavi (SSE-KMSDSSE-KMS), gli oggetti di replica nel bucket di destinazione utilizzano lo stesso tipo di crittografia degli oggetti di origine. Le impostazioni della crittografia predefinita del bucket di destinazione non vengono utilizzate.

Per ulteriori informazioni sull'utilizzo della crittografia predefinita con SSE-KMS, vedere [Replica di oggetti crittografati](#).

Utilizzo di chiavi bucket Amazon S3 con crittografia predefinita

Quando configuri il bucket da utilizzare SSE-KMS come comportamento di crittografia predefinito per i nuovi oggetti, puoi anche configurare S3 Bucket Keys. Le chiavi S3 Bucket riducono il numero di transazioni da Amazon S3 per ridurre il costo di AWS KMS . SSE-KMS

Quando configuri il bucket per utilizzare S3 Bucket Keys per SSE-KMS nuovi oggetti, AWS KMS genera una chiave a livello di bucket che viene utilizzata per creare una chiave dati univoca [per gli oggetti nel bucket](#). Questa chiave S3 Bucket viene utilizzata per un periodo di tempo limitato all'interno di Amazon S3, riducendo la necessità per Amazon S3 di effettuare richieste per completare le operazioni di crittografia. AWS KMS

Per ulteriori informazioni sull'utilizzo delle chiavi del bucket S3, consulta la sezione [Utilizzo di chiavi bucket Amazon S3](#).

Configurazione della crittografia predefinita

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS. Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

La crittografia dei bucket Amazon S3 è abilitata per impostazione predefinita e i nuovi oggetti vengono crittografati automaticamente utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Questa crittografia si applica a tutti i nuovi oggetti nei bucket Amazon S3 e non comporta costi aggiuntivi.

Se hai bisogno di un maggiore controllo sulle tue chiavi di crittografia, ad esempio gestendo la rotazione delle chiavi e la concessione delle politiche di accesso, puoi scegliere di utilizzare la crittografia lato server con AWS Key Management Service (AWS KMS) keys () o la crittografia lato server a doppio livello con chiavi (SSE-KMS). AWS KMS DSSE-KMS SSE-KMS Per ulteriori informazioni su, vedere. [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#) Per ulteriori informazioni su DSSE-KMS, vedere [the section called “Dual-layer crittografia lato server \(\) DSSE-KMS”](#).

Se desideri utilizzare una chiave KMS di proprietà di un account diverso, devi avere l'autorizzazione necessaria per l'uso della chiave. Per ulteriori informazioni sulle autorizzazioni tra account per le chiavi KMS, vedi [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Se imposti la crittografia del bucket predefinita su SSE-KMS, puoi anche configurare una chiave bucket S3 per ridurre i AWS KMS costi delle richieste. Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

 Note

Se si utilizza [PutBucketEncryption](#) per impostare la crittografia bucket predefinita su SSE-KMS, è necessario verificare che l'ID della chiave KMS sia corretto. Amazon S3 non convalida l'ID della chiave KMS fornito nelle richieste. PutBucketEncryption

L'uso della crittografia predefinita dei bucket S3 non comporta costi aggiuntivi. Per le richieste di configurare la funzione di crittografia predefinita vengono applicati i costi standard per le richieste Amazon S3. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#). Per SSE-KMS e DSSE-KMS, si applicano i AWS KMS costi indicati in base ai prezzi. [AWS KMS](#)

Server-side la crittografia con chiavi fornite dal cliente (SSE-C) non è supportata per la crittografia predefinita.

Puoi configurare la crittografia predefinita di Amazon S3 per un bucket S3 utilizzando la console Amazon S3, gli AWS SDK, l'API REST di Amazon S3 e (). AWS Command Line Interface AWS CLI

Modifiche alla nota prima dell'abilitazione della crittografia predefinita

Una volta abilitata la crittografia predefinita di un bucket, si applica il seguente comportamento di crittografia:

- Non avvengono modifiche della crittografia degli oggetti che esisteva nel bucket prima che la crittografia predefinita venisse abilitata.
- Quando si effettua il caricamento di oggetti dopo l'abilitazione della crittografia predefinita:
 - Se le intestazioni della richiesta PUT non includono le informazioni di crittografia, Amazon S3 utilizza le impostazioni di crittografia di default del bucket per eseguire la crittografia degli oggetti.
 - Se le intestazioni della richiesta PUT includono le informazioni di crittografia, Amazon S3 utilizza le informazioni di crittografia della richiesta PUT per eseguire la crittografia degli oggetti prima di archivarli in Amazon S3.
- Se utilizzi l' DSSE-KMS opzione SSE-KMS or per la configurazione di crittografia predefinita, sei soggetto alle quote di richieste per secondo (RPS) di. AWS KMS Per ulteriori informazioni sulle quote AWS KMS e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli sviluppatori di AWS Key Management Service .
- Se questo bucket viene utilizzato come destinazione per la registrazione degli accessi al server, il bucket di destinazione deve utilizzare le chiavi gestite di Amazon S3 (). SSE-S3 Se il bucket di destinazione utilizza la crittografia SSE-KMS predefinita, Amazon S3 potrebbe fornire oggetti di

log crittografati con una chiave a cui non puoi accedere. Per risolvere questo problema, modifica la crittografia predefinita del bucket di destinazione in. SSE-S3 Per ulteriori informazioni sulla registrazione degli accessi al server, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

Note

Gli oggetti caricati prima dell'abilitazione della crittografia predefinita non verranno crittografati. Per ulteriori informazioni sulla crittografia di oggetti, consulta [the section called "Impostazione della crittografia predefinita del bucket"](#).

Utilizzo della console S3

Per configurare la crittografia predefinita per un bucket Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il nome del bucket desiderato.
4. Scegliere la scheda Properties (Proprietà).
5. In Default encryption (Crittografia di default), scegliere Edit (Modifica).
6. Per configurare la crittografia, in Tipo di crittografia scegli una delle seguenti opzioni:
 - Server-side crittografia con chiavi gestite da Amazon S3 () SSE-S3
 - Server-side crittografia con AWS Key Management Service chiavi () SSE-KMS
 - Dual-layer crittografia lato server con AWS Key Management Service chiavi () DSSE-KMS

Important

Se si utilizzano le DSSE-KMS opzioni SSE-KMS or per la configurazione di crittografia predefinita, si è soggetti alle quote di richieste al secondo (RPS) di. AWS KMS Per ulteriori informazioni sulle AWS KMS quote e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli sviluppatori. AWS Key Management Service

I bucket e i nuovi oggetti sono crittografati per impostazione predefinita con SSE-S3, a meno che non si specifichi un altro tipo di crittografia predefinito per i bucket. Per ulteriori informazioni sulla crittografia predefinita, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#).

Per ulteriori informazioni sull'utilizzo della crittografia lato server di Amazon S3 per crittografare i dati, consulta [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).

7. Se hai scelto Server-side la crittografia con AWS Key Management Service chiavi (SSE-KMS) o la Dual-layer crittografia lato server con AWS Key Management Service chiavi (DSSE-KMS), procedi come segue:

- a. In Chiave AWS KMS specifica la tua chiave KMS in uno dei seguenti modi:

- Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS keys e scegli la tua chiave KMS dall'elenco delle chiavi disponibili.

Sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente vengono visualizzate in questo elenco. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta Chiavi e AWS chiavi del [cliente](#) nella Guida per gli AWS Key Management Service sviluppatori.

- Per specificare l'ARN della chiave KMS, scegli Inserisci l'ARN della AWS KMS key e quindi specifica l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

Important

È possibile utilizzare solo le chiavi KMS abilitate contemporaneamente Regione AWS al bucket. Quando scegli Choose from your KMS keys (Scegli tra le chiavi KMS), la console S3 elenca solo 100 chiavi KMS per regione. Se hai più di 100 chiavi KMS nella stessa regione, puoi vedere solo le prime 100 chiavi KMS nella console S3. Per utilizzare una chiave KMS non elencata nella console, seleziona Inserisci l'ARN AWS KMS key e specifica l'ARN della chiave KMS.

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetrica. Per ulteriori informazioni sulle chiavi, consulta [Chiavi KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni sull'utilizzo SSE-KMS con Amazon S3, consulta. [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#) Per ulteriori informazioni sull'utilizzo DSSE-KMS, consulta [the section called “Dual-layer crittografia lato server \(\) DSSE-KMS”](#).

- b. Quando configuri il bucket per utilizzare la crittografia predefinita con SSE-KMS, puoi anche abilitare una chiave S3 Bucket. Le chiavi S3 Bucket riducono il costo della crittografia diminuendo il traffico di richieste da Amazon S3 a AWS KMS Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

Per utilizzare le chiavi bucket S3, in Chiave bucket seleziona Abilita.

 Note

Le chiavi S3 Bucket non sono supportate per DSSE-KMS

- 8. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Questi esempi mostrano come configurare la crittografia predefinita utilizzando SSE-S3 o utilizzando SSE-KMS una chiave S3 Bucket.

Per ulteriori informazioni sulla crittografia predefinita, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#). Per ulteriori informazioni sull'utilizzo di per configurare la AWS CLI crittografia predefinita, vedere [put-bucket-encryption](#).

Example— Crittografia predefinita con SSE-S3

In questo esempio viene configurata la crittografia predefinita dei bucket con le chiavi gestite da Amazon S3.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-configuration '{
  "Rules": [
    {
      "ApplyServerSideEncryptionByDefault": {
        "SSEAlgorithm": "AES256"
      }
    }
  ]
}'
```

Example— Crittografia predefinita con SSE-KMS l'utilizzo di una chiave S3 Bucket

Questo esempio configura la crittografia bucket predefinita SSE-KMS utilizzando una chiave bucket S3.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-configuration '{
  "Rules": [
    {
      "ApplyServerSideEncryptionByDefault": {
        "SSEAlgorithm": "aws:kms",
        "KMSEMasterKeyID": "KMS-Key-ARN"
      },
      "BucketKeyEnabled": true
    }
  ]
}'
```

Utilizzo della REST API

Utilizza l'`PutBucketEncryption` operazione REST API per abilitare la crittografia predefinita e impostare il tipo di crittografia lato server da utilizzare—, or. SSE-S3 SSE-KMS DSSE-KMS

Per ulteriori informazioni, consulta [PutBucketEncryption](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Monitoraggio della crittografia predefinita con AWS CloudTrail e Amazon EventBridge

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS. Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

È possibile tenere traccia le richieste di configurazione della crittografia predefinita per i bucket Amazon S3 mediante gli eventi AWS CloudTrail. Nei log vengono utilizzati i seguenti nomi di eventi API: CloudTrail

- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

Puoi anche creare EventBridge regole per abbinare gli CloudTrail eventi di queste chiamate API. Per ulteriori informazioni sugli CloudTrail eventi, consulta [Abilitazione della registrazione per gli oggetti in un bucket utilizzando la console](#). Per ulteriori informazioni sugli EventBridge eventi, consulta [Eventi da Servizi AWS](#).

Puoi utilizzare CloudTrail i log per tracciare le azioni Amazon S3 a livello di oggetto PUT e le POST richieste ad Amazon S3. È possibile utilizzare queste azioni per verificare se la crittografia predefinita viene utilizzata per crittografare gli oggetti quando le richieste PUT in arrivo non dispongono di intestazioni di crittografia.

Quando Amazon S3 esegue la crittografia di un oggetto in base alle impostazioni della crittografia predefinita, il log include uno dei seguenti campi come coppia nome/valore: "SSEApplied": "Default_SSE_S3", "SSEApplied": "Default_SSE_KMS" o "SSEApplied": "Default_DSSE_KMS".

Quando Amazon S3 esegue la crittografia di un oggetto in base alle intestazioni di crittografia PUT, il log include uno dei campi seguenti come coppia nome/valore: "SSEApplied": "SSE_S3", "SSEApplied": "SSE_KMS", "SSEApplied": "DSSE_KMS" o "SSEApplied": "SSE_C".

Per i caricamenti in più parti, queste informazioni sono incluse nelle richieste dell'operazione API `InitiateMultipartUpload`. Per ulteriori informazioni sull'utilizzo CloudTrail di and, consulta. CloudWatch [Registrazione e monitoraggio in Amazon S3](#)

Domande frequenti sulla crittografia predefinita

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i nuovi oggetti caricati su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza impatto sulle prestazioni. SSE-S3, che utilizza Advanced Encryption Standard (AES-256) a 256 bit, viene applicato automaticamente a tutti i nuovi bucket e a qualsiasi bucket S3 esistente per il quale non è già configurata la crittografia predefinita. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei AWS CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva in AWS Command Line Interface (AWS CLI) e negli AWS SDK.

Nelle sezioni seguenti vengono fornite le risposte alle domande su questo aggiornamento.

Amazon S3 modifica le impostazioni della crittografia predefinita per i miei bucket esistenti che hanno già configurato la crittografia predefinita?

No Non sono state apportate modifiche alla configurazione di crittografia predefinita per un bucket esistente che dispone SSE-S3 già della crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS) configurata. Per ulteriori informazioni su come configurare il comportamento della crittografia predefinita per i bucket, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#). Per ulteriori informazioni SSE-S3 e impostazioni di SSE-KMS crittografia, vedere. [Protezione dei dati con la crittografia lato server](#)

La crittografia predefinita è abilitata nei miei bucket esistenti che non hanno la crittografia predefinita configurata?

Sì. Amazon S3 ora configura la crittografia predefinita su tutti i bucket non crittografati esistenti per applicare la crittografia lato server con chiavi gestite S3 (SSE-S3) come livello base di crittografia per i nuovi oggetti caricati in questi bucket. Gli oggetti già presenti in un bucket non crittografato esistente non verranno crittografati automaticamente.

Come posso visualizzare lo stato della crittografia predefinita dei caricamenti di nuovi oggetti?

Attualmente, puoi visualizzare lo stato di crittografia predefinito dei nuovi caricamenti di oggetti nei AWS CloudTrail log, in S3 Inventory e S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva in AWS Command Line Interface (AWS CLI) e negli AWS SDK.

- Per visualizzare i tuoi CloudTrail eventi, consulta [Visualizzazione CloudTrail degli eventi nella console nella Guida per l'utente. CloudTrail](#) AWS CloudTrail CloudTrail i log forniscono il monitoraggio delle API PUT e le POST richieste ad Amazon S3. Quando la crittografia predefinita viene utilizzata per crittografare gli oggetti nei bucket, i CloudTrail log PUT e le richieste POST API includeranno il seguente campo come coppia nome-valore:
`"SSEApplied": "Default_SSE_S3"`
- Per visualizzare lo stato di crittografia automatica dei nuovi caricamenti di oggetti in S3 Inventory, configura un report di S3 Inventory che includa il campo dei metadati Encryption (Crittografia), quindi visualizza lo stato di crittografia di ogni nuovo oggetto nel report. Per ulteriori informazioni, consulta [Impostazione di Amazon S3 Inventory](#).
- Per visualizzare lo stato di crittografia automatica per i nuovi caricamenti di oggetti in S3 Storage Lens, configura un pannello di controllo di S3 Storage Lens e visualizza le metriche Encrypted bytes (Byte crittografati) e Encrypted object count (Conteggio degli oggetti crittografati) nella categoria Data protection (Protezione dei dati) del pannello di controllo. Per ulteriori informazioni, consulta [Utilizzo della console S3](#) e [Visualizzazione dei parametri di S3 Storage Lens nei pannelli di controllo](#).
- Per visualizzare lo stato della crittografia automatica a livello di bucket nella console Amazon S3, controlla la crittografia predefinita dei bucket Amazon S3 nella console Amazon S3. Per ulteriori informazioni, consulta [Configurazione della crittografia predefinita](#).
- Per visualizzare lo stato della crittografia automatica come intestazione di risposta dell'API Amazon S3 aggiuntiva in AWS Command Line Interface (AWS CLI) e negli AWS SDK, controlla l'intestazione della risposta `x-amz-server-side-encryption` quando usi le API di azione degli oggetti, come e. [PutObject](#) [GetObject](#)

Cosa devo fare per trarre vantaggio da questa modifica?

Non è necessario apportare modifiche alle applicazioni esistenti. Poiché la crittografia predefinita è abilitata per tutti i bucket, tutti i nuovi oggetti caricati in Amazon S3 vengono crittografati automaticamente.

Posso disabilitare la crittografia per i nuovi oggetti che vengono scritti nel mio bucket?

No SSE-S3 è il nuovo livello base di crittografia che viene applicato a tutti i nuovi oggetti caricati nel bucket. Non è più possibile disabilitare la crittografia per il caricamento di nuovi oggetti.

Ciò avrà ripercussioni sui miei addebiti?

No La crittografia predefinita con SSE-S3 è disponibile senza costi aggiuntivi. Ti verranno fatturati lo spazio di archiviazione, le richieste e le altre funzionalità di S3, come al solito. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Amazon S3 crittograferà i miei oggetti esistenti non crittografati?

No. A partire dal 5 gennaio 2023, Amazon S3 crittografa automaticamente solo i caricamenti di nuovi oggetti. Per crittografare gli oggetti esistenti, è possibile utilizzare la funzionalità Operazioni in batch Amazon S3 per creare copie crittografate degli oggetti. Queste copie crittografate manterranno i dati e il nome dell'oggetto esistenti e verranno crittografate utilizzando le chiavi di crittografia specificate. Per ulteriori informazioni, consulta [Crittografia degli oggetti con Operazioni in batch Amazon S3](#) nel Blog dell'archiviazione AWS .

Non ho abilitato la crittografia per i miei bucket prima di questa versione. Devo cambiare la modalità di accesso agli oggetti?

No La crittografia predefinita crittografa SSE-S3 automaticamente i dati mentre vengono scritti su Amazon S3 e li decrittografa automaticamente quando vi accedi. Non vi è alcuna modifica nel modo in cui si accede agli oggetti crittografati automaticamente.

Devo cambiare il modo in cui accedo ai miei oggetti con crittografia lato client?

No. Tutti gli oggetti con crittografia lato client crittografati prima di essere caricati in Amazon S3 arrivano come oggetti di testo criptato crittografati all'interno di Amazon S3. Questi oggetti avranno ora un ulteriore livello di crittografia. SSE-S3 I carichi di lavoro che utilizzano oggetti con crittografia lato client non richiederanno alcuna modifica ai servizi client o alle impostazioni di autorizzazione.

Note

HashiCorp Gli utenti Terraform che non utilizzano una versione aggiornata del AWS provider potrebbero subire una deriva inaspettata dopo aver creato nuovi bucket S3 senza una configurazione di crittografia definita dal cliente. Per evitare questa deriva, aggiorna la

versione del tuo Terraform AWS Provider a una delle seguenti versioni: qualsiasi versione, o. 4.x 3.76.1 2.70.4

Aggiornamento della crittografia lato server per i dati esistenti

Tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita e gli oggetti vengono crittografati automaticamente utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3 Questa impostazione di crittografia predefinita si applica a tutti i nuovi oggetti nei tuoi bucket Amazon S3.

Utilizzando l'operazione `UpdateObjectEncryption` API, puoi aggiornare atomicamente il tipo di crittografia lato server di un oggetto crittografato esistente in un bucket generico dalla crittografia lato server con crittografia gestita Amazon S3 (SSE-S3) alla crittografia lato server con chiavi di crittografia () (). AWS Key Management Service AWS KMS SSE-KMS L'operazione `UpdateObjectEncryption` API utilizza la crittografia [a](#) involuppo per crittografare nuovamente la chiave di dati utilizzata per crittografare e decrittografare l'oggetto con il tipo di crittografia lato server appena specificato.

Amazon S3 esegue questo aggiornamento del tipo di crittografia senza alcun trasferimento di dati. In altre parole, quando si utilizza l'operazione `UpdateObjectEncryption`, i dati non vengono copiati, gli oggetti archiviati in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive non vengono ripristinati e gli oggetti nella classe di storage S3 non vengono spostati tra i livelli. Intelligent-Tiering Inoltre, l'operazione `UpdateObjectEncryption` conserva tutte le proprietà dei metadati degli oggetti, tra cui la classe di archiviazione, la data di creazione, la data dell'ultima modifica, ETag e le proprietà checksum.

L'operazione `UpdateObjectEncryption` è supportata per tutte le classi di archiviazione S3 supportate da bucket generici. È possibile utilizzare l'operazione `UpdateObjectEncryption` per effettuare le seguenti operazioni:

- Cambia gli oggetti crittografati dalla crittografia lato server con crittografia gestita Amazon S3 (SSE-S3) alla crittografia lato server con chiavi di crittografia AWS Key Management Service (AWS KMS) (). SSE-KMS
- Aggiorna gli oggetti SSE-KMS crittografati a livello di oggetto per utilizzare S3 Bucket Keys, che riduce il traffico di richieste da Amazon S3 a. AWS KMS AWS KMS Per ulteriori informazioni, consulta [the section called “Utilizzo di chiavi bucket Amazon S3”](#).

- Modifica la chiave KMS gestita dal cliente utilizzata per crittografare i dati in modo da rispettare gli standard personalizzati di rotazione delle chiavi.

Note

Gli oggetti di origine non crittografati o crittografati con crittografia lato server a doppio livello con () o chiavi di crittografia fornite dal cliente AWS KMS keys (DSSE-KMS) non sono supportati da questa operazione. SSE-C

L'UpdateObjectEncryptionoperazione viene in genere completata in millisecondi indipendentemente dalle dimensioni dell'oggetto o dalla classe di archiviazione, inclusi S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Questa operazione non è considerata un accesso per S3 Intelligent-Tiering, quindi gli oggetti nel livello Infrequent Access o Archive Instant Access non torneranno automaticamente al livello Frequent Access se si modifica il tipo di crittografia lato server dell'oggetto.

UpdateObjectEncryptionè un'operazione API a livello di oggetto (piano dati) che viene registrata nei log di accesso al server Amazon S3 e negli eventi ai dati. AWS CloudTrail Per ulteriori informazioni, consulta [the section called “Opzioni di registrazione”](#).

L'UpdateObjectEncryptionoperazione ha lo stesso prezzo diPUT, COPYPOST, e LIST delle richieste (per 1.000 richieste) e viene sempre addebitata come richiesta di classe di storage S3 Standard indipendentemente dalla classe di storage dell'oggetto sottostante. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Restrizioni e considerazioni

Quando si utilizza l'UpdateObjectEncryptionoperazione, si applicano le seguenti restrizioni e considerazioni:

- L'UpdateObjectEncryptionoperazione non supporta oggetti non crittografati o oggetti crittografati con crittografia lato server a doppio livello con AWS KMS keys (DSSE-KMS) o chiavi di crittografia fornite dal cliente (). SSE-C Inoltre, non è possibile specificare SSE-S3 come richiesta il nuovo tipo di crittografia richiesto. UpdateObjectEncryption
- È possibile utilizzare l'UpdateObjectEncryptionoperazione per aggiornare gli oggetti nei bucket in cui è abilitato il controllo delle versioni di S3. Per aggiornare il tipo di crittografia di una particolare versione, è necessario specificare un ID di versione nella UpdateObjectEncryption

richiesta. Se non si specifica l'ID di versione, la `UpdateObjectEncryption` richiesta agisce sulla versione corrente dell'oggetto. Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [the section called “Conservazione più versioni degli oggetti”](#).

- L'`UpdateObjectEncryption` operazione ha esito negativo su qualsiasi oggetto a cui è applicata una modalità di conservazione S3 Object Lock o un blocco legale. Se un oggetto ha un periodo di conservazione in modalità governativa o un blocco legale, è necessario rimuovere lo stato Object Lock sull'oggetto prima di emettere la richiesta. `UpdateObjectEncryption` Non è possibile utilizzare l'`UpdateObjectEncryption` operazione con oggetti a cui è applicato un periodo di conservazione in modalità di conformità Object Lock. Per ulteriori informazioni sul blocco degli oggetti S3, consulta [the section called “Blocco degli oggetti”](#).
- `UpdateObjectEncryption` le richieste sui bucket di origine con la replica in tempo reale abilitata non avvieranno eventi di replica nel bucket di destinazione. Se desideri modificare il tipo di crittografia degli oggetti nei bucket di origine e di destinazione, devi avviare `UpdateObjectEncryption` richieste separate sugli oggetti nei bucket di origine e di destinazione.
- Per impostazione predefinita, tutte le `UpdateObjectEncryption` richieste che specificano una chiave KMS gestita dal cliente sono limitate alle chiavi KMS di proprietà del proprietario del bucket. Account AWS Se stai utilizzando AWS Organizations, puoi richiedere la possibilità di utilizzare account di AWS KMS keys proprietà di altri membri all'interno della tua organizzazione contattando. Supporto AWS
- Se utilizzi S3 Batch Replication per replicare i set di dati in più regioni e in precedenza il tipo di crittografia lato server era aggiornato dal SSE-S3 al SSE-KMS, potresti aver bisogno di autorizzazioni aggiuntive. Nel bucket della regione di origine, è necessario disporre delle autorizzazioni `kms:decrypt`. Quindi, avrai bisogno delle `kms:encrypt` autorizzazioni `kms:decrypt` e per il bucket nella regione di destinazione.
- Nella richiesta è necessario fornire un ARN completo della chiave KMS.
`UpdateObjectEncryption` Non puoi utilizzare un nome alias o un alias ARN. Puoi determinare l'ARN completo della chiave KMS nella console AWS KMS o utilizzando l'API AWS KMS.
`DescribeKey`

Autorizzazioni richieste

Per eseguire l'`UpdateObjectEncryption` operazione, devi disporre delle seguenti autorizzazioni:

- `s3:UpdateObjectEncryption`
- `kms:Encrypt`

- kms:Decrypt
- kms:GenerateDataKey
- kms:ReEncrypt*

Se stai utilizzando AWS Organizations, per utilizzare questa operazione con chiavi KMS gestite dal cliente provenienti da altri membri della tua Account AWS organizzazione, devi disporre dell'autorizzazione. `organizations:DescribeAccount` È inoltre necessario richiedere la possibilità di utilizzare account AWS KMS keys di proprietà di altri membri all'interno dell'organizzazione contattando. Supporto AWS

Per eseguire l'UpdateObjectEncryptionoperazione, aggiungi la seguente policy AWS Identity and Access Management (IAM) al tuo ruolo IAM. Per utilizzare questa policy, *amzn-s3-demo-bucket* sostituiscila con il nome del tuo bucket generico e sostituisci l'altro *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowUpdateObjectEncryption",
    "Effect": "Allow",
    "Action": [
      "s3:UpdateObjectEncryption",
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:GenerateDataKey",
      "kms:ReEncrypt*",
      "organizations:DescribeAccount"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "arn:aws:kms:us-east-1:111122223333:key/01234567-89ab-
cdef-0123-456789abcdef"
    ]
  }]
}
```


Aggiornamento della crittografia in blocco

Per aggiornare il tipo di crittografia lato server di più di un oggetto Amazon S3 con una singola richiesta, puoi utilizzare S3 Batch Operations. Puoi fornire a S3 Batch Operations un elenco di oggetti su cui operare oppure puoi indirizzare Batch Operations a generare metadati degli oggetti basati su un elenco di oggetti, tra cui prefisso, classe di archiviazione, data di creazione, tipo di crittografia, ARN della chiave KMS o stato della chiave S3 Bucket. Le operazioni in batch S3 richiamano la rispettiva API per eseguire l'operazione specificata. Un singolo job Batch Operations può eseguire l'operazione specificata su miliardi di oggetti all'interno di un bucket contenente petabyte di dati. Per ulteriori informazioni su Batch Operations, consulta [the section called “Esecuzione di operazioni sugli oggetti in blocco”](#).

La funzionalità Operazioni in batch S3 tiene traccia dei progressi, invia notifiche e memorizza un report dettagliato sul completamento di tutte le azioni, offrendo un'esperienza serverless completamente gestita e verificabile. Puoi utilizzare S3 Batch Operations tramite la console Amazon S3, AWS Command Line Interface (AWS CLI) AWS SDK o l'API REST di Amazon S3. Per ulteriori informazioni, consulta [the section called “Aggiorna la crittografia degli oggetti”](#).

Aggiornamento della crittografia per gli oggetti

Puoi aggiornare il tipo di crittografia lato server per un oggetto tramite gli AWS SDK AWS Command Line Interface (AWS CLI) o l'API REST di Amazon S3.

Aggiorna la crittografia per un oggetto

Utilizzo di AWS CLI

Per eseguire i seguenti comandi, è necessario che siano AWS CLI installati e configurati. Se non è AWS CLI installato, consulta [Installare o aggiornare alla versione più recente di AWS CLI](#) nella Guida per l'AWS Command Line Interface utente.

In alternativa, puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da Console di gestione AWS. Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) e [Guida introduttiva AWS CloudShell](#) nella Guida AWS CloudShell per l'utente.

Per aggiornare la crittografia di un oggetto utilizzando AWS CLI

Per utilizzare il seguente comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

1. Usa il comando seguente per aggiornare la crittografia di un singolo oggetto (*index.html*) nel tuo bucket generico (ad esempio, *amzn-s3-demo-bucket*) da utilizzare SSE-KMS con una chiave bucket S3:

```
aws s3api update-object-encryption \  
--bucket amzn-s3-demo-bucket \  
--key index.html \  
--object-encryption '{"SSEKMS": { "KMSKeyArn": "arn:aws:kms:us-  
east-1:111122223333:key/f12a345a-678e-9bbb-1025-62e317037583", "BucketKeyEnabled":  
true } }'
```

Note

Devi specificare l' AWS KMS key Amazon Resource Name (ARN) completo. L'ID della chiave KMS e l'alias della chiave KMS non sono supportati.

2. Esegui il head-object comando per visualizzare il tipo di crittografia aggiornato del tuo oggetto:

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html
```

Utilizzo della REST API

È possibile inviare richieste REST per aggiornare la crittografia di un oggetto. Per ulteriori informazioni, consulta [UpdateObjectEncryption](#).

Utilizzo di AWS SDK

È possibile utilizzare gli AWS SDK per aggiornare la crittografia di un oggetto. Per ulteriori informazioni, consulta l'[elenco degli SDK](#) supportati.

Java

Example

L' AWS SDK for Java 2.x esempio seguente aggiorna il tipo di crittografia SSE-KMS per un oggetto in un bucket generico.

```
public void updateObjectEncryption(String bucketName,
```

```

        String objectKey,
        String versionId,
        String kmsKeyArn,
        boolean bucketKeyEnabled) {
    // Create the target object encryption type.
    ObjectEncryption objectEncryption = ObjectEncryption.builder()
        .ssekms(SSEKMSEncryption.builder()
            .kmsKeyArn(kmsKeyArn)
            .bucketKeyEnabled(bucketKeyEnabled)
            .build())
        .build();

    // Create the UpdateObjectEncryption request.
    UpdateObjectEncryptionRequest request =
UpdateObjectEncryptionRequest.builder()
    .bucket(bucketName)
    .key(objectKey)
    .versionId(versionId)
    .objectEncryption(objectEncryption)
    .build();

    // Update the object encryption.
    try {
        getS3Client().updateObjectEncryption(request);
        logger.info("Object encryption updated to SSE-KMS for {} in bucket {}",
objectKey, bucketName);
    } catch (S3Exception e) {
        logger.error("Failed to update to object encryption: {} - Error code:
{}", e.awsErrorDetails().errorMessage(),
            e.awsErrorDetails().errorCode());
        throw e;
    }
}

```

Python

Example

L' AWS SDK per Python (Boto3) esempio seguente mostra come aggiornare il tipo di crittografia SSE-KMS per un oggetto in un bucket generico.

```

response = client.update_object_encryption(
    Bucket='string',

```

```
Key='string',
VersionId='string',
ObjectEncryption={
  'SSEKMS': {
    'KMSKeyArn': 'string',
    'BucketKeyEnabled': True|False
  }
}
```

Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3)

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS. Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

Tutti i nuovi caricamenti di oggetti nei bucket Amazon S3 sono crittografati per impostazione predefinita con crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3).

Server-side la crittografia protegge i dati inattivi. Amazon S3 crittografa ogni oggetto con una chiave univoca. Come ulteriore tutela, crittografa la chiave con una chiave che ruota con regolarità. La crittografia lato server di Amazon S3 utilizza la Galois/Counter modalità Advanced Encryption Standard Mode (AES-GCM) a 256 bit per crittografare tutti gli oggetti caricati.

Non sono previsti costi aggiuntivi per l'utilizzo della crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3). Tuttavia, per le richieste di configurare la funzione di crittografia predefinita vengono applicati i costi delle richieste Amazon S3 standard. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Se desideri che i tuoi caricamenti di dati siano crittografati utilizzando solo le chiavi gestite da Amazon S3, puoi utilizzare la seguente policy dei bucket. Ad esempio, la seguente policy del bucket

rifiuta le autorizzazioni al caricamento di un oggetto a meno che la richiesta non includa l'intestazione `x-amz-server-side-encryption` per richiedere la codifica lato server:

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PutObjectPolicy",
  "Statement": [
    {
      "Sid": "DenyObjectsThatAreNotSSES3",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    }
  ]
}
```

Note

Server-side la crittografia crittografa solo i dati dell'oggetto, non i metadati dell'oggetto.

Note

La chiave di `s3:x-amz-server-side-encryption` condizione utilizzata nelle politiche dei bucket è uno spazio dei nomi delle chiavi di condizione IAM e differisce dall'intestazione HTTP mostrata nei log. `x-amz-server-side-encryption` CloudTrail Entrambi si riferiscono alla stessa impostazione di crittografia, ma utilizzano formati diversi. Inoltre, questa politica Deny potrebbe bloccare le scritture (come i log di accesso di Elastic Load Balancing o i CloudFront log Amazon) che inviano oggetti al bucket senza specificare l'intestazione di crittografia.

Supporto API per la crittografia lato server

Tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita e tutti i nuovi oggetti caricati in un bucket S3 vengono crittografati automaticamente quando sono inattivi. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket in Amazon S3. Per utilizzare un diverso tipo di crittografia, puoi specificare il tipo di crittografia lato server da utilizzare nelle richieste PUT S3 oppure aggiornare la configurazione di crittografia predefinita nel bucket di destinazione.

Se desideri specificare un tipo di crittografia diverso nelle tue PUT richieste, puoi utilizzare la crittografia lato server con () chiavi AWS Key Management Service (AWS KMS), la crittografia lato server a doppio livello con chiavi (SSE-KMS) o la crittografia lato server con AWS KMS chiavi fornite dal cliente (DSSE-KMS). SSE-C Se desideri impostare una diversa configurazione di crittografia predefinita nel bucket di destinazione, puoi utilizzare o. SSE-KMS DSSE-KMS

Per ulteriori informazioni su come modificare la configurazione di crittografia predefinita per i bucket per uso generico, consulta [Configurazione della crittografia predefinita](#).

Quando modifichi la configurazione di crittografia predefinita del bucket in SSE-KMS, il tipo di crittografia degli oggetti Amazon S3 esistenti nel bucket non viene modificato. Per modificare il tipo di crittografia degli oggetti preesistenti dopo aver aggiornato la configurazione di crittografia predefinita in SSE-KMS, puoi utilizzare Amazon S3 Batch Operations. Si fornisce a Operazioni in batch S3 un elenco di oggetti e Operazioni in batch richiama la rispettiva operazione API. Puoi utilizzare l'[Copia oggetti](#) per copiare oggetti esistenti e riscriverli nello stesso bucket degli oggetti crittografati SSE-KMS . Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch](#) e il post [Come crittografare retroattivamente gli oggetti esistenti in Amazon S3 utilizzando Inventario S3, Amazon Athena e Operazioni in batch S3](#) nel Blog dell'archiviazione AWS .

Per configurare la crittografia lato server utilizzando le REST API della creazione dell'oggetto, devi fornire l'intestazione della richiesta `x-amz-server-side-encryption`. Per ulteriori informazioni sulle APIs REST, consulta [Utilizzo della REST API](#).

Le seguenti API Amazon S3 supportano questa intestazione:

- Operazioni PUT: specifica l'intestazione della richiesta quando si caricano i dati utilizzando l'API PUT. Per ulteriori informazioni, consulta [PUT Object](#).

- Avvia caricamento in più parti: specifica l'intestazione nella richiesta di avvio quando si caricano oggetti di grandi dimensioni utilizzando l'API per il caricamento in più parti. Per ulteriori informazioni, consulta [Initiate Multipart Upload](#).
- Operazione COPY: l'operazione di copia di un oggetto coinvolge un oggetto di origine e un oggetto di destinazione. Per ulteriori informazioni, consulta [PUT Object - Copy](#).

Note

Quando si utilizza un'operazione POST per caricare un oggetto anziché l'intestazione della richiesta, si specificano le stesse informazioni nei campi del modulo. Per ulteriori informazioni, consulta [POST Object](#).

Gli AWS SDK forniscono anche API wrapper che puoi utilizzare per richiedere la crittografia lato server. Puoi anche utilizzarlo per caricare oggetti e richiedere la crittografia Console di gestione AWS lato server.

Per ulteriori informazioni generali, consulta [Concetti di AWS KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Argomenti

- [Specificare la crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#)

Specificare la crittografia lato server con chiavi gestite da Amazon S3 () SSE-S3

Tutti i bucket Amazon S3 hanno la crittografia configurata per impostazione predefinita e tutti i nuovi oggetti caricati in un bucket S3 vengono crittografati automaticamente quando sono inattivi. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket in Amazon S3. Per utilizzare un diverso tipo di crittografia, puoi specificare il tipo di crittografia lato server da utilizzare nelle richieste PUT S3 oppure aggiornare la configurazione di crittografia predefinita nel bucket di destinazione.

Se desideri specificare un tipo di crittografia diverso nelle tue PUT richieste, puoi utilizzare la crittografia lato server con () chiavi AWS Key Management Service (AWS KMS), la crittografia lato server a doppio livello con chiavi (SSE-KMS) o la crittografia lato server con AWS KMS chiavi fornite dal cliente (DSSE-KMS). SSE-C Se desideri impostare una diversa configurazione di crittografia predefinita nel bucket di destinazione, puoi utilizzare o. SSE-KMS DSSE-KMS

Per ulteriori informazioni su come modificare la configurazione di crittografia predefinita per i bucket per uso generico, consulta [Configurazione della crittografia predefinita](#).

Quando modifichi la configurazione di crittografia predefinita del bucket in SSE-KMS, il tipo di crittografia degli oggetti Amazon S3 esistenti nel bucket non viene modificato. Per modificare il tipo di crittografia degli oggetti preesistenti dopo aver aggiornato la configurazione di crittografia predefinita in SSE-KMS, puoi utilizzare Amazon S3 Batch Operations. Si fornisce a Operazioni in batch S3 un elenco di oggetti e Operazioni in batch richiama la rispettiva operazione API. Puoi utilizzare l'[Copia oggetti](#) per copiare oggetti esistenti e riscriverli nello stesso bucket degli oggetti crittografati SSE-KMS. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch](#) e il post [Come crittografare retroattivamente gli oggetti esistenti in Amazon S3 utilizzando Inventario S3, Amazon Athena e Operazioni in batch S3](#) nel Blog dell'archiviazione AWS.

È possibile specificare SSE-S3 utilizzando la console S3, le API REST, AWS gli SDK e (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#).

Utilizzo della console S3

Questo argomento descrive in che modo impostare o modificare il tipo di crittografia che viene utilizzato da un oggetto utilizzando la Console di gestione AWS. Quando si copia un oggetto utilizzando la console, l'oggetto viene copiato da Amazon S3 così com'è: Ciò significa che se l'oggetto di origine è crittografato, anche l'oggetto di destinazione sarà crittografato. Puoi usare la console per aggiungere o modificare la crittografia per un oggetto.

Note

- È possibile modificare la crittografia di un oggetto se l'oggetto è inferiore a 5 GB. Se l'oggetto è superiore a 5 GB, è necessario utilizzare gli SDK [AWS CLI](#) o [AWS per modificare la crittografia di un oggetto](#).
- Per un elenco delle autorizzazioni aggiuntive necessarie per modificare la crittografia di un oggetto, consulta [the section called “Autorizzazioni necessarie per le operazioni API S3”](#). Per esempi di policy che concedono questa autorizzazione, consulta [the section called “Identity-based esempi di policy”](#).
- Se si modifica la crittografia di un oggetto, viene creato un nuovo oggetto per sostituire quello precedente. Se è abilitata la funzione Controllo delle versioni S3, viene creata una nuova versione dell'oggetto e l'oggetto esistente diventa una versione precedente. Il ruolo

che modifica la proprietà diventa anche il proprietario del nuovo oggetto o della versione dell'oggetto.

Per modificare la crittografia di un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket, quindi scegli la scheda Bucket per uso generico. Naviga al bucket o alla cartella Amazon S3 che contiene gli oggetti da modificare.
3. Seleziona la casella di controllo degli oggetti da modificare.
4. Nel menu Azioni, scegli Modifica crittografia lato server dall'elenco di opzioni visualizzato.
5. Scorri fino alla sezione Server-side di crittografia.
6. In Impostazioni di crittografia, scegli Utilizza le impostazioni del bucket per la crittografia predefinita o Ignora le impostazioni del bucket per la crittografia predefinita.
7. Se scegli Sostituisci impostazioni del bucket per la crittografia predefinita, configura le seguenti impostazioni di crittografia.
 - In Tipo di crittografia, scegli Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3). SSE-S3 utilizza uno dei più potenti cifrari a blocchi: Advanced Encryption Standard () a 256 bit per crittografare ogni oggetto. AES-256 Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).
8. In Impostazioni di copia aggiuntive, scegli se eseguire Copia impostazioni dell'origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni dell'origine, scegli Non specificare le impostazioni. Scegli Specifica le impostazioni per specificare le impostazioni per la classe di storage, le ACL, i tag degli oggetti, i metadati, la crittografia lato server e i checksum aggiuntivi.
9. Scegli Save changes (Salva modifiche).

Note

Questa azione applica la crittografia a tutti gli oggetti specificati. Durante la crittografia delle cartelle, attendere il completamento dell'operazione di salvataggio prima di aggiungere nuovi oggetti alla cartella.

Utilizzo della REST API

Al momento della creazione dell'oggetto, ovvero quando carichi un nuovo oggetto o fai una copia di un oggetto esistente, puoi specificare se desideri che Amazon S3 crittografi i tuoi dati con le chiavi gestite di Amazon S3 () aggiungendo l'intestazione alla richiesta. SSE-S3 `x-amz-server-side-encryption` Imposta il valore dell'intestazione sull'algoritmo della crittografia AES256 supportato da Amazon S3. Amazon S3 conferma che l'oggetto è archiviato con restituendo l'intestazione della risposta. SSE-S3 `x-amz-server-side-encryption`

Le operazioni API per il caricamento REST elencate di seguito accettano l'intestazione della richiesta `x-amz-server-side-encryption`.

- [PUT Object](#)
- [PUT Object - Copy](#)
- [POST Object](#)
- [Avvio del caricamento in più parti](#)

Quando si caricano oggetti di grandi dimensioni utilizzando l'operazione API per il caricamento in più parti, è possibile specificare la crittografia lato server aggiungendo l'intestazione `x-amz-server-side-encryption` alla richiesta di avvio del caricamento in più parti. Quando si copia un oggetto esistente, indipendentemente dal fatto che l'oggetto di origine sia stato o meno crittografato, l'oggetto di destinazione non viene crittografato, a meno che non si richieda esplicitamente la crittografia lato server.

Le intestazioni di risposta delle seguenti operazioni API REST restituiscono l'`x-amz-server-side-encryption` intestazione quando un oggetto viene archiviato utilizzando. SSE-S3

- [PUT Object](#)
- [PUT Object - Copy](#)
- [POST Object](#)
- [Avvio del caricamento in più parti](#)
- [Upload Part](#)
- [Caricamento di parte - Copy](#)
- [Completamento del caricamento in più parti](#)
- [Get Object](#)
- [Head Object](#)

 Note

Non inviate le intestazioni delle richieste di crittografia per GET richieste e HEAD richieste se l'oggetto utilizza SSE-S3, altrimenti riceverete un errore con codice di stato HTTP 400 (Bad Request).

Utilizzo di AWS SDK

Quando utilizzi AWS gli SDK, puoi richiedere ad Amazon S3 di utilizzare la crittografia lato server con le chiavi di crittografia gestite di Amazon S3 (). SSE-S3 Questa sezione fornisce esempi di utilizzo degli SDK in più AWS lingue. Per ulteriori informazioni su altri SDK, consulta [Codici di esempio e librerie](#).

Java

Quando si utilizza il AWS SDK per Java per caricare un oggetto, è possibile utilizzarlo SSE-S3 per crittografarlo. Per richiedere la crittografia lato server, utilizza la proprietà `ObjectMetadata` della `PutObjectRequest` per impostare l'intestazione della richiesta `x-amz-server-side-encryption`. Quando si utilizza il metodo `putObject()` di `AmazonS3Client`, Amazon S3 cripta i dati e li salva.

Puoi anche richiedere la SSE-S3 crittografia quando carichi oggetti con l'operazione API di caricamento in più parti:

- Quando si utilizza l'operazione API per il caricamento in più parti di alto livello, usi i metodi `TransferManager` per applicare la crittografia lato server agli oggetti durante il loro caricamento. È possibile utilizzare uno qualsiasi dei metodi di caricamento che accetta `ObjectMetadata` come parametro. Per ulteriori informazioni, consulta [Caricamento di un oggetto utilizzando il caricamento in più parti](#).
- Quando si utilizza l'operazione API per il caricamento in più parti di basso livello, specifichi la crittografia lato server quando avvii il caricamento in più parti. Si aggiungi la proprietà `ObjectMetadata` mediante una chiamata al metodo `InitiateMultipartUploadRequest.setObjectMetadata()`. Per ulteriori informazioni, consulta [Utilizzo di AWS SDK \(API di basso livello\)](#).

Non puoi direttamente modificare lo stato di crittografia di un oggetto (la crittografia di un oggetto non crittografato o la decrittografia dell'oggetto crittografato). Per modificare lo stato di crittografia

di un oggetto, effettuare una copia dell'oggetto, specificando lo stato di crittografia per la copia e poi eliminare l'oggetto originale. Amazon S3 esegue la crittografia dell'oggetto copiato solo se hai effettuato una richiesta specifica di crittografia lato server. Per richiedere la crittografia dell'oggetto copiato tramite l'API Java, utilizza la proprietà `ObjectMetadata` per specificare la crittografia lato server in `CopyObjectRequest`, come mostrato nell'esempio di codice Java riportato di seguito.

Example Esempio

L'esempio che segue mostra come impostare la crittografia lato server utilizzando AWS SDK per Java. Mostra come eseguire le seguenti operazioni:

- Carica un nuovo oggetto utilizzando. SSE-S3
- Modifica lo stato di crittografia di un oggetto (in questo esempio, crittografare un oggetto precedentemente non crittografato) eseguendo una copia dell'oggetto.
- Controlla lo stato di crittografia dell'oggetto.

Per ulteriori informazioni sulla crittografia lato server, consulta [Utilizzo della REST API](#). Per istruzioni su come creare e testare un campione funzionante, consulta [Getting Started](#) nella AWS SDK per Java Developer Guide.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.internal.SSEResultBase;
import com.amazonaws.services.s3.model.*;

import java.io.ByteArrayInputStream;

public class SpecifyServerSideEncryption {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "**** Bucket name ****";
        String keyNameToEncrypt = "**** Key name for an object to upload and encrypt ****";
        String keyNameToCopyAndEncrypt = "**** Key name for an unencrypted object to be encrypted by copying ****";
```

```
String copiedObjectName = "**** Key name for the encrypted copy of the
unencrypted object ****";

try {
    AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
        .withRegion(clientRegion)
        .withCredentials(new ProfileCredentialsProvider())
        .build();

    // Upload an object and encrypt it with SSE.
    uploadObjectWithSSEEncryption(s3Client, bucketName, keyNameToEncrypt);

    // Upload a new unencrypted object, then change its encryption state
    // to encrypted by making a copy.
    changeSSEEncryptionStatusByCopying(s3Client,
        bucketName,
        keyNameToCopyAndEncrypt,
        copiedObjectName);
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it, so it returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}

}

private static void uploadObjectWithSSEEncryption(AmazonS3 s3Client, String
bucketName, String keyName) {
    String objectContent = "Test object encrypted with SSE";
    byte[] objectBytes = objectContent.getBytes();

    // Specify server-side encryption.
    ObjectMetadata objectMetadata = new ObjectMetadata();
    objectMetadata.setContentLength(objectBytes.length);

    objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
    PutObjectRequest putRequest = new PutObjectRequest(bucketName,
        keyName,
        new ByteArrayInputStream(objectBytes),
        objectMetadata);
```

```

        // Upload the object and check its encryption status.
        PutObjectResult putResult = s3Client.putObject(putRequest);
        System.out.println("Object \"" + keyName + "\" uploaded with SSE.");
        printEncryptionStatus(putResult);
    }

    private static void changeSSEEncryptionStatusByCopying(AmazonS3 s3Client,
        String bucketName,
        String sourceKey,
        String destKey) {
        // Upload a new, unencrypted object.
        PutObjectResult putResult = s3Client.putObject(bucketName, sourceKey,
"Object example to encrypt by copying");
        System.out.println("Unencrypted object \"" + sourceKey + "\" uploaded.");
        printEncryptionStatus(putResult);

        // Make a copy of the object and use server-side encryption when storing the
        // copy.
        CopyObjectRequest request = new CopyObjectRequest(bucketName,
            sourceKey,
            bucketName,
            destKey);
        ObjectMetadata objectMetadata = new ObjectMetadata();

        objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
        request.setNewObjectMetadata(objectMetadata);

        // Perform the copy operation and display the copy's encryption status.
        CopyObjectResult response = s3Client.copyObject(request);
        System.out.println("Object \"" + destKey + "\" uploaded with SSE.");
        printEncryptionStatus(response);

        // Delete the original, unencrypted object, leaving only the encrypted copy
in
        // Amazon S3.
        s3Client.deleteObject(bucketName, sourceKey);
        System.out.println("Unencrypted object \"" + sourceKey + "\" deleted.");
    }

    private static void printEncryptionStatus(SSEResultBase response) {
        String encryptionStatus = response.getSSEAlgorithm();
        if (encryptionStatus == null) {
            encryptionStatus = "Not encrypted with SSE";
        }
    }

```

```
        System.out.println("Object encryption status is: " + encryptionStatus);  
    }  
}
```

.NET

Quando carichi un oggetto, puoi indirizzare Amazon S3 per crittografarlo. Per modificare lo stato di crittografia di un oggetto esistente, effettuare una copia dell'oggetto ed eliminare l'oggetto di origine. Per impostazione predefinita, l'operazione di copia crittografa la destinazione solo se si richiede esplicitamente la crittografia lato server dell'oggetto di destinazione. Per specificarlo SSE-S3 CopyObjectRequest, aggiungi quanto segue:

```
ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
```

Per un esempio di come copiare un oggetto, consulta [Utilizzo di AWS SDK](#).

Nel seguente esempio viene caricato un oggetto. Nella richiesta l'esempio indirizza Amazon S3 per crittografare l'oggetto. L'esempio poi recupera i metadati dell'oggetto e verifica i metodi di crittografia utilizzati. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella AWS SDK for .NET Developer Guide.

```
using Amazon;  
using Amazon.S3;  
using Amazon.S3.Model;  
using System;  
using System.Threading.Tasks;  
  
namespace Amazon.DocSamples.S3  
{  
    class SpecifyServerSideEncryptionTest  
    {  
        private const string bucketName = "**** bucket name ****";  
        private const string keyName = "**** key name for object created ****";  
        // Specify your bucket region (an example region is shown).  
        private static readonly RegionEndpoint bucketRegion =  
            RegionEndpoint.USWest2;  
        private static IAmazonS3 client;  
  
        public static void Main()  
        {  
            client = new AmazonS3Client(bucketRegion);  
        }  
    }  
}
```

```
        WritingAnObjectAsync().Wait();
    }

    static async Task WritingAnObjectAsync()
    {
        try
        {
            var putRequest = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                ContentBody = "sample text",
                ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
            };

            var putResponse = await client.PutObjectAsync(putRequest);

            // Determine the encryption state of an object.
            GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest
            {
                BucketName = bucketName,
                Key = keyName
            };
            GetObjectMetadataResponse response = await
client.GetObjectMetadataAsync(metadataRequest);
            ServerSideEncryptionMethod objectEncryption =
response.ServerSideEncryptionMethod;

            Console.WriteLine("Encryption method used: {0}",
objectEncryption.ToString());
        }
        catch (AmazonS3Exception e)
        {
            Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
        }
        catch (Exception e)
        {
            Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
        }
    }
}
```



```
}
```

PHP

Questo argomento mostra come utilizzare le classi della versione 3 AWS SDK per PHP per aggiungerle SSE-S3 agli oggetti caricati su Amazon S3. Per ulteriori informazioni sull'API AWS SDK for Ruby, consulta [AWS SDK for Ruby - Version 2](#).

Per caricare un oggetto su Amazon S3, si utilizza il metodo [Aws\S3\S3Client::putObject\(\)](#). Per aggiungere l'intestazione di richiesta `x-amz-server-side-encryption` alla richiesta di caricamento, specificare il parametro `ServerSideEncryption` con il valore `AES256`, come mostrato nel seguente esempio di codice. Per ulteriori informazioni sulla crittografia lato server delle richieste, consultare [Utilizzo della REST API](#).

```
require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

// $filepath should be an absolute path to a file on disk.
$filepath = '*** Your File Path ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Upload a file with server-side encryption.
$result = $s3->putObject([
    'Bucket'           => $bucket,
    'Key'              => $keyname,
    'SourceFile'       => $filepath,
    'ServerSideEncryption' => 'AES256',
]);
```

Nella risposta Amazon S3 restituisce l'intestazione `x-amz-server-side-encryption` con il valore dell'algoritmo di crittografia utilizzato per crittografare i dati dell'oggetto.

Quando carichi oggetti di grandi dimensioni utilizzando l'operazione API di caricamento in più parti, puoi specificare SSE-S3 gli oggetti che stai caricando, come segue:

- Quando utilizzi l'operazione API di caricamento in più parti di basso livello, specifica la crittografia lato server quando chiami il metodo [Aws\S3\S3Client::create\(\). MultipartUpload](#). Per aggiungere l'intestazione di richiesta x-amz-server-side-encryption alla richiesta, specificare la chiave array del parametro `ServerSideEncryption` con il valore `AES256`. Per ulteriori informazioni sull'operazione API per il caricamento in più parti di basso livello, consulta [Utilizzo di AWS SDK \(API di basso livello\)](#).
- Quando utilizzi l'operazione API di caricamento in più parti di alto livello, specifica la crittografia lato server utilizzando il parametro dell'operazione API. `ServerSideEncryption` [CreateMultipartUpload](#). Per un esempio di utilizzo del metodo `setOption()` con l'operazione API per il caricamento in più parti di alto livello, consulta [Caricamento di un oggetto utilizzando il caricamento in più parti](#).

Per determinare lo stato di crittografia di un oggetto esistente, recuperare i metadati dell'oggetto richiamando il metodo [Aws\S3\S3Client::headObject\(\)](#), come mostrato nell'esempio di codice PHP riportato di seguito.

```
require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Check which server-side encryption algorithm is used.
$result = $s3->headObject([
    'Bucket' => $bucket,
    'Key'    => $keyname,
]);
echo $result['ServerSideEncryption'];
```

Per modificare lo stato di crittografia di un oggetto esistente, effettuare una copia dell'oggetto utilizzando il metodo [Aws\S3\S3Client::copyObject\(\)](#) ed eliminare l'oggetto di origine. Per impostazione predefinita, `copyObject()` non esegue la crittografia della destinazione, a meno che non si richieda esplicitamente la crittografia lato server dell'oggetto di destinazione utilizzando il parametro `ServerSideEncryption` con il valore `AES256`. Il seguente esempio di codice PHP esegue una copia di un oggetto e aggiunge la crittografia lato server all'oggetto copiato.

```
require 'vendor/autoload.php';

use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';

$targetBucket = '*** Your Target Bucket Name ***';
$targetKeyname = '*** Your Target Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Copy an object and add server-side encryption.
$s3->copyObject([
    'Bucket'           => $targetBucket,
    'Key'              => $targetKeyname,
    'CopySource'       => "$sourceBucket/$sourceKeyname",
    'ServerSideEncryption' => 'AES256',
]);
```

Per ulteriori informazioni, consulta i seguenti argomenti:

- [AWS SDK per PHP per Amazon S3 `Aws\S3\S3Client` Class](#)
- [Documentazione di AWS SDK per PHP](#)

Ruby

Quando si utilizza AWS SDK per Ruby per caricare un oggetto, è possibile specificare che l'oggetto venga archiviato crittografato a riposo con. SSE-S3. Dopo essere stato letto, l'oggetto viene automaticamente decrittografato.

Il seguente esempio della AWS SDK per Ruby versione 3 dimostra come specificare che un file caricato su Amazon S3 deve essere crittografato quando è inattivo.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutSseWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  def put_object_encrypted(object_content, encryption)
    @object.put(body: object_content, server_side_encryption: encryption)
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put your content to #{object.key}. Here's why: #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-encrypted-content"
  object_content = "This is my super-secret content."
  encryption = "AES256"

  wrapper = ObjectPutSseWrapper.new(Aws::S3::Object.new(bucket_name,
    object_content))
  return unless wrapper.put_object_encrypted(object_content, encryption)

  puts "Put your content into #{bucket_name}:#{object_key} and encrypted it with
    #{encryption}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

L'esempio di codice seguente dimostra come determinare lo stato di crittografia di un oggetto esistente.

```

require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectGetEncryptionWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Gets the object into memory.
  #
  # @return [Aws::S3::Types::GetObjectOutput, nil] The retrieved object data if
  # successful; otherwise nil.
  def object
    @object.get
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't get object #{@object.key}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object.txt"

  wrapper = ObjectGetEncryptionWrapper.new(Aws::S3::Object.new(bucket_name,
    object_key))
  obj_data = wrapper.get_object
  return unless obj_data

  encryption = obj_data.server_side_encryption.nil? ? 'no' :
    obj_data.server_side_encryption
  puts "Object #{object_key} uses #{encryption} encryption."
end

run_demo if $PROGRAM_NAME == __FILE__

```

Se la crittografia lato server non viene utilizzata per l'oggetto archiviato in Amazon S3, il metodo restituisce `null`.

Per modificare lo stato di crittografia di un oggetto esistente, effettuare una copia dell'oggetto ed eliminare l'oggetto di origine. Per default, i metodi di copia non eseguono la crittografia della destinazione, a meno che non si richieda esplicitamente la crittografia lato server. È possibile richiedere la crittografia dell'oggetto di destinazione specificando il valore `server_side_encryption` nell'argomento hash dell'opzione, come mostrato nel seguente esempio di codice Ruby. L'esempio di codice dimostra come copiare un oggetto e crittografare la copia con. SSE-S3

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyEncryptWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
  # used as the source object for
  #                                     copy actions.
  def initialize(source_object)
    @source_object = source_object
  end

  # Copy the source object to the specified target bucket, rename it with the target
  # key, and encrypt it.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
  # object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
  # nil.
  def copy_object(target_bucket, target_object_key, encryption)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key,
server_side_encryption: encryption)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
#{e.message}"
  end
end

# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
```

```

source_key = "my-source-file.txt"
target_bucket_name = "amzn-s3-demo-bucket2"
target_key = "my-target-file.txt"
target_encryption = "AES256"

source_bucket = Aws::S3::Bucket.new(source_bucket_name)
wrapper = ObjectCopyEncryptWrapper.new(source_bucket.object(source_key))
target_bucket = Aws::S3::Bucket.new(target_bucket_name)
target_object = wrapper.copy_object(target_bucket, target_key, target_encryption)
return unless target_object

puts "Copied #{source_key} from #{source_bucket_name} to
#{target_object.bucket_name}:#{target_object.key} and "\
    "encrypted the target with #{target_object.server_side_encryption}
encryption."
end

run_demo if $PROGRAM_NAME == __FILE__

```

Utilizzo di AWS CLI

Per specificare SSE-S3 quando si carica un oggetto utilizzando il AWS CLI, utilizzare l'esempio seguente.

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key object-key-name --server-side-encryption AES256 --body file path
```

Per ulteriori informazioni, consulta [put-object](#) in Riferimenti della AWS CLI . Per specificare SSE-S3 quando si copia un oggetto utilizzando il AWS CLI, vedere <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/copy-object.html> `copy-object`.

Utilizzo CloudFormation

Per esempi di configurazione della crittografia utilizzando CloudFormation, consulta [Creare un bucket con crittografia predefinita](#) e [Creare un bucket utilizzando la crittografia AWS KMS lato server con una chiave](#) bucket S3 nell'argomento della Guida per l'utente. `Aws::S3::Bucket` `ServerSideEncryptionRule` AWS CloudFormation

Utilizzo della crittografia lato server con AWS KMS chiavi () SSE-KMS

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS. Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

Server-side la crittografia è la crittografia dei dati a destinazione da parte dell'applicazione o del servizio che li riceve.

Amazon S3 abilita automaticamente la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) per il caricamento di nuovi oggetti.

Salvo diversa indicazione, i bucket vengono utilizzati SSE-S3 per impostazione predefinita per crittografare gli oggetti. Tuttavia, puoi scegliere di configurare i bucket per utilizzare invece la crittografia lato server con AWS Key Management Service (AWS KMS) keys (). SSE-KMS Per ulteriori informazioni, consulta [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#).

AWS KMS è un servizio che combina hardware e software sicuri e ad alta disponibilità per fornire un sistema di gestione delle chiavi scalabile per il cloud. Amazon S3 utilizza la crittografia lato server con AWS KMS (SSE-KMS) per crittografare i dati degli oggetti S3. Inoltre, quando SSE-KMS viene richiesto l'oggetto, il checksum S3 (come parte dei metadati dell'oggetto) viene archiviato in forma crittografata. Per ulteriori informazioni sui checksum, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Se utilizzi le chiavi KMS, puoi utilizzarle AWS KMS tramite [Console di gestione AWS](#) o l'[AWS KMS API](#) per effettuare le seguenti operazioni:

- Creare, visualizzare, modificare, monitorare, abilitare o disabilitare, ruotare e pianificare l'eliminazione delle chiavi KMS in modo centralizzato.
- Definire le policy che controllano come e da chi possono essere utilizzate le chiavi KMS.

- Controllare l'utilizzo delle chiavi KMS per verificarne l'uso corretto. Il controllo è supportato dall'[API AWS KMS](#), ma non dalla [console AWS KMS](#).

I controlli di sicurezza in ingresso AWS KMS possono aiutarti a soddisfare i requisiti di conformità relativi alla crittografia. Puoi utilizzare queste chiavi KMS per proteggere i dati nei bucket Amazon S3. Quando si utilizza SSE-KMS la crittografia con un bucket S3, questo AWS KMS keys deve trovarsi nella stessa regione del bucket.

Sono previsti costi aggiuntivi per l'utilizzo. AWS KMS keys Per ulteriori informazioni, consulta la sezione [Concetti di AWS KMS key](#) nella Guida per gli sviluppatori di AWS Key Management Service e i [Prezzi di AWS KMS](#).

Per istruzioni su come consentire agli utenti IAM di accedere ai KMS-encrypted bucket, consulta [My Amazon S3 bucket has default encryption using a custom key. AWS KMS Come posso consentire agli utenti di scaricare e caricare nel bucket?](#) nel AWS re:Post Knowledge Center.

Permissions

Per effettuare correttamente una richiesta `PutObject` per crittografare un oggetto con una chiave AWS KMS su Amazon S3, sono necessarie le autorizzazioni `kms:GenerateDataKey` per la chiave. Per scaricare un oggetto crittografato con un AWS KMS key, sono necessarie `kms:Decrypt` le autorizzazioni per la chiave. Per [eseguire un caricamento in più parti](#) per crittografare un oggetto con un AWS KMS key, è necessario disporre delle `kms:Decrypt` autorizzazioni `kms:GenerateDataKey` e per la chiave.

Important

- Esamina attentamente le autorizzazioni concesse nelle policy delle chiavi KMS. Limita sempre le autorizzazioni delle policy chiave KMS gestite dal cliente solo ai principali e ai AWS servizi IAM che devono accedere all'azione chiave pertinente. AWS KMS Per ulteriori informazioni, consulta [Policy delle chiavi in AWS KMS](#).
- Se un bucket viene utilizzato come destinazione per la registrazione degli accessi al server Amazon S3, il bucket di destinazione deve utilizzare le chiavi gestite da Amazon S3 (). SSE-S3 Se il bucket di destinazione utilizza la crittografia SSE-KMS predefinita, Amazon S3 potrebbe fornire oggetti di log crittografati con una chiave a cui non puoi accedere. Per risolvere questo problema, modifica la crittografia predefinita del bucket di destinazione in.

SSE-S3 Per ulteriori informazioni, consulta [Abilitazione della registrazione degli accessi al server Amazon S3](#).

Argomenti

- [AWS KMS keys](#)
- [Chiavi bucket Amazon S3](#)
- [Richiesta della crittografia lato server](#)
- [Contesto di crittografia](#)
- [Invio di richieste per AWS KMS oggetti crittografati](#)
- [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#)
- [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#)

AWS KMS keys

Quando utilizzi la crittografia lato server con AWS KMS (SSE-KMS), puoi utilizzare la chiave [AWS gestita predefinita oppure puoi specificare una chiave](#) gestita [dal cliente](#) che hai già creato. AWS KMS supporta la crittografia delle buste. S3 utilizza le AWS KMS funzionalità di crittografia delle buste per proteggere ulteriormente i dati. La crittografia a busta consiste nel crittografare i dati di testo non crittografato con una chiave di dati e quindi nel crittografare la chiave di dati con una chiave KMS. Per ulteriori informazioni sulla crittografia envelope, consulta [Crittografia envelope](#) nella Guida per sviluppatori di AWS Key Management Service .

Se non specifichi una chiave gestita dal cliente, Amazon S3 ne crea automaticamente una Chiave gestita da AWS in Account AWS la prima volta che aggiungi un oggetto crittografato con SSE-KMS un bucket. Per impostazione predefinita, Amazon S3 utilizza questa chiave KMS per. SSE-KMS

Note

Gli oggetti crittografati utilizzando SSE-KMS with non [Chiavi gestite da AWS](#) possono essere condivisi tra più account. Se devi condividere SSE-KMS i dati tra più account, devi utilizzare una chiave [gestita](#) dal cliente di. AWS KMS

Se desideri utilizzare una chiave gestita dal cliente per SSE-KMS, crea una chiave gestita dal cliente con crittografia simmetrica prima della configurazione. SSE-KMS Quindi, quando SSE-KMS configuri

il bucket, specifica la chiave gestita dal cliente esistente. Per ulteriori informazioni sulla chiave di crittografia simmetrica, consulta [Chiavi KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori di AWS Key Management Service .

La creazione di una chiave gestita dal cliente offre maggiore flessibilità e controllo. Ad esempio, puoi creare, ruotare e disabilitare le chiavi gestite dal cliente. Puoi anche definire controlli di accesso e controllare le chiavi gestite dal cliente utilizzate per proteggere i dati. Per ulteriori informazioni sulle chiavi gestite e AWS gestite dal cliente, consulta Chiavi e AWS chiavi [del cliente](#) nella Guida per gli AWS Key Management Service sviluppatori.

Note

Quando utilizzi la crittografia lato server con una chiave gestita dal cliente archiviata in un archivio di chiavi esterno, a differenza delle chiavi KMS standard, hai la responsabilità di garantire la disponibilità e la durata del materiale chiave. Per ulteriori informazioni sugli archivi di chiavi esterni e sul loro impatto sul modello di responsabilità condivisa, vedi [Archivi di chiavi esterni](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Utilizzo della SSE-KMS crittografia per le operazioni su più account

Quando si utilizza la crittografia per operazioni multi-account, tieni presente quanto segue:

- Se un AWS KMS key Amazon Resource Name (ARN) o un alias non viene fornito al momento della richiesta o tramite la configurazione di crittografia predefinita del bucket, la Chiave gestita da AWS (aws/s3) dell'account di caricamento viene utilizzata per la crittografia e richiesta per la decrittografia.
- Chiave gestita da AWS (aws/s3) può essere utilizzata come chiave KMS per operazioni su più account quando i principali di caricamento e accesso AWS Identity and Access Management (IAM) sono gli stessi. Account AWS
- Se desideri concedere l'accesso multi-account agli oggetti S3, utilizza una chiave gestita dal cliente. È possibile configurare la policy di una chiave gestita dal cliente per consentire l'accesso da un altro account.
- Se si specifica una chiave KMS gestita dal cliente, si consiglia di utilizzare un ARN della chiave KMS completamente qualificato. Se invece utilizzi un alias di chiave KMS, AWS KMS risolve la chiave all'interno dell'account del richiedente. Ciò potrebbe comportare la crittografia dei dati con una chiave KMS di proprietà del richiedente e non del proprietario del bucket.

- È necessario specificare una chiave per cui il richiedente ha ottenuto l'autorizzazione Encrypt. Per ulteriori informazioni, consulta l'argomento relativo all'[autorizzazione concessa agli utenti delle chiavi di utilizzare una chiave KMS per le operazioni di crittografia](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni su quando utilizzare le chiavi gestite dal cliente e le chiavi KMS AWS gestite, consulta [Devo usare una Chiave gestita da AWS o una chiave gestita dal cliente per crittografare i miei oggetti in Amazon S3?](#)

SSE-KMS flusso di lavoro di crittografia

Se scegli di crittografare i tuoi dati utilizzando una Chiave gestita da AWS o una chiave gestita dal cliente, AWS KMS Amazon S3 esegue le seguenti azioni di crittografia a inviluppo:

1. Amazon S3 richiede una [chiave di dati](#) in testo non formattato e una copia della chiave crittografata con la chiave KMS specificata.
2. AWS KMS genera una chiave dati, la crittografa con la chiave KMS e invia sia la chiave dati in testo normale che la chiave dati crittografata ad Amazon S3.
3. Amazon S3 crittografa i dati utilizzando la chiave di dati ed eliminando appena possibile la chiave di testo normale dalla memoria dopo l'utilizzo.
4. Amazon S3 archivia la chiave di dati crittografata come metadati con i dati crittografati.

Quando richiedi che i tuoi dati vengano decrittografati, Amazon S3 esegue le seguenti azioni: AWS KMS

1. Amazon S3 invia la chiave di dati crittografata a AWS KMS in una richiesta. Decrypt
2. AWS KMS decrittografa la chiave dati crittografata utilizzando la stessa chiave KMS e restituisce la chiave dati in testo normale ad Amazon S3.
3. Amazon S3 utilizza la chiave di dati non crittografati per decrittografare i dati crittografati, quindi rimuove il prima possibile la chiave di dati non crittografati dalla memoria.

Important

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia

simmetrica. Per ulteriori informazioni sulle chiavi, consulta [Chiavi KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Verifica della crittografia SSE-KMS

Per identificare le richieste specificate SSE-KMS, puoi utilizzare le metriche. Tutte le SSE-KMS richieste e% tutte le SSE-KMS richieste in Amazon S3 Storage Lens. S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti. Puoi anche utilizzare i bucket count SSE-KMS abilitati e% bucket SSE-KMS enabled per comprendere il numero di bucket that () SSE-KMS per la crittografia predefinita dei bucket. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html> Per ulteriori informazioni, consulta [Valutazione dell'attività e dell'utilizzo dello storage con S3 Storage Lens](#). Per un elenco completo dei parametri, consulta [Glossario dei parametri di S3 Storage](#).

Per verificare l'utilizzo delle AWS KMS chiavi per i dati SSE-KMS crittografati, puoi utilizzare i log. AWS CloudTrail Puoi ottenere informazioni dettagliate sulle tue operazioni [crittografiche](#), ad esempio [GenerateDataKey](#) e [Decrypt](#). CloudTrail supporta numerosi valori di [attributo](#) per filtrare la ricerca, tra cui nome dell'evento, nome utente e origine dell'evento.

Chiavi bucket Amazon S3

Quando configuri la crittografia lato server utilizzando AWS KMS (SSE-KMS), puoi configurare i tuoi bucket in modo che utilizzino S3 Bucket Keys per. SSE-KMS L'utilizzo di una chiave a livello di bucket per SSE-KMS può ridurre i costi delle AWS KMS richieste fino al 99% diminuendo il traffico di richieste da Amazon S3 a. AWS KMS

Quando configuri un bucket per utilizzare una chiave S3 Bucket SSE-KMS su nuovi oggetti, AWS KMS genera una chiave a livello di bucket che viene utilizzata per creare chiavi di dati univoche per gli oggetti nel bucket. <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys> Questa chiave bucket S3 viene utilizzata per un periodo di tempo limitato all'interno di Amazon S3, riducendo ulteriormente la necessità per Amazon S3 di effettuare richieste per completare le operazioni di crittografia. AWS KMS Per ulteriori informazioni sull'utilizzo delle chiavi del bucket S3, consulta la sezione [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

Richiesta della crittografia lato server

Per richiedere la crittografia lato server di tutti gli oggetti in uno specifico bucket Amazon S3, è possibile utilizzare una policy di bucket. Ad esempio, la seguente policy bucket nega l'autorizzazione

upload object (s3:PutObject) a tutti se la richiesta non include un'`x-amz-server-side-encryption-aws-kms-key-id` intestazione che richiede la crittografia lato server con. SSE-KMS

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PutObjectPolicy",
  "Statement": [{
    "Sid": "DenyObjectsThatAreNotSSEKMS",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
      }
    }
  }]
}
```

Per richiedere l'uso di un particolare AWS KMS key per crittografare gli oggetti in un bucket, puoi utilizzare la chiave di condizione. `s3:x-amz-server-side-encryption-aws-kms-key-id` Per specificare la chiave KMS, devi utilizzare una chiave Amazon Resource Name (ARN) nel formato indicato. `arn:aws:kms:region:acct-id:key/key-id` AWS Identity and Access Management non convalida se la stringa per esiste. `s3:x-amz-server-side-encryption-aws-kms-key-id`

Note

Quando si carica un oggetto, è possibile specificare la chiave KMS utilizzando l'intestazione `x-amz-server-side-encryption-aws-kms-key-id` o affidarsi alla [configurazione predefinita della crittografia del bucket](#). Se la tua PutObject richiesta è specificata `aws:kms` nell'`x-amz-server-side-encryption` intestazione, ma non nell'`x-amz-server-side-encryption-aws-kms-key-id` intestazione, Amazon S3 presuppone che tu voglia utilizzare il. Chiave gestita da AWS In ogni caso, l'ID AWS KMS chiave utilizzato da Amazon

S3 per la crittografia degli oggetti deve corrispondere all'ID della AWS KMS chiave nella policy, altrimenti Amazon S3 respinge la richiesta.

Per un elenco completo delle chiavi di condizione specifiche per Amazon S3, consulta [Chiavi di condizione per Amazon S3](#) in Riferimento alle autorizzazioni di servizio.

Contesto di crittografia

Un contesto di crittografia è un set di coppie chiave-valore che contiene ulteriori informazioni contestuali sui dati. Il contesto di crittografia non è crittografato. Quando viene specificato un contesto di crittografia per un'operazione di crittografia, Amazon S3 deve specificare lo stesso contesto di crittografia per l'operazione di decrittografia. In caso contrario, la decrittografia non riesce. AWS KMS utilizza il contesto di crittografia come dati autenticati [aggiuntivi](#) (AAD) per supportare la crittografia autenticata. <https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#cryptographic-operations#digital-sigs> Per ulteriori informazioni sul contesto di crittografia, consulta il [Contesto di crittografia](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per impostazione predefinita, Amazon S3 utilizza il nome della risorsa Amazon (ARN) dell'oggetto o del bucket come coppia di contesto di crittografia:

- Se si utilizza SSE-KMS senza abilitare una chiave S3 Bucket, l'oggetto ARN viene utilizzato come contesto di crittografia.

```
arn:aws:s3:::object_ARN
```

- Se si utilizza SSE-KMS e si abilita una chiave bucket S3, l'ARN del bucket viene utilizzato come contesto di crittografia. Per ulteriori informazioni sui bucket S3, consulta la sezione [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

```
arn:aws:s3:::bucket_ARN
```

È possibile fornire facoltativamente una coppia di contesti di crittografia aggiuntiva utilizzando l'`x-amz-server-side-encryption-context` in una richiesta s3: [PutObject](#). Tuttavia, poiché il contesto di crittografia non è crittografato, assicurati che non includa informazioni sensibili. Amazon S3 archivia questa coppia di chiavi aggiuntiva insieme al contesto di crittografia predefinito. Quando elabora la tua richiesta PUT, Amazon S3 aggiunge il contesto di crittografia predefinito di `aws:s3:arn` a quello che fornisci.

È possibile utilizzare il contesto di crittografia per identificare e categorizzare le operazioni di crittografia. Puoi anche utilizzare il valore ARN del contesto di crittografia predefinito per tenere traccia delle richieste pertinenti AWS CloudTrail visualizzando quale ARN Amazon S3 è stato utilizzato con quale chiave di crittografia.

Nel `requestParameters` campo di un file di CloudTrail registro, il contesto di crittografia è simile a quello seguente.

```
"encryptionContext": {  
  "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1/file_name"  
}
```

Quando si utilizza SSE-KMS la funzionalità opzionale S3 Bucket Keys, il valore del contesto di crittografia è l'ARN del bucket.

```
"encryptionContext": {  
  "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1"  
}
```

Invio di richieste per AWS KMS oggetti crittografati

Important

Tutte GET le PUT richieste di oggetti AWS KMS crittografati devono essere effettuate utilizzando Secure Sockets Layer (SSL) o Transport Layer Security (TLS). Le richieste devono inoltre essere firmate utilizzando credenziali valide, come AWS Signature Version 4 (o AWS Signature Version 2).

AWS La versione 4 di Signature è il processo di aggiunta delle informazioni di autenticazione alle AWS richieste inviate tramite HTTP. Per motivi di sicurezza, la maggior parte delle richieste AWS deve essere firmata con una chiave di accesso, costituita da un ID della chiave di accesso e una chiave di accesso segreta. Queste due chiavi in genere vengono definite come le tue credenziali di sicurezza. Per ulteriori informazioni, consulta le sezioni [Autenticazione delle richieste \(AWS Signature Version 4\)](#) e [Processo di firma Signature Version 4](#).

 Important

Se il tuo oggetto utilizza SSE-KMS, non inviare intestazioni di richiesta di crittografia per GET richieste e HEAD richieste. In caso contrario, riceverai un errore HTTP 400 Bad Request (HTTP 400 - Richiesta non valida).

Argomenti

- [Specificare la crittografia lato server con AWS KMS \(SSE-KMS\)](#)
- [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#)

Specificare la crittografia lato server con AWS KMS (SSE-KMS)

Tutti i bucket Amazon S3 hanno la crittografia configurata di default e tutti i nuovi oggetti caricati in un bucket S3 vengono crittografati automaticamente quando sono inattivi. Server-side la crittografia con chiavi gestite da Amazon S3 (SSE-S3) è la configurazione di crittografia predefinita per ogni bucket in Amazon S3. Per utilizzare un diverso tipo di crittografia, puoi specificare il tipo di crittografia lato server da utilizzare nelle richieste PUT S3 oppure aggiornare la configurazione di crittografia predefinita nel bucket di destinazione.

Se desideri specificare un tipo di crittografia diverso nelle tue PUT richieste, puoi utilizzare la crittografia lato server con () chiavi AWS Key Management Service (AWS KMS), la crittografia lato server a doppio livello con chiavi (SSE-KMS) o la crittografia lato server con AWS KMS chiavi fornite dal cliente (DSSE-KMS). SSE-C Se desideri impostare una diversa configurazione di crittografia predefinita nel bucket di destinazione, puoi utilizzare o. SSE-KMS DSSE-KMS

Per ulteriori informazioni su come modificare la configurazione di crittografia predefinita per i bucket per uso generico, consulta [Configurazione della crittografia predefinita](#).

Quando modifichi la configurazione di crittografia predefinita del bucket in SSE-KMS, il tipo di crittografia degli oggetti Amazon S3 esistenti nel bucket non viene modificato. Per modificare il tipo di crittografia degli oggetti preesistenti dopo aver aggiornato la configurazione di crittografia predefinita in SSE-KMS, puoi utilizzare Amazon S3 Batch Operations. Si fornisce a Operazioni in batch S3 un elenco di oggetti e Operazioni in batch richiama la rispettiva operazione API. Puoi utilizzare l'[Copia oggetti](#) per copiare oggetti esistenti e riscriverli nello stesso bucket degli oggetti crittografati SSE-KMS. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le](#)

[operazioni in batch](#) e il post [Come crittografare retroattivamente gli oggetti esistenti in Amazon S3 utilizzando Inventario S3, Amazon Athena e Operazioni in batch S3](#) nel Blog dell'archiviazione AWS .

Puoi specificarlo SSE-KMS utilizzando la console Amazon S3, le operazioni API REST, AWS gli SDK e (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta i seguenti argomenti.

Note

Puoi usare Multi-region AWS KMS keys in Amazon S3. Tuttavia, Amazon S3 attualmente tratta le chiavi multiregionali come se fossero chiavi monoregionali e non utilizza le caratteristiche multiregionali della chiave. Per ulteriori informazioni, consulta [Utilizzo delle chiavi multiregione](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Note

Se si desidera utilizzare una chiave KMS di proprietà di un altro account, è necessario avere l'autorizzazione a utilizzarla. Per ulteriori informazioni sulle autorizzazioni tra account per le chiavi KMS, vedi [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Utilizzo della console S3

Questo argomento descrive come impostare o modificare il tipo di crittografia di un oggetto per utilizzare la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS) utilizzando la console Amazon S3.

Note

- È possibile modificare la crittografia di un oggetto se l'oggetto è inferiore a 5 GB. Se l'oggetto è superiore a 5 GB, è necessario utilizzare gli SDK [AWS CLI](#) o [AWS per modificare la crittografia di un oggetto](#).
- Per un elenco delle autorizzazioni aggiuntive necessarie per modificare la crittografia di un oggetto, consulta [the section called “Autorizzazioni necessarie per le operazioni API S3”](#). Per esempi di policy che concedono questa autorizzazione, consulta [the section called “Identity-based esempi di policy”](#).

- Se si modifica la crittografia di un oggetto, viene creato un nuovo oggetto per sostituire quello precedente. Se è abilitata la funzione Controllo delle versioni S3, viene creata una nuova versione dell'oggetto e l'oggetto esistente diventa una versione precedente. Il ruolo che modifica la proprietà diventa anche il proprietario del nuovo oggetto o della versione dell'oggetto.

Per aggiungere o modificare la crittografia di un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket, quindi scegli la scheda Bucket per uso generico. Naviga al bucket o alla cartella Amazon S3 che contiene gli oggetti da modificare.
3. Seleziona la casella di controllo degli oggetti da modificare.
4. Nel menu Azioni, scegli Modifica crittografia lato server dall'elenco di opzioni visualizzato.
5. Scorri fino alla sezione Server-side di crittografia.
6. In Impostazioni di crittografia, scegli Utilizza le impostazioni del bucket per la crittografia predefinita o Ignora le impostazioni del bucket per la crittografia predefinita.

 Important

Se si utilizza l' SSE-KMS opzione per la configurazione di crittografia predefinita, si è soggetti alle quote di richieste al secondo (RPS) di AWS KMS. Per ulteriori informazioni sulle quote AWS KMS e su come richiedere un aumento delle quote, consulta [Quote](#) nella Guida per gli sviluppatori di AWS Key Management Service .

7. Se scegli Sostituisci impostazioni del bucket per la crittografia predefinita, configura le seguenti impostazioni di crittografia.
 - a. In Tipo di crittografia, scegli Server-side la crittografia con AWS Key Management Service chiavi (SSE-KMS).
 - b. In AWS KMS key, esegui una delle seguenti operazioni per scegliere la chiave KMS:
 - Per scegliere da un elenco di chiavi KMS disponibili, seleziona Scegli tra le chiavi AWS KMS keys, quindi scegli la chiave KMS dall'elenco delle chiavi disponibili.

In questo elenco vengono visualizzate sia le chiavi Chiave gestita da AWS (aws/s3) che quelle gestite dal cliente. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per inserire l'ARN della chiave KMS, scegli Inserisci AWS KMS key ARN, quindi inserisci l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

 Important

È possibile utilizzare solo le chiavi KMS disponibili nella Regione AWS stesso bucket. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, devi inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione necessaria per l'uso della chiave e quindi inserire l'ARN della chiave KMS.

Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

8. In Impostazioni di copia aggiuntive, scegli se eseguire Copia impostazioni dell'origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni dell'origine, scegli Non specificare le impostazioni. Scegli Specifica le impostazioni per specificare le impostazioni per la classe di storage, le ACL, i tag degli oggetti, i metadati, la crittografia lato server e i checksum aggiuntivi.
9. Scegli Save changes (Salva modifiche).

 Note

Questa azione applica la crittografia a tutti gli oggetti specificati. Durante la crittografia delle cartelle, attendere il completamento dell'operazione di salvataggio prima di aggiungere nuovi oggetti alla cartella.

Utilizzo della REST API

Quando crei un oggetto, ovvero quando carichi un nuovo oggetto o copi un oggetto esistente, puoi specificare l'uso della crittografia lato server con () per crittografare i tuoi dati. AWS KMS keys SSE-KMS Per fare ciò, aggiungi l'intestazione `x-amz-server-side-encryption` alla richiesta. Impostare il valore dell'intestazione sull'algoritmo di crittografia `aws:kms`. Amazon S3 conferma che l'oggetto è archiviato utilizzando restituendo l'intestazione della risposta. SSE-KMS `x-amz-server-side-encryption`

Se specifichi l'intestazione `x-amz-server-side-encryption` con il valore `aws:kms`, puoi anche utilizzare le intestazioni di richiesta seguenti:

- `x-amz-server-side-encryption-aws-kms-key-id`
- `x-amz-server-side-encryption-context`
- `x-amz-server-side-encryption-bucket-key-enabled`

Argomenti

- [Operazioni API REST di Amazon S3 che supportano SSE-KMS](#)
- [Contesto di crittografia \(x-amz-server-side-encryption-context\)](#)
- [AWS KMS ID della chiave \(x-amz-server-side-encryption-aws-kms-key-id\)](#)
- [Chiavi S3 Bucket \(x-amz-server-side-encryption-aws-bucket-key-enabled\)](#)

Operazioni API REST di Amazon S3 che supportano SSE-KMS

Le operazioni REST API seguenti accettano le intestazioni di richiesta `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id` e `x-amz-server-side-encryption-context`.

- [PutObject](#): quando carichi i dati utilizzando l'operazione API PUT, è possibile specificare queste intestazioni di richiesta.

- [CopyObject](#) - Quando si copia un oggetto, si ha un oggetto di origine e un oggetto di destinazione. Quando si trasmettono le SSE-KMS intestazioni con l'CopyObject operazione, queste vengono applicate solo all'oggetto di destinazione. Quando si copia un oggetto esistente, indipendentemente dal fatto che l'oggetto di partenza sia criptato o meno, l'oggetto di destinazione non viene criptato, a meno che non si richieda esplicitamente la crittografia lato server.
- [POST Object](#) - Quando si usa un'operazione POST per caricare un oggetto, invece delle intestazioni della richiesta, si forniscono le stesse informazioni nei campi del modulo.
- [CreateMultipartUpload](#) - Quando si caricano oggetti di grandi dimensioni utilizzando l'operazione API di caricamento multipart, è possibile specificare queste intestazioni. Queste intestazioni vengono specificate nella richiesta CreateMultipartUpload.

Le intestazioni di risposta delle seguenti operazioni REST API restituiscono l'intestazione x-amz-server-side-encryption quando un oggetto viene memorizzato utilizzando la crittografia lato server.

- [PutObject](#)
- [CopyObject](#)
- [POST Object](#)
- [CreateMultipartUpload](#)
- [UploadPart](#)
- [UploadPartCopy](#)
- [CompleteMultipartUpload](#)
- [GetObject](#)
- [HeadObject](#)

 Important

- Tutte le richieste di GET e PUT per un oggetto protetto da AWS KMS falliscono se non si effettuano queste richieste utilizzando Secure Sockets Layer (SSL), Transport Layer Security (TLS) o Signature Version 4.
- Se il tuo oggetto utilizza SSE-KMS, non inviare intestazioni di richiesta di crittografia per GET richieste e HEAD richieste, altrimenti riceverai un errore HTTP 400 BadRequest.

Contesto di crittografia (x-amz-server-side-encryption-context)

Se si specifica `x-amz-server-side-encryption:aws:kms`, l'API Amazon S3 supporta un contesto di crittografia con l'intestazione `x-amz-server-side-encryption-context`. Un contesto di crittografia è un set di coppie chiave-valore che possono contenere ulteriori informazioni contestuali sui dati.

Amazon S3 utilizza automaticamente l'oggetto o il bucket Amazon Resource Name (ARN) come coppia di contesto di crittografia. Se si utilizza SSE-KMS senza abilitare una chiave S3 Bucket, si utilizza l'oggetto ARN come contesto di crittografia; ad esempio, `arn:aws:s3:::object_ARN`. Tuttavia, se si utilizza SSE-KMS e si abilita una chiave S3 Bucket, si utilizza il bucket ARN per il contesto di crittografia; ad esempio, `arn:aws:s3:::bucket_ARN`.

Facoltativamente, è possibile fornire una coppia di contesto di crittografia aggiuntiva utilizzando l'intestazione `x-amz-server-side-encryption-context`. Tuttavia, poiché il contesto di crittografia non è criptato, assicurarsi che non contenga informazioni sensibili. Amazon S3 archivia questa coppia di chiavi aggiuntiva insieme al contesto di crittografia predefinito.

Per informazioni sul contesto di crittografia in Amazon S3, consulta la sezione [Contesto di crittografia](#). Per informazioni generali sul contesto di crittografia, consulta [Concetti di AWS Key Management Service : Contesto di crittografia](#) nella Guida per gli sviluppatori di AWS Key Management Service .

AWS KMS ID della chiave (x-amz-server-side-encryption-aws-kms-key-id)

Puoi utilizzare l'intestazione `x-amz-server-side-encryption-aws-kms-key-id` per specificare l'ID della chiave gestita dal cliente utilizzata per proteggere i dati. Se specifichi l'intestazione `x-amz-server-side-encryption:aws:kms`, ma non fornisci l'intestazione `x-amz-server-side-encryption-aws-kms-key-id`, Amazon S3 utilizza la Chiave gestita da AWS (`aws/s3`) per proteggere i dati. Se desideri utilizzare una chiave gestita dal cliente, devi fornire l'intestazione `x-amz-server-side-encryption-aws-kms-key-id` della chiave gestita dal cliente.

Important

Quando utilizzi una crittografia lato server in Amazon S3, devi scegliere una AWS KMS key chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetrica. Per ulteriori informazioni sulle chiavi, consulta [Chiavi KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Chiavi S3 Bucket (x-amz-server-side-encryption-aws-bucket-key-enabled)

È possibile utilizzare l'intestazione della richiesta `x-amz-server-side-encryption-aws-bucket-key-enabled` per abilitare o disabilitare un bucket S3 Key a livello di oggetto. Le chiavi S3 Bucket riducono i costi delle richieste diminuendo il traffico di richieste da Amazon AWS KMS S3 a. AWS KMS Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

Se specifichi l'intestazione `x-amz-server-side-encryption:aws:kms` ma non fornisci l'intestazione `x-amz-server-side-encryption-aws-bucket-key-enabled`, per crittografare l'oggetto saranno utilizzate le impostazioni della chiave bucket S3 per il bucket di destinazione. Per ulteriori informazioni, consulta [Configurazione di una chiave bucket S3 a livello di oggetto](#).

Utilizzo di AWS CLI

Per utilizzare i seguenti AWS CLI comandi di esempio, sostituiscili *user input placeholders* con le tue informazioni.

Quando si carica un nuovo oggetto o si copia un oggetto esistente, è possibile specificare l'uso della crittografia lato server con AWS KMS chiavi per crittografare i dati. Per fare ciò, aggiungi l'intestazione `--server-side-encryption aws:kms` alla richiesta. Usa `--ssekms-key-id example-key-id` per aggiungere la AWS KMS chiave gestita [dal cliente](#) che hai creato. Se specifichi `--server-side-encryption aws:kms`, ma non fornisci un ID AWS KMS chiave, Amazon S3 utilizzerà una chiave AWS gestita.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-side-encryption aws:kms --ssekms-key-id example-key-id --body filepath
```

Puoi inoltre abilitare o disabilitare le chiavi di bucket Amazon S3 nelle operazioni PUT o COPY aggiungendo `--bucket-key-enabled` o `--no-bucket-key-enabled`. Amazon S3 Bucket Keys può ridurre i costi delle AWS KMS richieste diminuendo il traffico di richieste da Amazon S3 a. AWS KMS Per ulteriori informazioni, consulta [Ridurre i costi SSE-KMS con Amazon S3 Bucket Keys](#).

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-side-encryption aws:kms --bucket-key-enabled --body filepath
```

È possibile crittografare un oggetto non crittografato SSE-KMS da utilizzare copiandolo nuovamente al suo posto.


```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --  
body filepath --bucket amzn-s3-demo-bucket --key example-object-key --sse aws:kms --  
sse-kms-key-id example-key-id --body filepath
```

Utilizzo di AWS SDK

Quando usi AWS gli SDK, puoi richiedere ad Amazon S3 di utilizzarlo per la crittografia lato server. AWS KMS keys Gli esempi seguenti mostrano come utilizzarli SSE-KMS con gli AWS SDK per Java e .NET. Per informazioni su altri SDK, vedi Codice e librerie [di](#) esempio nel AWS Developer Center.

Important

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetrica. Per ulteriori informazioni sulle chiavi, consulta [Chiavi KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Operazione CopyObject

Quando copi gli oggetti, puoi aggiungere le stesse proprietà della richiesta (ServerSideEncryptionMethod e ServerSideEncryptionKeyManagementServiceKeyId) per richiedere che Amazon S3 utilizzi una AWS KMS key. Per ulteriori informazioni sulla copia di oggetti, consulta la sezione [Copia, spostamento e denominazione di oggetti](#).

Operazione PUT

Java

Quando carichi un oggetto utilizzando AWS SDK per Java, puoi richiedere ad Amazon S3 di utilizzare un AWS KMS key aggiungendo la SSEAwsKeyManagementParams proprietà come mostrato nella seguente richiesta:

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,  
    keyName, file).withSSEAwsKeyManagementParams(new SSEAwsKeyManagementParams());
```

In questo caso, Amazon S3 utilizza (). Chiave gestita da AWS aws/s3 Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#). È possibile creare

facoltativamente una chiave KMS di crittografia simmetrica e specificarla nella richiesta, come mostrato nell'esempio seguente:

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
    keyName, file).withSSEAwsKeyManagementParams(new
    SSEAwsKeyManagementParams(keyID));
```

Per ulteriori informazioni sulla creazione di chiavi gestite dal cliente, consulta [Programming the AWS KMS API](#) nella AWS Key Management Service Developer Guide.

Per esempi di codice di utilizzo per il caricamento di un oggetto, consulta gli argomenti elencati di seguito. Per usare questi esempi dovrai aggiornare gli esempi di codice e fornire informazioni sulla crittografia come mostrato nel frammento di codice precedente.

- Per il caricamento di un oggetto in un'unica operazione, consulta [Caricamento degli oggetti](#).
- Per i caricamenti multiparte che utilizzano le operazioni API di caricamento multiparte di alto livello o di basso livello, consulta [Caricamento di un oggetto utilizzando il caricamento in più parti](#).

.NET

Quando carichi un oggetto utilizzando AWS SDK per .NET, puoi richiedere ad Amazon S3 di utilizzare un AWS KMS key aggiungendo la `ServerSideEncryptionMethod` proprietà come mostrato nella seguente richiesta:

```
PutObjectRequest putRequest = new PutObjectRequest
{
    BucketName = amzn-s3-demo-bucket,
    Key = keyName,
    // other properties
    ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS
};
```

In questo caso, Amazon S3 utilizza la chiave gestita da AWS. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#). È possibile creare una propria chiave di crittografia simmetrica gestita dal cliente e specificarla nella richiesta, come mostrato nell'esempio seguente:

```
PutObjectRequest putRequest1 = new PutObjectRequest
```

```
{  
    BucketName = amzn-s3-demo-bucket,  
    Key = keyName,  
    // other properties  
    ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS,  
    ServerSideEncryptionKeyManagementServiceKeyId = keyId  
};
```

Per ulteriori informazioni sulla creazione di chiavi gestite dal cliente, consulta [Programming the AWS KMS API](#) nella AWS Key Management Service Developer Guide.

Per esempi di codice di utilizzo per il caricamento di un oggetto, consulta gli argomenti elencati di seguito. Per usare questi esempi dovrai aggiornare gli esempi di codice e fornire informazioni sulla crittografia come mostrato nel frammento di codice precedente.

- Per il caricamento di un oggetto in un'unica operazione, consulta [Caricamento degli oggetti](#).
- Per i caricamenti multiparte che utilizzano le operazioni API di caricamento multiparte di alto livello o di basso livello, consulta [Caricamento di un oggetto utilizzando il caricamento in più parti](#).

URL prefirmati

Java

Quando si crea un URL prefirmato per un oggetto crittografato con AWS KMS key, è necessario specificare esplicitamente Signature Version 4, come mostrato nell'esempio seguente:

```
ClientConfiguration clientConfiguration = new ClientConfiguration();  
clientConfiguration.setSignerOverride("AWSS3V4SignerType");  
AmazonS3Client s3client = new AmazonS3Client(  
    new ProfileCredentialsProvider(), clientConfiguration);  
...
```

Per un esempio di codice, consulta [Condivisione di oggetti mediante URL prefirmati](#).

.NET

Quando si crea un URL prefirmato per un oggetto crittografato con AWS KMS key, è necessario specificare esplicitamente Signature Version 4, come mostrato nell'esempio seguente:

```
AWSConfigs.S3Config.UseSignatureVersion4 = true;
```

Per un esempio di codice, consulta [Condivisione di oggetti mediante URL prefirmati](#).

Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys

Amazon S3 Bucket Keys riduce il costo della crittografia lato server di Amazon S3 con () keys (). AWS Key Management Service AWS KMS SSE-KMS L'utilizzo di una chiave a livello di bucket per SSE-KMS può ridurre i costi delle AWS KMS richieste fino al 99% diminuendo il traffico di richieste da Amazon S3 a. AWS KMS Con pochi clic e senza alcuna modifica alle applicazioni client Console di gestione AWS, puoi configurare il bucket in modo che utilizzi una chiave bucket S3 per la crittografia su nuovi oggetti. SSE-KMS

Note

Le chiavi S3 Bucket non sono supportate per la crittografia lato server a doppio livello con chiavi () (). AWS Key Management Service AWS KMS DSSE-KMS

Chiavi S3 Bucket per SSE-KMS

I carichi di lavoro che accedono a milioni o miliardi di oggetti crittografati SSE-KMS possono generare grandi volumi di richieste verso. AWS KMS Quando lo usi SSE-KMS per proteggere i tuoi dati senza una chiave S3 Bucket, Amazon S3 utilizza una chiave AWS KMS [dati individuale per ogni oggetto](#). In questo caso, Amazon S3 effettua una chiamata AWS KMS ogni volta che viene effettuata una richiesta su un oggetto. KMS-encrypted Per informazioni su come SSE-KMS funziona, consulta [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#).

Quando configuri il bucket per utilizzare una chiave S3 Bucket per SSE-KMS, AWS genera una chiave a livello di bucket di breve durata da AWS KMS, quindi la mantiene temporaneamente in S3. Questa chiave a livello di bucket creerà chiavi di dati per i nuovi oggetti durante il relativo ciclo di vita. Le chiavi S3 Bucket vengono utilizzate per un periodo di tempo limitato in Amazon S3, riducendo la necessità per S3 di effettuare richieste per completare le operazioni di crittografia. AWS KMS Ciò riduce il traffico da S3 a AWS KMS, consentendoti di accedere a oggetti AWS KMS crittografati in Amazon S3 a una frazione del costo precedente.

Le chiavi univoche a livello di bucket vengono recuperate almeno una volta per richiedente per garantire che l'accesso del richiedente alla chiave venga acquisito in un evento. AWS KMS CloudTrail Amazon S3 considera i chiamanti come richiedenti diversi quando utilizzano ruoli o account diversi o lo stesso ruolo con politiche di ambito diverse. AWS KMS I risparmi sulle richieste

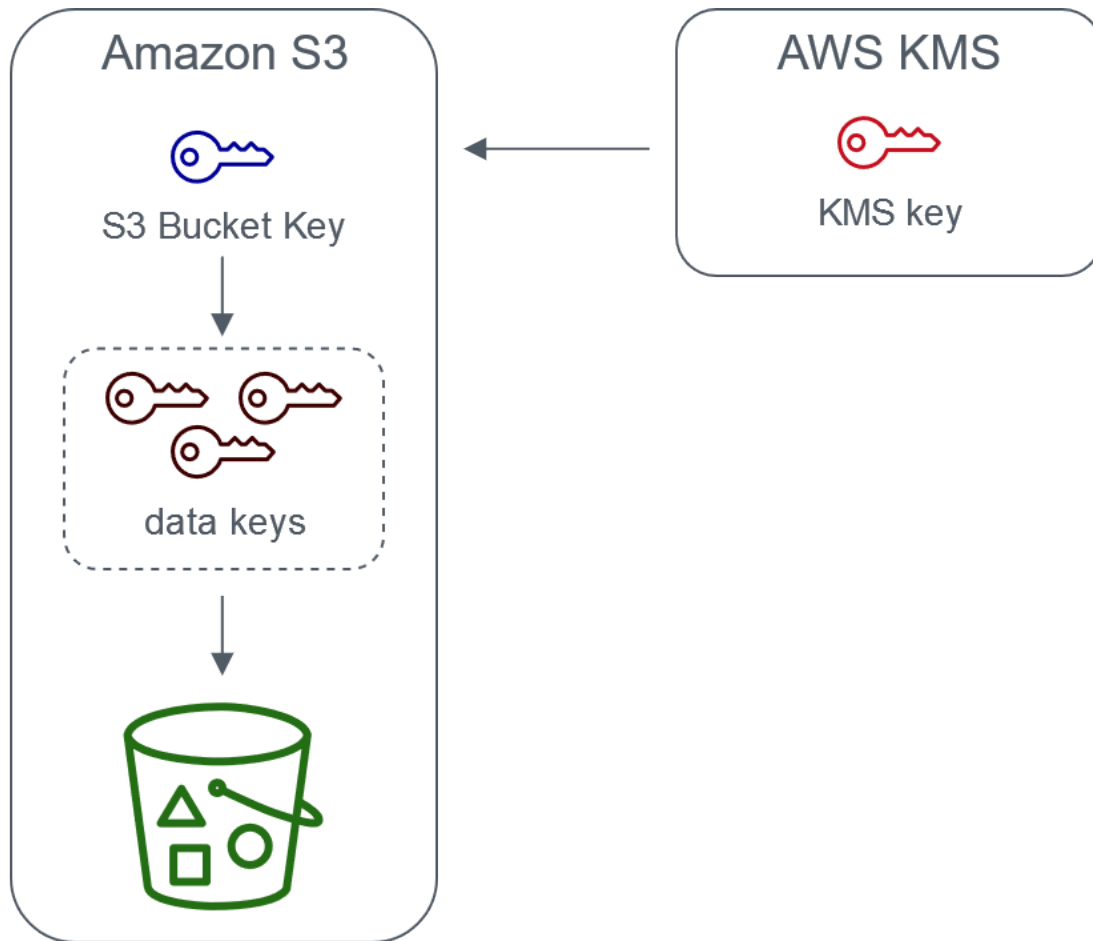
riflettono il numero di richiedenti, i modelli di richiesta e l'età relativa degli oggetti richiesti. Ad esempio, un numero inferiore di richiedenti, la richiesta di più oggetti in una finestra temporale limitata e la crittografia con la stessa chiave a livello di bucket comportano un risparmio maggiore.

Note

L'utilizzo di S3 Bucket Keys consente di risparmiare sui costi delle AWS KMS richieste riducendo le richieste a AWS KMS for Encrypt e le Decrypt operazioni tramite l'uso di una chiave a livello di bucket. GenerateDataKey In base alla progettazione, le richieste successive che sfruttano questa chiave a livello di bucket non generano richieste AWS KMS API né convalidano l'accesso in base alla policy chiave. AWS KMS

Quando si configura una chiave bucket S3, gli oggetti già presenti nel bucket non utilizzano la chiave Bucket S3. Per configurare una chiave bucket S3 per gli oggetti esistenti, è possibile utilizzare un'operazione CopyObject. Per ulteriori informazioni, consulta [Configurazione di una chiave bucket S3 a livello di oggetto](#).

Amazon S3 condividerà una chiave S3 bucket solo per gli oggetti crittografati dalla stessa AWS KMS key. Le chiavi S3 Bucket sono compatibili con le chiavi KMS create da AWS KMS, il materiale chiave [importato e il materiale chiave supportato da](#) archivi di [chiavi personalizzati](#).



Server-side encryption with AWS Key Management service using an S3 Bucket Key

Configurazione delle chiavi bucket S3

Puoi configurare il bucket per utilizzare una chiave S3 Bucket per SSE-KMS nuovi oggetti tramite la console Amazon S3, gli AWS SDK o l'API REST. AWS CLI Con le chiavi S3 Bucket abilitate sul bucket, gli oggetti caricati con una SSE-KMS chiave specificata diversa utilizzeranno le proprie chiavi S3 Bucket. Indipendentemente dall'impostazione della chiave di bucket S3, puoi includere l'intestazione `x-amz-server-side-encryption-bucket-key-enabled` con un valore `true` o `false` o nella richiesta, per sovrascrivere l'impostazione del bucket.

Prima di configurare il bucket per utilizzare una chiave bucket S3, consulta [Modifiche alla nota prima dell'abilitazione di una chiave bucket S3](#).

Configurazione di una chiave bucket S3 tramite la console di Amazon S3

Quando crei un nuovo bucket, puoi configurarlo in modo che utilizzi una chiave S3 Bucket per nuovi oggetti. SSE-KMS Puoi anche configurare un bucket esistente per utilizzare una chiave S3 Bucket SSE-KMS su nuovi oggetti aggiornando le proprietà del bucket.

Per ulteriori informazioni, consulta [Configurazione del bucket per l'utilizzo di una chiave S3 Bucket per i nuovi oggetti SSE-KMS](#).

API REST, AWS CLI e AWS Supporto SDK per S3 Bucket Keys

Puoi utilizzare l'API REST o AWS SDK per configurare il bucket in modo che utilizzi una chiave S3 Bucket per nuovi oggetti. AWS CLI SSE-KMS Puoi inoltre abilitare una chiave bucket S3 a livello di oggetto.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Configurazione di una chiave bucket S3 a livello di oggetto](#)
- [Configurazione del bucket per l'utilizzo di una chiave S3 Bucket per i nuovi oggetti SSE-KMS](#)

Le seguenti operazioni API supportano S3 Bucket Keys per: SSE-KMS

- [PutBucketEncryption](#)
 - `ServerSideEncryptionRule` accetta il parametro `BucketKeyEnabled` per abilitare e disabilitare una chiave bucket S3.
- [GetBucketEncryption](#)
 - `ServerSideEncryptionRule` restituisce le impostazioni per `BucketKeyEnabled`.
- [PutObject](#), [CopyObject](#), [CreateMultipartUpload](#), e POST Object <https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectPOST.html>
 - L'intestazione della richiesta `x-amz-server-side-encryption-bucket-key-enabled` abilita o disabilita una chiave bucket S3 a livello di oggetto.
- [HeadObject](#), [GetObject](#), [UploadPartCopy](#), [UploadPart](#), e [CompleteMultipartUpload](#)
 - L'intestazione della risposta `x-amz-server-side-encryption-bucket-key-enabled` indica se una chiave bucket S3 è abilitata o disabilitata per un oggetto.

Lavorare con CloudFormation

In CloudFormation, la `AWS::S3::Bucket` risorsa include una proprietà di crittografia denominata `BucketKeyEnabled` che puoi utilizzare per abilitare o disabilitare una chiave S3 Bucket.

Per ulteriori informazioni, consulta [Utilizzo CloudFormation](#).

Modifiche alla nota prima dell'abilitazione di una chiave bucket S3

Prima di abilitare una chiave bucket S3, tieni presente le seguenti modifiche correlate:

IAM o AWS KMS policy della chiave

Se le tue policy o policy AWS KMS chiave AWS Identity and Access Management (IAM) esistenti utilizzano il tuo oggetto Amazon Resource Name (ARN) come contesto di crittografia per perfezionare o limitare l'accesso alla tua chiave KMS, queste policy non funzioneranno con una chiave S3 Bucket. Le chiavi bucket S3 utilizzano l'ARN del bucket come contesto di crittografia. Prima di abilitare una chiave S3 Bucket, aggiorna le policy o le policy chiave IAM per utilizzare il bucket AWS KMS ARN come contesto di crittografia.

Per ulteriori informazioni sul contesto di crittografia e sulle chiavi bucket S3, consulta [Contesto di crittografia](#).

CloudTrail eventi per AWS KMS

Dopo aver abilitato una chiave S3 Bucket, AWS KMS CloudTrail gli eventi registrano l'ARN del bucket anziché l'ARN dell'oggetto. Inoltre, nei log vengono visualizzati meno CloudTrail eventi KMS per gli oggetti. SSE-KMS Poiché il materiale chiave è limitato nel tempo in Amazon S3, vengono effettuate meno richieste. AWS KMS

Utilizzo di una chiave bucket S3 con la replica

Puoi utilizzare S3 Bucket Keys with Same-Region Replication (SRR) and Replication (CRR). Cross-Region

Quando Amazon S3 replica un oggetto crittografato, in genere conserva le impostazioni di crittografia dell'oggetto di replica nel bucket di destinazione. Tuttavia, se l'oggetto di origine non è crittografato e il bucket di destinazione utilizza la crittografia predefinita o una chiave bucket S3, Amazon S3 crittografa l'oggetto con la configurazione del bucket di destinazione.

Negli esempi seguenti viene illustrato il funzionamento di una chiave bucket S3 con la replica. Per ulteriori informazioni, consulta [Replica di oggetti crittografati \(,,\) SSE-S3 SSE-KMS DSSE-KMS SSE-C](#).

Example Esempio 1: l'oggetto di origine utilizza le chiavi bucket S3 e il bucket di destinazione usa la crittografia predefinita

Se l'oggetto di origine utilizza una chiave bucket S3 ma il bucket di destinazione utilizza la crittografia predefinita con SSE-KMS, l'oggetto replica mantiene le impostazioni di crittografia S3 Bucket Key nel bucket di destinazione. Il bucket di destinazione utilizza ancora la crittografia predefinita con SSE-KMS

Example Esempio 2: l'oggetto sorgente non è crittografato; il bucket di destinazione utilizza una chiave bucket S3 con SSE-KMS

Se l'oggetto di origine non è crittografato e il bucket di destinazione utilizza una chiave S3 Bucket con SSE-KMS, l'oggetto di replica viene crittografato utilizzando una chiave S3 Bucket con nel bucket di destinazione. SSE-KMS Ciò fa sì che l'ETag dell'oggetto di origine sia diverso dall'ETag dell'oggetto replicato. È necessario aggiornare le applicazioni che utilizzano l'ETag per tenere conto di tale differenza.

Operazioni con le chiavi bucket S3

Per ulteriori informazioni sull'abilitazione e l'utilizzo di chiavi bucket S3, consulta le sezioni seguenti:

- [Configurazione del bucket per l'utilizzo di una chiave S3 Bucket per i nuovi oggetti SSE-KMS](#)
- [Configurazione di una chiave bucket S3 a livello di oggetto](#)
- [Visualizzazione delle impostazioni per una chiave bucket S3](#)

Configurazione del bucket per l'utilizzo di una chiave S3 Bucket per i nuovi oggetti SSE-KMS

Quando configuri la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS), puoi configurare il bucket in modo che utilizzi una chiave bucket S3 per i nuovi oggetti. SSE-KMS Le chiavi S3 Bucket riducono il traffico di richieste da Amazon S3 e riducono il costo di. AWS KMS SSE-KMS Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

Puoi configurare il bucket per utilizzare una chiave S3 Bucket per SSE-KMS nuovi oggetti utilizzando la console Amazon S3, l'API REST, gli SDK, () o. AWS AWS Command Line Interface AWS CLI CloudFormation Se desideri abilitare o disabilitare una chiave bucket S3 per gli oggetti esistenti, puoi utilizzare un'operazione CopyObject. Per ulteriori informazioni, consulta [Configurazione di una chiave bucket S3 a livello di oggetto](#) e [Utilizzo di Batch Operations per abilitare S3 Bucket Keys per SSE-KMS](#).

Quando una chiave bucket S3 è abilitata per il bucket di origine o di destinazione, il contesto di crittografia sarà l'Amazon Resource Name (ARN) del bucket e non l'ARN dell'oggetto, ad esempio, `arn:aws:s3:::bucket_ARN`. Dovrai aggiornare le policy IAM per utilizzare l'ARN del bucket per il contesto di crittografia. Per ulteriori informazioni, consulta [Chiavi bucket S3 e replica](#).

Negli esempi seguenti viene illustrato il funzionamento di una chiave bucket S3 con la replica. Per ulteriori informazioni, consulta [Replica di oggetti crittografati \(,,,\) SSE-S3 SSE-KMS DSSE-KMS SSE-C](#).

Prerequisiti

Prima di configurare il bucket per utilizzare una chiave bucket S3, consulta [Modifiche alla nota prima dell'abilitazione di una chiave bucket S3](#).

Utilizzo della console S3

Nella console S3, puoi abilitare o disabilitare una chiave bucket S3 per un bucket nuovo o esistente. Gli oggetti nella console S3 ereditano l'impostazione della chiave bucket S3 dalla configurazione del bucket. Quando abiliti una chiave S3 Bucket per il tuo bucket, i nuovi oggetti che carichi nel bucket utilizzano una chiave S3 Bucket per. SSE-KMS

Caricamento, copia o modifica di oggetti nei bucket che dispongono di una chiave bucket S3 abilitata

Se carichi, modifichi o copi un oggetto in un bucket con una chiave bucket S3 abilitata, le impostazioni della chiave bucket S3 per tale oggetto potrebbero essere aggiornate in modo da allinearsi alla configurazione del bucket.

Se un oggetto ha già una chiave bucket S3 abilitata, le impostazioni della chiave bucket S3 per quell'oggetto non cambiano quando si copia o si modifica l'oggetto. Tuttavia, se modifichi o copi un oggetto che non dispone di una chiave bucket S3 attivata e il bucket di destinazione ha una configurazione con una chiave bucket S3, l'oggetto eredita le impostazioni della chiave bucket S3 del bucket di destinazione. Ad esempio, se l'oggetto di origine non ha una chiave bucket S3 abilitata ma il bucket di destinazione ne ha una, una chiave bucket S3 è abilitata per l'oggetto.

Abilitazione di una chiave bucket S3 quando si crea un nuovo bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Seleziona Crea bucket.

4. Inserisci il nome del bucket e scegli la tua Regione AWS.
5. In Crittografia predefinita, per Tipo di chiave di crittografia, scegli AWS Key Management Service key (SSE-KMS).
6. In AWS KMS key, esegui una delle seguenti operazioni per scegliere la chiave KMS:
 - Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS keys, quindi scegli la tua chiave KMS dall'elenco delle chiavi disponibili.

Sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente vengono visualizzate in questo elenco. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta Chiavi e AWS chiavi del [cliente](#) nella Guida per gli AWS Key Management Service sviluppatori.

- Per specificare l'ARN della chiave KMS, scegli Inserisci l'ARN della AWS KMS key e quindi specifica l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creating Keys](#) nella AWS Key Management Service Developer Guide.

7. In Chiave bucket scegli Abilita.
8. Scegliere Create bucket (Crea bucket).

Amazon S3 crea il tuo bucket con una chiave bucket S3 abilitata. I nuovi oggetti caricati nel bucket utilizzeranno una chiave bucket S3.

Per disabilitare una chiave bucket S3, completa i passaggi precedenti e scegli Disabilita.

Abilitazione di una chiave bucket S3 per un bucket esistente

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il bucket per cui desideri abilitare una chiave bucket S3.
4. Scegliere la scheda Properties (Proprietà).
5. In Default encryption (Crittografia di default), scegliere Edit (Modifica).
6. In Crittografia predefinita, per Tipo di chiave di crittografia, scegli AWS Key Management Service key (SSE-KMS).

7. In AWS KMS key, esegui una delle seguenti operazioni per scegliere la chiave KMS:

- Per scegliere da un elenco di chiavi KMS disponibili, scegli **Scegli tra le tue AWS KMS keys**, quindi scegli la tua chiave KMS dall'elenco delle chiavi disponibili.

Sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente vengono visualizzate in questo elenco. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta **Chiavi e AWS chiavi del [cliente](#)** nella Guida per gli AWS Key Management Service sviluppatori.

- Per specificare l'ARN della chiave KMS, scegli **Inserisci l'ARN della AWS KMS key** e quindi specifica l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli **Crea una chiave KMS**.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creating Keys](#) nella AWS Key Management Service Developer Guide.

8. In Chiave bucket scegli **Abilita**.

9. Seleziona **Salva modifiche**.

Amazon S3 abilita una chiave bucket S3 per i nuovi oggetti aggiunti al tuo bucket. Gli oggetti esistenti non utilizzano la chiave bucket S3. Per configurare una chiave bucket S3 per gli oggetti esistenti, è possibile utilizzare un'operazione CopyObject. Per ulteriori informazioni, consulta [Configurazione di una chiave bucket S3 a livello di oggetto](#).

Per disabilitare una chiave bucket S3, completa i passaggi precedenti e scegli **Disabilita**.

Utilizzo dell'API REST

Puoi usarla [PutBucketEncryption](#) per abilitare o disabilitare una chiave S3 Bucket per il tuo bucket. Per configurare una chiave S3 Bucket conPutBucketEncryption, utilizza il tipo di [ServerSideEncryptionRule](#) dati, che include la crittografia predefinita con. SSE-KMS Puoi inoltre utilizzare una chiave gestita dal cliente specificando l'ID della chiave KMS per la chiave gestita dal cliente.

Per ulteriori informazioni ed esempi di sintassi, vedere. [PutBucketEncryption](#)

Utilizzo di AWS SDK per Java

L'esempio seguente abilita la crittografia del bucket predefinita con SSE-KMS una chiave bucket S3 utilizzando il. AWS SDK per Java

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

ServerSideEncryptionByDefault serverSideEncryptionByDefault = new
    ServerSideEncryptionByDefault()
    .withSSEAlgorithm(SSEAlgorithm.KMS);
ServerSideEncryptionRule rule = new ServerSideEncryptionRule()
    .withApplyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
    .withBucketKeyEnabled(true);
ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
    new ServerSideEncryptionConfiguration().withRules(Collections.singleton(rule));

SetBucketEncryptionRequest setBucketEncryptionRequest = new
    SetBucketEncryptionRequest()
    .withServerSideEncryptionConfiguration(serverSideEncryptionConfiguration)
    .withBucketName(bucketName);

s3client.setBucketEncryption(setBucketEncryptionRequest);
```

Utilizzo di AWS CLI

L'esempio seguente abilita la crittografia del bucket predefinita con SSE-KMS una chiave bucket S3 utilizzando il. AWS CLI Sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-configuration '{
    "Rules": [
        {
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "aws:kms",
                "KMSMasterKeyID": "KMS-Key-ARN"
            },
            "BucketKeyEnabled": true
        }
    ]
}
```

```
} ' ]
```

Utilizzo CloudFormation

Per ulteriori informazioni sulla configurazione di una chiave S3 Bucket con CloudFormation, consulta [AWS: :S3: :Bucket nella Guida per l'utente. ServerSideEncryptionRule](#) AWS CloudFormation

Configurazione di una chiave bucket S3 a livello di oggetto

Quando esegui un'operazione PUT o COPY utilizzando l'API REST, AWS gli SDK o AWS CLI, puoi abilitare o disabilitare una chiave S3 Bucket a livello di oggetto aggiungendo l'intestazione della `x-amz-server-side-encryption-bucket-key-enabled` richiesta con un valore `or. true false`. Le chiavi S3 Bucket riducono il costo della crittografia lato server utilizzando AWS Key Management Service (AWS KMS) (SSE-KMS) diminuendo il traffico di richieste da Amazon S3 a. AWS KMS Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

Quando configuri una chiave bucket S3 per un oggetto utilizzando un'operazione PUT o COPY, Amazon S3 aggiorna le impostazioni solo per quell'oggetto. Le impostazioni della chiave bucket S3 per il bucket di destinazione non cambiano. Se invii una richiesta PUT o COPY per un KMS-encrypted oggetto in un bucket con S3 Bucket Keys abilitate, l'operazione a livello di oggetto utilizzerà automaticamente le chiavi S3 Bucket Keys a meno che non disabiliti le chiavi nell'intestazione della richiesta. Se non specifichi una chiave bucket S3 per il tuo oggetto, Amazon S3 applica le impostazioni della chiave bucket S3 per il bucket di destinazione all'oggetto.

Prerequisito

Prima di configurare l'oggetto per utilizzare una chiave bucket S3, consulta [Modifiche alla nota prima dell'abilitazione di una chiave bucket S3](#).

Argomenti

- [Operazioni in Batch Amazon S3](#)
- [Utilizzo della REST API](#)
- [Utilizzo di AWS SDK per Java \(\) PutObject](#)
- [Utilizzo di AWS CLI \(PutObject\)](#)

Operazioni in Batch Amazon S3

Per crittografare gli oggetti Amazon S3 esistenti, puoi utilizzare le operazioni in batch di Amazon S3. Fornisci alle operazioni in batch S3 un elenco di oggetti da utilizzare e le operazioni in batch chiamano la rispettiva API per eseguire l'operazione specifica.

Puoi utilizzare l'operazione di [copia delle operazioni in batch S3](#) per copiare gli oggetti non crittografati esistenti e scriverli nello stesso bucket degli oggetti crittografati. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch](#) e [Crittografia di oggetti con le operazioni in batch di Amazon S3](#).

Utilizzo della REST API

Quando si utilizza SSE-KMS, è possibile abilitare una chiave S3 Bucket per un oggetto utilizzando le seguenti operazioni API:

- [PutObject](#)— Quando carichi un oggetto, puoi specificare l'intestazione della `x-amz-server-side-encryption-bucket-key-enabled` richiesta per abilitare o disabilitare una chiave S3 Bucket a livello di oggetto.
- [CopyObject](#)— Quando copi un oggetto e lo configuri SSE-KMS, puoi specificare l'intestazione della `x-amz-server-side-encryption-bucket-key-enabled` richiesta per abilitare o disabilitare una chiave S3 Bucket per il tuo oggetto.
- [Oggetto POST](#): quando si utilizza un'POSToperazione per caricare un oggetto e configurarlo SSE-KMS, è possibile utilizzare il campo del `x-amz-server-side-encryption-bucket-key-enabled` modulo per abilitare o disabilitare una chiave S3 Bucket per l'oggetto.
- [CreateMultipartUpload](#)— Quando carichi oggetti di grandi dimensioni utilizzando l'operazione e la configurazione `CreateMultipartUpload` API SSE-KMS, puoi utilizzare l'intestazione della `x-amz-server-side-encryption-bucket-key-enabled` richiesta per abilitare o disabilitare una chiave S3 Bucket per il tuo oggetto.

Per abilitare una chiave bucket S3 a livello di oggetto, dovrai includere l'intestazione della richiesta `x-amz-server-side-encryption-bucket-key-enabled`. Per ulteriori informazioni sull'API REST SSE-KMS e sull'API REST, consulta. [Utilizzo della REST API](#)

Utilizzo di AWS SDK per Java () PutObject

Il seguente esempio può essere utilizzato per configurare una chiave bucket S3 a livello di oggetto utilizzando AWS SDK per Java.

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

String bucketName = "amzn-s3-demo-bucket1";
String keyName = "key name for object";
String contents = "file contents";

PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName, keyName,
    contents)
    .withBucketKeyEnabled(true);

s3client.putObject(putObjectRequest);
```

Utilizzo di AWS CLI (PutObject)

È possibile utilizzare l' AWS CLI esempio seguente per configurare una chiave S3 Bucket a livello di oggetto come parte di una richiesta. PutObject

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object key name --server-side-
encryption aws:kms --bucket-key-enabled --body filepath
```

Visualizzazione delle impostazioni per una chiave bucket S3

Puoi visualizzare le impostazioni per una chiave S3 Bucket a livello di bucket o oggetto utilizzando la console Amazon S3, l'API REST, AWS Command Line Interface () o gli SDK.AWS CLI AWS

Le chiavi S3 Bucket riducono il traffico di richieste da Amazon S3 AWS KMS e riducono il costo della crittografia lato server utilizzando (). AWS Key Management Service SSE-KMS Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).

Per visualizzare le impostazioni della chiave bucket S3 per un bucket o un oggetto che ha ereditato le impostazioni della chiave bucket S3 dalla configurazione del bucket, è necessaria l'autorizzazione per eseguire l'operazione s3:GetEncryptionConfiguration. Per ulteriori informazioni, consulta [GetBucketEncryption](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo della console S3

Nella console S3, puoi visualizzare le impostazioni della chiave bucket S3 per il bucket o l'oggetto. Le impostazioni della chiave bucket S3 vengono ereditate dalla configurazione del bucket a meno che gli oggetti di origine non dispongano già di una chiave bucket S3 configurata.

Oggetti e cartelle nello stesso bucket possono avere diverse impostazioni della chiave bucket S3. Ad esempio, se carichi un oggetto utilizzando REST API e abiliti una chiave bucket S3 per tale oggetto, questo manterrà l'impostazione della chiave bucket S3 nel bucket di destinazione anche se la chiave bucket S3 è disabilitata. Come altro esempio, se abiliti una chiave bucket S3 per un bucket esistente, gli oggetti già presenti nel bucket non utilizzeranno una chiave bucket S3. Tuttavia, i nuovi oggetti avranno una chiave bucket S3 abilitata.

Visualizzazione dell'impostazione della chiave bucket S3 per il bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il bucket per cui desideri abilitare una chiave bucket S3.
4. Scegliere Properties (Proprietà).
5. Nella sezione Crittografia predefinita, in Chiave bucket, viene visualizzata l'impostazione della chiave bucket S3 per il bucket.

Se non riesci a visualizzare l'impostazione della chiave bucket S3, è possibile che non disponi dell'autorizzazione per eseguire l'operazione `s3:GetEncryptionConfiguration`. Per ulteriori informazioni, consulta [GetBucketEncryption](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Visualizzazione dell'impostazione della chiave bucket S3 per l'oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket scegli il bucket per cui desideri abilitare una chiave bucket S3.
3. Nell'elenco Oggetti scegli il nome dell'oggetto.
4. Nella scheda Dettagli, nelle impostazioni di Server-side crittografia, scegli Modifica.

In Chiave bucket è visualizzata l'impostazione della chiave bucket S3 per l'oggetto. Non è possibile modificare questa impostazione.

Utilizzo di AWS CLI

Restituzione delle impostazioni della chiave bucket S3 a livello di bucket

Per usare questo comando, sostituire *user input placeholder* con le proprie informazioni.

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

Per ulteriori informazioni, consulta [get-bucket-encryption](#) nella Guida di riferimento dei comandi della AWS CLI .

Restituzione delle impostazioni a livello di oggetto di una chiave bucket S3

Per usare questo comando, sostituire *user input placeholder* con le proprie informazioni.

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key my_images.tar.bz2
```

Per ulteriori informazioni, consulta [head-object](#) in Guida di riferimento dei comandi di AWS CLI .

Utilizzo della REST API

Restituzione delle impostazioni della chiave bucket S3 a livello di bucket

Per restituire le informazioni di crittografia per un bucket, incluse le impostazioni per una chiave bucket S3, utilizza l'operazione `GetBucketEncryption`. Le impostazioni della chiave bucket S3 vengono restituite nel corpo della risposta nell'elemento `ServerSideEncryptionConfiguration` con l'impostazione `BucketKeyEnabled`. Per ulteriori informazioni, consulta [GetBucketEncryption](#) nella documentazione di riferimento delle API di Amazon S3.

Restituzione delle impostazioni a livello di oggetto per una chiave bucket S3

Per restituire lo stato della chiave bucket S3 per un oggetto, utilizza l'operazione `HeadObject`. `HeadObject` restituisce l'intestazione della risposta `x-amz-server-side-encryption-bucket-key-enabled` per mostrare se una chiave bucket S3 è abilitata o disabilitata per l'oggetto. Per ulteriori informazioni, consulta [HeadObject](#) nella documentazione di riferimento delle API di Amazon S3.

Le seguenti operazioni delle API restituiscono l'intestazione della risposta `x-amz-server-side-encryption-bucket-key-enabled` anche se una chiave bucket S3 è configurata per un oggetto:

- [PutObject](#)
- [PostObject](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [UploadPartCopy](#)
- [UploadPart](#)
- [CompleteMultipartUpload](#)
- [GetObject](#)

Utilizzo della crittografia lato server a doppio livello con AWS KMS chiavi DSSE-KMS ()

L'utilizzo della crittografia lato server a doppio livello con AWS Key Management Service (AWS KMS) keys (DSSE-KMS) applica due livelli di crittografia agli oggetti quando vengono caricati su Amazon S3. DSSE-KMS ti aiuta a soddisfare più facilmente gli standard di conformità che richiedono di applicare la crittografia multistrato ai tuoi dati e di avere il pieno controllo delle tue chiavi di crittografia.

Il «doppio» in DSSE-KMS si riferisce a due livelli indipendenti di AES-256 crittografia applicati ai dati:

- Primo livello: i dati vengono crittografati utilizzando una chiave di crittografia dei dati univoca (DEK) generata da AWS KMS
- Secondo livello: i dati già crittografati vengono nuovamente crittografati utilizzando una chiave di AES-256 crittografia separata gestita da Amazon S3

Questo è diverso dallo standard SSE-KMS, che applica solo un singolo livello di crittografia.

L'approccio a doppio livello offre una maggiore sicurezza garantendo che, anche se un livello di crittografia fosse compromesso, i dati rimangano protetti dal secondo livello. Questa sicurezza aggiuntiva comporta un aumento del sovraccarico di elaborazione e delle chiamate AWS KMS API, il che rappresenta il costo più elevato rispetto allo standard. SSE-KMS Per ulteriori informazioni sui DSSE-KMS prezzi, consulta [AWS KMS key i concetti e i AWS KMS prezzi](#) nella Guida per AWS Key Management Service gli sviluppatori.

Quando si utilizza DSSE-KMS con un bucket Amazon S3, le AWS KMS chiavi devono trovarsi nella stessa regione del bucket. Inoltre, quando DSSE-KMS viene richiesto l'oggetto, il checksum S3 che

fa parte dei metadati dell'oggetto viene archiviato in forma crittografata. Per ulteriori informazioni sui checksum, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Note

Le chiavi S3 Bucket non sono supportate per. DSSE-KMS

Le principali differenze tra DSSE-KMS e standard sono: SSE-KMS

- **Livelli di crittografia:** DSSE-KMS applica due livelli di AES-256 crittografia indipendenti, mentre lo standard SSE-KMS applica un livello
- **Sicurezza:** DSSE-KMS fornisce una protezione avanzata contro potenziali vulnerabilità di crittografia
- **Conformità:** DSSE-KMS aiuta a soddisfare i requisiti normativi che impongono la crittografia multistrato
- **Prestazioni:** DSSE-KMS ha una latenza leggermente superiore a causa dell'ulteriore elaborazione della crittografia
- **Costo:** DSSE-KMS comporta costi più elevati a causa dell'aumento del sovraccarico di calcolo e delle operazioni aggiuntive AWS KMS

Richiede una crittografia lato server a doppio livello con AWS KMS keys (DSSE-KMS)

Per richiedere la crittografia lato server a doppio livello di tutti gli oggetti in uno specifico bucket Amazon S3, è possibile utilizzare una policy del bucket. Ad esempio, la seguente policy del bucket nega l'autorizzazione di upload object (`s3:PutObject`) a tutti se la richiesta non include un'`x-amz-server-side-encryption` intestazione che richiede la crittografia lato server con. DSSE-KMS

JSON

```
{
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [{
        "Sid": "DenyUnEncryptedObjectUploads",
        "Effect": "Deny",
        "Principal": {
```

```
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "StringNotEquals": {
            "s3:x-amz-server-side-encryption": "aws:kms:dsse"
        }
    }
}
```

Argomenti

- [Specificare la crittografia lato server a doppio livello con AWS KMS chiavi DSSE-KMS \(\)](#)

Specificare la crittografia lato server a doppio livello con AWS KMS chiavi DSSE-KMS ()

È possibile applicare la crittografia quando stai caricando un nuovo oggetto o copiando un oggetto esistente.

È possibile specificare DSSE-KMS utilizzando la console Amazon S3, l'API REST di Amazon S3 e (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta i seguenti argomenti.

Note

Puoi usare Multi-region AWS KMS keys in Amazon S3. Tuttavia, Amazon S3 attualmente tratta le chiavi multiregionali come se fossero chiavi monoregionali e non utilizza le caratteristiche multiregionali della chiave. Per ulteriori informazioni, consulta [Utilizzo delle chiavi multiregione](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Note

Se desideri utilizzare una chiave KMS di proprietà di un account diverso, devi avere l'autorizzazione necessaria per l'uso della chiave. Per ulteriori informazioni sulle autorizzazioni tra account per le chiavi KMS, vedi [Creazione di chiavi KMS utilizzabili da altri account](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Utilizzo della console S3

Questa sezione descrive come impostare o modificare il tipo di crittografia di un oggetto per utilizzare la crittografia lato server a doppio livello con AWS Key Management Service (AWS KMS) keys (DSSE-KMS) utilizzando la console Amazon S3.

Note

- È possibile modificare la crittografia di un oggetto se l'oggetto è inferiore a 5 GB. Se l'oggetto è superiore a 5 GB, è necessario utilizzare gli SDK [AWS CLI](#) o [AWS per modificare la crittografia di un oggetto](#).
- Per un elenco delle autorizzazioni aggiuntive necessarie per modificare la crittografia di un oggetto, consulta [the section called “Autorizzazioni necessarie per le operazioni API S3”](#). Per esempi di policy che concedono questa autorizzazione, consulta [the section called “Identity-based esempi di policy”](#).
- Se si modifica la crittografia di un oggetto, viene creato un nuovo oggetto per sostituire quello precedente. Se è abilitata la funzione Controllo delle versioni S3, viene creata una nuova versione dell'oggetto e l'oggetto esistente diventa una versione precedente. Il ruolo che modifica la proprietà diventa anche il proprietario del nuovo oggetto o della versione dell'oggetto.

Per aggiungere o modificare la crittografia di un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Bucket, quindi scegli la scheda Bucket per uso generico. Naviga al bucket o alla cartella Amazon S3 che contiene gli oggetti da modificare.
3. Seleziona la casella di controllo degli oggetti da modificare.
4. Nel menu Azioni, scegli Modifica crittografia lato server dall'elenco di opzioni visualizzato.
5. Scorri fino alla sezione Server-side di crittografia.
6. In Impostazioni di crittografia, scegli Utilizza le impostazioni del bucket per la crittografia predefinita o Ignora le impostazioni del bucket per la crittografia predefinita.
7. Se scegli Sostituisci impostazioni del bucket per la crittografia predefinita, configura le seguenti impostazioni di crittografia.

- a. In Tipo di crittografia, scegli la Dual-layer crittografia lato server con AWS Key Management Service chiavi (DSSE-KMS).
- b. In AWS KMS key, esegui una delle seguenti operazioni per scegliere la chiave KMS:
 - Per scegliere da un elenco di chiavi KMS disponibili, seleziona Scegli tra le chiavi AWS KMS keys, quindi scegli la chiave KMS dall'elenco delle chiavi disponibili.

In questo elenco vengono visualizzate sia le chiavi Chiave gestita da AWS (aws/s3) che quelle gestite dal cliente. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per inserire l'ARN della chiave KMS, scegli Inserisci AWS KMS key ARN, quindi inserisci l'ARN della chiave KMS nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

 Important

Puoi utilizzare solo le chiavi KMS disponibili nella stessa Regione AWS del bucket. La console Amazon S3 elenca solo le prime 100 chiavi KMS nella stessa Regione del bucket. Per utilizzare una chiave KMS non elencata, devi inserire l'ARN della chiave KMS. Se desideri utilizzare una chiave KMS di proprietà di un account diverso, è necessario innanzitutto disporre dell'autorizzazione necessaria per l'uso della chiave e quindi inserire l'ARN della chiave KMS.

Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

8. Per Chiave bucket scegli Disabilita. Le chiavi S3 Bucket non sono supportate per DSSE-KMS
9. In Impostazioni di copia aggiuntive, scegli se eseguire Copia impostazioni dell'origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni dell'origine, scegli Non specificare le impostazioni. Scegli Specifica le impostazioni per specificare le

impostazioni per la classe di storage, le ACL, i tag degli oggetti, i metadati, la crittografia lato server e i checksum aggiuntivi.

10. Scegli Save changes (Salva modifiche).

Note

Questa azione applica la crittografia a tutti gli oggetti specificati. Durante la crittografia delle cartelle, attendere il completamento dell'operazione di salvataggio prima di aggiungere nuovi oggetti alla cartella.

Utilizzo della REST API

Quando crei un oggetto, ovvero quando carichi un nuovo oggetto o copi un oggetto esistente, puoi specificare l'uso della crittografia lato server a doppio livello con () per crittografare i tuoi dati. AWS KMS keys DSSE-KMS Per fare ciò, aggiungi l'intestazione `x-amz-server-side-encryption` alla richiesta. Impostare il valore dell'intestazione sull'algoritmo di crittografia `aws:kms:dsse`. Amazon S3 conferma che l'oggetto è archiviato con crittografia restituendo l'intestazione della risposta. DSSE-KMS `x-amz-server-side-encryption`

Se specifichi l'intestazione `x-amz-server-side-encryption` con il valore `aws:kms:dsse`, puoi anche utilizzare le intestazioni di richiesta seguenti:

- `x-amz-server-side-encryption-aws-kms-key-id`: *SSEKMSKeyId*
- `x-amz-server-side-encryption-context`: *SSEKMSEncryptionContext*

Argomenti

- [Operazioni API REST di Amazon S3 che supportano DSSE-KMS](#)
- [Contesto di crittografia \(x-amz-server-side-encryption-context\)](#)
- [AWS KMS ID della chiave \(x-amz-server-side-encryption-aws-kms-key-id\)](#)

Operazioni API REST di Amazon S3 che supportano DSSE-KMS

Le operazioni REST API seguenti accettano le intestazioni di richiesta `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id` e `x-amz-server-side-encryption-context`.

- [PutObject](#): quando carichi i dati utilizzando l'operazione API PUT, è possibile specificare queste intestazioni di richiesta.
- [CopyObject](#) - Quando si copia un oggetto, si ha un oggetto di origine e un oggetto di destinazione. Quando si trasmettono le DSSE-KMS intestazioni con l'CopyObject operazione, queste vengono applicate solo all'oggetto di destinazione. Quando si copia un oggetto esistente, indipendentemente dal fatto che l'oggetto di origine sia stato o meno crittografato, l'oggetto di destinazione non viene crittografato, a meno che non si richieda esplicitamente la crittografia lato server.
- [POST Object](#): quando utilizzi un'operazione POST per caricare un oggetto, anziché le intestazioni di richiesta, specifica le stesse informazioni dei campi del modulo.
- [CreateMultipartUpload](#): quando carichi oggetti di grandi dimensioni utilizzando il caricamento in più parti, puoi specificare queste intestazioni nella richiesta CreateMultipartUpload.

Quando un oggetto viene archiviato con la crittografia lato server, le intestazioni di risposta delle seguenti operazioni REST API restituiscono l'intestazione `x-amz-server-side-encryption`.

- [PutObject](#)
- [CopyObject](#)
- [POST Object](#)
- [CreateMultipartUpload](#)
- [UploadPart](#)
- [UploadPartCopy](#)
- [CompleteMultipartUpload](#)
- [GetObject](#)
- [HeadObject](#)

 Important

- Tutte GET le PUT richieste relative a un oggetto protetto hanno AWS KMS esito negativo se non vengono effettuate utilizzando Secure Sockets Layer (SSL), Transport Layer Security (TLS) o Signature Version 4.
- Se il tuo oggetto utilizza DSSE-KMS, non inviare intestazioni di richiesta di crittografia per GET richieste e HEAD richieste, altrimenti riceverai un errore HTTP 400 (Bad Request).

Contesto di crittografia (x-amz-server-side-encryption-context)

Se si specifica `x-amz-server-side-encryption:aws:kms:dsse`, l'API Amazon S3 supporta un contesto di crittografia con l'intestazione `x-amz-server-side-encryption-context`. Un contesto di crittografia è un set di coppie chiave-valore che possono contenere ulteriori informazioni contestuali sui dati.

Amazon S3 utilizza automaticamente il nome della risorsa Amazon (ARN) dell'oggetto come coppia di contesto di crittografia; ad esempio, `arn:aws:s3:::object_ARN`.

Facoltativamente, è possibile fornire una coppia di contesto di crittografia aggiuntiva utilizzando l'intestazione `x-amz-server-side-encryption-context`. Tuttavia, poiché il contesto di crittografia non è crittografato, assicurati che non includa informazioni sensibili. Amazon S3 archivia questa coppia di chiavi aggiuntiva insieme al contesto di crittografia predefinito.

Per informazioni sul contesto di crittografia in Amazon S3, consulta la sezione [Contesto di crittografia](#). Per informazioni generali sul contesto di crittografia, consulta [Concetti di AWS Key Management Service : Contesto di crittografia](#) nella Guida per gli sviluppatori di AWS Key Management Service .

AWS KMS ID della chiave (x-amz-server-side-encryption-aws-kms-key-id)

Puoi utilizzare l'intestazione `x-amz-server-side-encryption-aws-kms-key-id` per specificare l'ID della chiave gestita dal cliente utilizzata per proteggere i dati. Se specifichi l'`x-amz-server-side-encryption:aws:kms:dsse` intestazione ma non la fornisci, Amazon S3 utilizza () per proteggere i dati. `x-amz-server-side-encryption-aws-kms-key-id` Chiave gestita da AWS `aws/s3` Se desideri utilizzare una chiave gestita dal cliente, devi fornire l'intestazione `x-amz-server-side-encryption-aws-kms-key-id` della chiave gestita dal cliente.

Important

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetrica. Per ulteriori informazioni sulle chiavi, consulta [Chiavi KMS di crittografia simmetrica](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Utilizzo di AWS CLI

Quando carichi un nuovo oggetto o copi un oggetto esistente, puoi specificarne l'uso per crittografare i dati. DSSE-KMS Per farlo, aggiungi il parametro `--server-side-encryption aws:kms:dsse`

alla richiesta. Usa il parametro `--ssekms-key-id` *example-key-id* per aggiungere la [chiave AWS KMS gestita dal cliente](#) che hai creato. Se specifichi `--server-side-encryption` `aws:kms:dsse`, ma non fornisci un ID AWS KMS chiave, Amazon S3 utilizzerà la chiave AWS gestita (`aws/s3`).

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-side-encryption aws:kms:dsse --ssekms-key-id example-key-id --body filepath
```

È possibile crittografare un oggetto non crittografato DSSE-KMS da utilizzare copiandolo nuovamente al suo posto.

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --copy-source amzn-s3-demo-bucket/example-object-key --server-side-encryption aws:kms:dsse --ssekms-key-id example-key-id
```

Utilizzo della crittografia lato server con chiavi fornite dal cliente () SSE-C

Server-side la crittografia riguarda la protezione dei dati inattivi. Server-side la crittografia crittografa solo i dati dell'oggetto, non i metadati dell'oggetto. È possibile utilizzare la crittografia lato server con chiavi fornite dal cliente (SSE-C) nei bucket generici per crittografare i dati con le proprie chiavi di crittografia. Con la chiave di crittografia fornita come parte della richiesta, Amazon S3 gestisce la crittografia dei dati durante le operazioni di scrittura su disco e decrittografia dei dati quando viene eseguito l'accesso agli oggetti. Pertanto, non è necessario mantenere alcun codice per effettuare la crittografia e la decrittografia dei dati. L'unica cosa che rimane da fare è gestire le chiavi di crittografia fornite.

A partire da aprile 2026, SSE-C è disabilitata per impostazione predefinita per tutti i nuovi bucket generici e per i bucket esistenti negli account senza oggetti crittografati. SSE-C La maggior parte dei carichi di lavoro moderni utilizza invece la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) o chiavi AWS KMS (SSE-KMS), perché SSE-C richiede di fornire la chiave di crittografia con ogni richiesta, rendendo poco pratico condividere l'accesso con altri utenti, ruoli o servizi che operano sui tuoi dati. AWS Per saperne di più, consulta. SSE-KMS [the section called “chiavi KMS memorizzate in AWS KMS \(\) SSE-KMS”](#)

Se il carico di lavoro lo richiede SSE-C, devi abilitarlo esplicitamente impostandolo `NONE` nella configurazione `BlockedEncryptionTypes` di crittografia predefinita del bucket utilizzando l'API. `PutBucketEncryption` Se SSE-C è bloccato `PutObject` `CopyObject` `PostObject`, qualsiasi richiesta di replica o caricamento in più parti che specifichi la SSE-C crittografia viene rifiutata con

un errore HTTP 403. AccessDenied Per ulteriori informazioni, consulta [the section called “Blocco o sblocco SSE-C”](#).

Non sono previsti costi aggiuntivi per l'utilizzo. SSE-C Tuttavia, le richieste di configurazione e utilizzo SSE-C comportano costi di richiesta standard di Amazon S3. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Important

Amazon Simple Storage Service applica ora una nuova impostazione di sicurezza predefinita per i bucket che disabilita automaticamente la crittografia lato server con chiavi fornite dal cliente () SSE-C per tutti i nuovi bucket generici. Nell'aprile 2026, Amazon S3 ha implementato un aggiornamento in modo che tutti i nuovi bucket generici abbiano la crittografia disabilitata per tutte le nuove richieste di scrittura. SSE-C Per i bucket esistenti senza oggetti SSE-C crittografati, Amazon S3 è disabilitato SSE-C anche per tutte le nuove richieste di scrittura. Account AWS Con questa modifica, le applicazioni che richiedono SSE-C la crittografia devono essere abilitate deliberatamente SSE-C utilizzando l'operazione [PutBucketEncryption](#) API dopo aver creato un nuovo bucket. Per ulteriori informazioni su questa modifica, vedere. [SSE-C Impostazione predefinita per i nuovi bucket \(domande frequenti\)](#)

Considerazioni prima dell'uso SSE-C

- S3 non memorizza mai la chiave di crittografia quando la usi. SSE-C Devi fornire la chiave di crittografia ogni volta che desideri che qualcuno scarichi i tuoi dati SSE-C crittografati da S3.
- L'utente gestisce una mappatura per tenere traccia della chiave di crittografia che è stata utilizzata per crittografare un determinato oggetto. L'utente è responsabile della tracciatura di ciascuna chiave di crittografia fornita per ogni determinato oggetto. Ciò significa anche che se perdi la chiave di crittografia, perdi l'oggetto.
- Dato che l'utente gestisce le chiavi di crittografia lato cliente, gestisce anche eventuali tutele aggiuntive, come la rotazione delle chiavi, lato cliente.
- Questa progettazione può rendere difficile la condivisione della SSE-C chiave con altri utenti, ruoli o AWS servizi che devono operare sui dati. A causa del diffuso supporto per SSE-KMS across AWS, la maggior parte dei carichi di lavoro moderni non viene utilizzata SSE-C perché non offre la flessibilità di SSE-KMS. Per ulteriori informazioni SSE-KMS, consulta [Utilizzo della crittografia lato server con chiavi AWS KMS \(\)](#). [SSE-KMS](#)

- Ciò significa che gli oggetti crittografati con SSE-C non possono essere decrittografati in modo nativo dai servizi gestiti. AWS
- È necessario utilizzare HTTPS quando si specificano le SSE-C intestazioni delle richieste.
 - Amazon S3 rifiuta qualsiasi richiesta effettuata tramite HTTP durante l'utilizzo. SSE-C Per motivi di sicurezza, ti consigliamo di considerare compromessa qualsiasi chiave inviata erroneamente tramite HTTP. Elimina la chiave ed esegui la rotazione come opportuno.
- Se il bucket è abilitato per il controllo delle versioni, ogni versione dell'oggetto che carichi può avere una propria chiave di crittografia. L'utente è responsabile della tracciatura di ciascuna chiave di crittografia utilizzata per ogni determinato oggetto.
- SSE-C non è supportato nella console Amazon S3. Non è possibile utilizzare la console Amazon S3 per caricare un oggetto e specificare SSE-C la crittografia. Inoltre, non è possibile utilizzare la console per aggiornare (ad esempio, modificare la classe di storage o aggiungere metadati) un oggetto esistente archiviato utilizzando. SSE-C
- SSE-C è bloccato per impostazione predefinita per i nuovi bucket. È necessario abilitare esplicitamente l' SSE-C utilizzo dell'`PutBucketEncryptionAPI` prima di poter caricare oggetti con SSE-C crittografia. Per ulteriori informazioni, consulta [the section called “Blocco o sblocco SSE-C”](#).

Argomenti

- [Specificare la crittografia lato server con chiavi fornite dal cliente \(\) SSE-C](#)
- [Blocco o sblocco SSE-C per un bucket per uso generico](#)
- [SSE-C Impostazione predefinita per i nuovi bucket \(domande frequenti\)](#)

Specificare la crittografia lato server con chiavi fornite dal cliente () SSE-C

Server-side La crittografia con chiavi fornite dal cliente (SSE-C) è disabilitata per impostazione predefinita per i nuovi bucket generici. Prima di poter caricare oggetti utilizzando SSE-C, devi abilitarlo impostando su `NONE` nella configurazione `BlockedEncryptionTypes` di crittografia predefinita del bucket. Per ulteriori informazioni, consulta [Blocco o sblocco SSE-C per un bucket per uso generico](#).

Una volta SSE-C abilitato per il bucket, puoi utilizzarlo SSE-C nelle tue richieste di caricamento passando le intestazioni richieste. Vedi [Azioni Amazon S3 che supportano la scrittura di dati con SSE-C](#) e assicurati di includere [l'intestazioni API S3 necessarie per le richieste di crittografia e decrittografia SSE-C degli oggetti](#).

Quando carichi un oggetto specificando SSE-C, Amazon S3 utilizza la chiave di crittografia fornita per applicare la AES-256 crittografia ai tuoi dati. Amazon S3 rimuove quindi la chiave di crittografia dalla memoria. Quando viene recuperato un oggetto, è necessario fornire la stessa chiave di crittografia come parte della richiesta. Amazon S3 verifica prima che la chiave di crittografia fornita corrisponda, quindi esegue la decrittografia dell'oggetto prima di restituire i relativi dati.

Prima di SSE-C utilizzarlo, assicurati di aver esaminato il [Considerazioni prima dell'uso SSE-C](#)

Note

Amazon S3 non archivia le chiavi di crittografia fornite. Invece, memorizza un valore HMAC (Hash-based Message Authentication Code) della chiave di crittografia salato in modo casuale per convalidare le richieste future. Il valore HMAC con l'introduzione di un sale non può essere utilizzato per derivare il valore della chiave di crittografia o per decrittografare i contenuti dell'oggetto crittografato. Ciò significa che se si perde la chiave di crittografia, si perde l'oggetto.

Argomenti

- [SSE-C Azioni e intestazioni obbligatorie](#)
- [Esempio di politica SSE-C del bucket per applicare la crittografia](#)
- [URL prefirmati e SSE-C](#)
- [Effettuare richieste con SSE-C](#)
- [Utilizzo della REST API](#)
- [Utilizzo di AWS SDK da specificare SSE-C per le operazioni PUT, GET, Head e Copy](#)
- [Utilizzo di AWS SDK da specificare per i caricamenti in più parti SSE-C](#)

SSE-C Azioni e intestazioni obbligatorie

La specifica SSE-C sulle API S3 supportate richiede il passaggio di parametri di richiesta specifici.

Note

L'PutBucketEncryptionAPI non supporta l'impostazione SSE-C come metodo di crittografia predefinito per un bucket, gli oggetti non verranno utilizzati automaticamente. SSE-C SSE-C è un metodo di crittografia a livello di oggetto in cui si fornisce la chiave di

crittografia con ogni richiesta di caricamento o download. Amazon S3 utilizza questa chiave per crittografare o decrittografare l'oggetto durante la richiesta e quindi scarta la chiave. Tuttavia, la usi `PutBucketEncryption` per controllare se i SSE-C caricamenti sono consentiti per il bucket tramite il parametro `BlockedEncryptionTypes`. Per impostazione predefinita, i nuovi bucket sono SSE-C bloccati, è necessario impostare l'opzione `BlockedEncryptionTypes` NONE per consentire i caricamenti. SSE-C

Azioni Amazon S3 che supportano la scrittura di dati con SSE-C

È possibile richiedere la crittografia lato server con le chiavi fornite dal cliente (SSE-C) quando si scrivono oggetti in un bucket generico utilizzando le seguenti operazioni o azioni API:

- [CopyObject](#)
- [CreateMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [POST Object](#)
- [PutObject](#)
- [UploadPart](#)
- [UploadPartCopy](#)

 Note

S3 Replication supporta oggetti crittografati con. SSE-C Per ulteriori informazioni sulla replica di oggetti crittografati, vedere. [Replica di oggetti crittografati \(,,,\) SSE-S3 SSE-KMS DSSE-KMS SSE-C](#)

Intestazioni API S3 necessarie per le richieste di crittografia e decrittografia SSE-C degli oggetti

È necessario fornire le seguenti tre intestazioni API con cui crittografare o decrittografare gli oggetti: SSE-C

- `x-amz-server-side-encryption-customer-algorithm` Usa questa intestazione per specificare l'algoritmo di crittografia. Il valore dell'intestazione deve essere AES256.

- `x-amz-server-side-encryption-customer-key` Usa questa intestazione per fornire la chiave di crittografia a 256 bit con codifica Base64 che Amazon S3 può utilizzare per crittografare o decrittografare i tuoi dati.
- `x-amz-server-side-encryption-customer-key-MD5` Usa questa intestazione per fornire il digest MD5 a 128 bit con codifica Base64 della chiave di crittografia secondo RFC 1321. Amazon S3 utilizza questa intestazione per il controllo dell'integrità del messaggio per accertarsi che la chiave di crittografia sia stata trasmessa senza errori.

Le intestazioni dell'API S3 sono necessarie per le richieste di copia di oggetti sorgente crittografati con SSE-C

È necessario fornire le tre intestazioni API seguenti per copiare gli oggetti sorgente crittografati con SSE-C

- `x-amz-copy-source-server-side-encryption-customer-algorithm` Includi questa intestazione per specificare l'algoritmo che Amazon S3 deve utilizzare per decrittografare l'oggetto sorgente. Questo valore deve essere AES256.
- `x-amz-copy-source-server-side-encryption-customer-key` Includi questa intestazione per fornire la chiave di crittografia con codifica base64 che Amazon S3 può utilizzare per decrittografare l'oggetto sorgente. Questa chiave di crittografia deve essere quella fornita ad Amazon S3 quando è stato creato l'oggetto di origine. In caso contrario, Amazon S3 non riesce a decrittare l'oggetto.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5` Includi questa intestazione per fornire il digest MD5 a 128 bit con codifica Base64 della chiave di crittografia secondo RFC 1321.

Esempio di politica SSE-C del bucket per applicare la crittografia

SSE-C Per richiedere tutti gli oggetti scritti in un bucket Amazon S3, puoi utilizzare una bucket policy. Ad esempio, la seguente policy del bucket nega le autorizzazioni di upload object (`s3:PutObject`) per tutte le richieste che non includono l'header request. `x-amz-server-side-encryption-customer-algorithm` SSE-C

```
{  
  "Version": "2012-10-17",  
  "Id": "PutObjectPolicy",
```



```
"Statement": [
  {
    "Sid": "RequireSSEObjectUploads",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption-customer-algorithm": "true"
      }
    }
  }
]
```

Important

Se utilizzi una policy bucket per richiedere `s3:PutObject`, devi includere l'intestazione `x-amz-server-side-encryption-customer-algorithm` in tutte le richieste di caricamento composte da più parti (., e). `CreateMultipartUpload`, `UploadPart`, `CompleteMultipartUpload`

URL prefirmati e SSE-C

È possibile generare un URL prefirmato che possa essere utilizzato per operazioni quali il caricamento di un nuovo oggetto, il recupero di un oggetto esistente o dei metadata di un oggetto. Gli URL prefirmati supportano quanto segue: SSE-C

- Quando viene creato un URL prefirmato, è necessario specificare l'algoritmo utilizzando l'intestazione `x-amz-server-side-encryption-customer-algorithm` nel calcolo della firma.
- Quando viene utilizzato l'URL prefirmato per il caricamento di un nuovo oggetto, il recupero di un oggetto esistente o solo dei metadata di un oggetto, è necessario fornire tutte le intestazioni di crittografia nella richiesta dell'applicazione client.

 Note

Per i non SSE-C oggetti, puoi generare un URL prefirmato e incollarlo direttamente in un browser per accedere ai dati.

Tuttavia, non è possibile eseguire questa operazione per SSE-C gli oggetti, poiché oltre all'URL prefirmato, è necessario includere anche intestazioni HTTP specifiche degli oggetti. SSE-C Pertanto, è possibile utilizzare gli URL predefiniti per SSE-C gli oggetti solo a livello di programmazione.

Per ulteriori informazioni sugli URL prefirmati, consulta [Download e caricamento di oggetti con URL predefiniti](#).

Effettuare richieste con SSE-C

Al momento della creazione dell'oggetto con l'API REST, è possibile specificare la crittografia lato server con chiavi fornite dal cliente (). SSE-C Quando si utilizza SSE-C, è necessario fornire le informazioni sulla chiave di crittografia utilizzando. [Le intestazioni dell'API S3 sono necessarie per le richieste di copia di oggetti sorgente crittografati con SSE-C](#) Puoi utilizzare le librerie di wrapper AWS SDK per aggiungere queste intestazioni alla tua richiesta. Se necessario, è possibile anche effettuare le chiamate REST API di Amazon S3 direttamente nell'applicazione.

 Important

SSE-C è disabilitato per impostazione predefinita per tutti i nuovi bucket. Prima di caricare oggetti con SSE-C, devi abilitarlo aggiornando la configurazione di crittografia predefinita del bucket. Per ulteriori informazioni, consulta [Blocco o sblocco SSE-C per un bucket per uso generico](#).

 Note

Non è possibile utilizzare la console Amazon S3 per caricare un oggetto e richiederlo. SSE-C Inoltre, non è possibile utilizzare la console per aggiornare (ad esempio, modificare la classe di storage o aggiungere metadati) un oggetto esistente archiviato utilizzando. SSE-C Per ulteriori informazioni, consulta [Intestazioni API S3 necessarie per le richieste di crittografia e decrittografia SSE-C degli oggetti](#).

Utilizzo della REST API

API REST di Amazon S3 che supportano SSE-C

Le seguenti API Amazon S3 supportano la crittografia lato server con chiavi di crittografia fornite dal cliente (). SSE-C

- Operazione GET: quando si recuperano oggetti utilizzando l'API GET (consulta l'argomento relativo all'[operazione GetObject](#)), è possibile specificare le intestazioni di richiesta.
- Operazione HEAD: per recuperare i metadati dell'oggetto utilizzando l'API HEAD (consulta l'argomento relativo all'[operazione HeadObject](#)), è possibile specificare queste intestazioni di richiesta.
- Operazione PUT: quando si caricano dati utilizzando l'API PUT (consulta l'argomento relativo all'[operazione PutObject](#)), è possibile specificare queste intestazioni di richiesta.
- Caricamento in più parti: quando si caricano oggetti di grandi dimensioni utilizzando l'API per il caricamento in più parti, è possibile specificare queste intestazioni. Specifica queste intestazioni nella richiesta iniziale (vedi [Initiate Multipart Upload](#)) e in ogni successiva richiesta di caricamento delle parti (vedi Upload Part or). <https://docs.aws.amazon.com/AmazonS3/latest/API/mpUploadUploadPart.html> [UploadPartCopy](#) Per ogni richiesta di caricamento di parte, le informazioni della crittografia devono essere uguali a quelle specificate nella richiesta di avvio di caricamento in più parti.
- Operazione POST: quando si utilizza un'operazione POST per caricare un oggetto (consulta l'argomento relativo all'[oggetto POST](#)), anziché nelle intestazioni di richiesta, è necessario specificare le stesse informazioni nei campi del modulo.
- Operazione di copia: quando copi un oggetto (vedi [CopyObject](#)), hai sia un oggetto di origine che un oggetto di destinazione:
 - Se si desidera specificare il tipo di crittografia dell'oggetto di destinazione, è necessario fornire l'intestazione della `x-amz-server-side-encryption` richiesta.
 - Se desideri che l'oggetto di destinazione venga crittografato utilizzando SSE-C, devi fornire le informazioni di crittografia utilizzando l'API S3. [Intestazioni API S3 necessarie per le richieste di crittografia e decrittografia SSE-C degli oggetti](#)
 - Se l'oggetto di origine è crittografato utilizzando SSE-C, è necessario fornire le informazioni sulla chiave di crittografia utilizzando le intestazioni dell'API S3. [Le intestazioni dell'API S3 sono necessarie per le richieste di copia di oggetti sorgente crittografati con SSE-C](#)

Utilizzo di AWS SDK da specificare SSE-C per le operazioni PUT, GET, Head e Copy

Gli esempi seguenti mostrano come richiedere la crittografia lato server con chiavi () fornite dal cliente per gli oggetti. SSE-C Negli esempi vengono eseguite le operazioni riportate di seguito. Ogni operazione mostra come specificare le SSE-C-related intestazioni nella richiesta:

- Put object: consente di caricare un oggetto e richiedere la crittografia lato server utilizzando la chiave di crittografia fornita dal cliente.
- Get object: consente di scaricare l'oggetto caricato durante la fase precedente. Nella richiesta, vengono fornite le stesse informazioni di crittografia specificate quando è stato caricato l'oggetto. per consentire ad Amazon S3 di decrittare l'oggetto e di restituirlo.
- Get object metadata: consente di recuperare i metadati dell'oggetto. Fornire le stesse informazioni di crittografia utilizzate quando l'oggetto è stato creato.
- Copy object: consente di creare una copia dell'oggetto caricato in precedenza. Poiché l'oggetto sorgente viene archiviato utilizzando SSE-C, è necessario fornire le relative informazioni di crittografia nella richiesta di copia. Per impostazione predefinita, Amazon S3 esegue la crittografia dell'oggetto solo se richiesta esplicitamente. In questo esempio, Amazon S3 viene configurato per archiviare una copia crittografata dell'oggetto.

Java

Note

In questo esempio viene illustrato come caricare un oggetto in un'unica operazione. Quando si utilizza l'API per il caricamento in più parti per caricare oggetti di grandi dimensioni, fornire le informazioni di crittografia nello stesso modo mostrato in questo esempio. Per esempi di caricamenti in più parti che utilizzano il AWS SDK per Java, vedere [Caricamento di un oggetto utilizzando il caricamento in più parti](#)

Per aggiungere le informazioni di crittografia richieste, includere SSECustomerKey nella richiesta. Per ulteriori informazioni sulla classe SSECustomerKey, consulta la sezione relativa a REST API.

Per istruzioni su come creare e testare un campione funzionante, consulta [Getting Started](#) nella AWS SDK per Java Developer Guide.

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import javax.crypto.KeyGenerator;
import java.io.BufferedReader;
import java.io.File;
import java.io.IOException;
import java.io.InputStreamReader;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;

public class ServerSideEncryptionUsingClientSideEncryptionKey {
    private static SSECustomerKey SSE_KEY;
    private static AmazonS3 S3_CLIENT;
    private static KeyGenerator KEY_GENERATOR;

    public static void main(String[] args) throws IOException,
        NoSuchAlgorithmException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "**** Bucket name ****";
        String keyName = "**** Key name ****";
        String uploadFileName = "**** File path ****";
        String targetKeyName = "**** Target key name ****";

        // Create an encryption key.
        KEY_GENERATOR = KeyGenerator.getInstance("AES");
        KEY_GENERATOR.init(256, new SecureRandom());
        SSE_KEY = new SSECustomerKey(KEY_GENERATOR.generateKey());

        try {
            S3_CLIENT = AmazonS3ClientBuilder.standard()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(clientRegion)
                .build();

            // Upload an object.
```

```
        uploadObject(bucketName, keyName, new File(uploadFileName));

        // Download the object.
        downloadObject(bucketName, keyName);

        // Verify that the object is properly encrypted by attempting to
retrieve it
        // using the encryption key.
        retrieveObjectMetadata(bucketName, keyName);

        // Copy the object into a new object that also uses SSE-C.
        copyObject(bucketName, keyName, targetKeyName);
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}

private static void uploadObject(String bucketName, String keyName, File file) {
    PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
file).withSSECustomerKey(SSE_KEY);
    S3_CLIENT.putObject(putRequest);
    System.out.println("Object uploaded");
}

private static void downloadObject(String bucketName, String keyName) throws
IOException {
    GetObjectRequest getObjectRequest = new GetObjectRequest(bucketName,
keyName).withSSECustomerKey(SSE_KEY);
    S3Object object = S3_CLIENT.getObject(getObjectRequest);

    System.out.println("Object content: ");
    displayTextInputStream(object.getObjectContent());
}

private static void retrieveObjectMetadata(String bucketName, String keyName) {
    GetObjectMetadataRequest getMetadataRequest = new
GetObjectMetadataRequest(bucketName, keyName)
        .withSSECustomerKey(SSE_KEY);
```

```

        ObjectMetadata objectMetadata =
S3_CLIENT.getObjectMetadata(getMetadataRequest);
        System.out.println("Metadata retrieved. Object size: " +
objectMetadata.getContentLength());
    }

    private static void copyObject(String bucketName, String keyName, String
targetKeyName)
        throws NoSuchAlgorithmException {
        // Create a new encryption key for target so that the target is saved using
        // SSE-C.
        SSECustomerKey newSSEKey = new SSECustomerKey(KEY_GENERATOR.generateKey());

        CopyObjectRequest copyRequest = new CopyObjectRequest(bucketName, keyName,
bucketName, targetKeyName)
            .withSourceSSECustomerKey(SSE_KEY)
            .withDestinationSSECustomerKey(newSSEKey);

        S3_CLIENT.copyObject(copyRequest);
        System.out.println("Object copied");
    }

    private static void displayTextInputStream(S3ObjectInputStream input) throws
IOException {
        // Read one line at a time from the input stream and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}

```

.NET

Note

Per esempi di caricamento di oggetti di grandi dimensioni utilizzando l'API per il caricamento in più parti, consulta [Caricamento di un oggetto utilizzando il caricamento in più parti](#) e [Utilizzo di AWS SDK \(API di basso livello\)](#).

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella AWS SDK for .NET Developer Guide.

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSEClientEncryptionKeyObjectOperationsTest
    {
        private const string bucketName = "**** bucket name ****";
        private const string keyName = "**** key name for new object created ****";
        private const string copyTargetKeyName = "**** key name for object copy ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            ObjectOpsUsingClientEncryptionKeyAsync().Wait();
        }
        private static async Task ObjectOpsUsingClientEncryptionKeyAsync()
        {
            try
            {
                // Create an encryption key.
                Aes aesEncryption = Aes.Create();
                aesEncryption.KeySize = 256;
                aesEncryption.GenerateKey();
                string base64Key = Convert.ToBase64String(aesEncryption.Key);

                // 1. Upload the object.
                PutObjectRequest putObjectRequest = await
UploadObjectAsync(base64Key);
```



```

        // 2. Download the object and verify that its contents matches what
you uploaded.
        await DownloadObjectAsync(base64Key, putObjectRequest);
        // 3. Get object metadata and verify that the object uses AES-256
encryption.
        await GetObjectMetadataAsync(base64Key);
        // 4. Copy both the source and target objects using server-side
encryption with
        //    a customer-provided encryption key.
        await CopyObjectAsync(aesEncryption, base64Key);
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
}

private static async Task<PutObjectRequest> UploadObjectAsync(string
base64Key)
{
    PutObjectRequest putObjectRequest = new PutObjectRequest
    {
        BucketName = bucketName,
        Key = keyName,
        ContentBody = "sample text",
        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
        ServerSideEncryptionCustomerProvidedKey = base64Key
    };
    PutObjectResponse putObjectResponse = await
client.PutObjectAsync(putObjectRequest);
    return putObjectRequest;
}

private static async Task DownloadObjectAsync(string base64Key,
PutObjectRequest putObjectRequest)
{
    GetObjectRequest getObjectRequest = new GetObjectRequest
    {

```

```
        BucketName = bucketName,
        Key = keyName,
        // Provide encryption information for the object stored in Amazon
S3.
        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
        ServerSideEncryptionCustomerProvidedKey = base64Key
    };

    using (GetObjectResponse getResponse = await
client.GetObjectAsync(getObjectRequest))
        using (StreamReader reader = new
StreamReader(getResponse.ResponseStream))
        {
            string content = reader.ReadToEnd();
            if (String.Compare(putObjectRequest.ContentBody, content) == 0)
                Console.WriteLine("Object content is same as we uploaded");
            else
                Console.WriteLine("Error...Object content is not same.");

            if (getResponse.ServerSideEncryptionCustomerMethod ==
ServerSideEncryptionCustomerMethod.AES256)
                Console.WriteLine("Object encryption method is AES256, same as
we set");
            else
                Console.WriteLine("Error...Object encryption method is not the
same as AES256 we set");

            // Assert.AreEqual(putObjectRequest.ContentBody, content);
            // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getResponse.ServerSideEncryptionCustomerMethod);
        }
    }

    private static async Task GetObjectMetadataAsync(string base64Key)
    {
        GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest
        {
            BucketName = bucketName,
            Key = keyName,

            // The object stored in Amazon S3 is encrypted, so provide the
necessary encryption information.
        }
    }
}
```

```
        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
        ServerSideEncryptionCustomerProvidedKey = base64Key
    };

    GetObjectMetadataResponse getObjectMetadataResponse = await
client.GetObjectMetadataAsync(getObjectMetadataRequest);
    Console.WriteLine("The object metadata show encryption method used is:
{0}", getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
    // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
}
private static async Task CopyObjectAsync(Aes aesEncryption, string
base64Key)
{
    aesEncryption.GenerateKey();
    string copyBase64Key = Convert.ToBase64String(aesEncryption.Key);

    CopyObjectRequest copyRequest = new CopyObjectRequest
    {
        SourceBucket = bucketName,
        SourceKey = keyName,
        DestinationBucket = bucketName,
        DestinationKey = copyTargetKeyName,
        // Information about the source object's encryption.
        CopySourceServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
        CopySourceServerSideEncryptionCustomerProvidedKey = base64Key,
        // Information about the target object's encryption.
        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
        ServerSideEncryptionCustomerProvidedKey = copyBase64Key
    };
    await client.CopyObjectAsync(copyRequest);
}
}
```

Utilizzo di AWS SDK da specificare per i caricamenti in più parti SSE-C

L'esempio nella sezione precedente mostra come richiedere la crittografia lato server con key (SSE-C) fornita dal cliente nelle operazioni PUT, GET, Head e Copy. Questa sezione descrive altre API Amazon S3 che supportano SSE-C.

Java

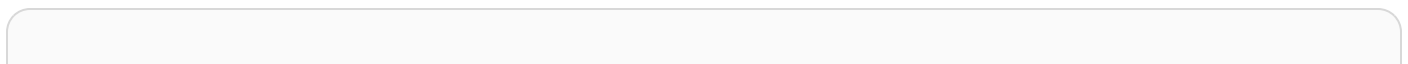
Per caricare oggetti di grandi dimensioni, puoi utilizzare API di caricamento in più parti. Per ulteriori informazioni, consulta [Caricamento e copia di oggetti utilizzando il caricamento multipart in Amazon S3](#). È possibile utilizzare indifferentemente API di livello alto o basso per caricare gli oggetti di grandi dimensioni. Queste API supportano l'uso di intestazioni correlate alla crittografia nella richiesta.

- Quando utilizzi l'`TransferManager` API di alto livello, fornisci le intestazioni specifiche della crittografia nel `PutObjectRequest`. Per ulteriori informazioni, consulta [Caricamento di un oggetto utilizzando il caricamento in più parti](#).
- Quando si utilizza l'API di basso livello, è necessario fornire informazioni correlate alla crittografia nella `InitiateMultipartUploadRequest`, seguite da informazioni di crittografia identiche in ogni `UploadPartRequest`. Non è necessario fornire alcuna intestazione specifica della crittografia nella `CompleteMultipartUploadRequest`. Per alcuni esempi, consulta [Utilizzo di AWS SDK \(API di basso livello\)](#).

L'esempio seguente viene utilizzato `TransferManager` per creare oggetti e mostra come fornire informazioni correlate SSE-C. Inoltre, vengono effettuate le seguenti operazioni:

- Viene creato un oggetto utilizzando il metodo `TransferManager.upload()`. In tal `PutObjectRequest` caso, si forniscono le informazioni sulla chiave di crittografia nella richiesta. Amazon S3 esegue la crittografia dell'oggetto utilizzando la chiave fornita dal cliente.
- Viene eseguita una copia dell'oggetto richiamando il metodo `TransferManager.copy()`. Nell'esempio Amazon S3 viene configurato per crittografare la copia dell'oggetto utilizzando una nuova `SSECustomerKey`. Poiché l'oggetto sorgente è crittografato utilizzando SSE-C, fornisce `CopyObjectRequest` anche la chiave di crittografia dell'oggetto sorgente in modo che Amazon S3 possa decrittografare l'oggetto prima di copiarlo.

Example



```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.model.SSECustomerKey;
import com.amazonaws.services.s3.transfer.Copy;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.TransferManagerBuilder;
import com.amazonaws.services.s3.transfer.Upload;

import javax.crypto.KeyGenerator;
import java.io.File;
import java.security.SecureRandom;

public class ServerSideEncryptionCopyObjectUsingHlwithSSEC {

    public static void main(String[] args) throws Exception {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "**** Bucket name ****";
        String fileToUpload = "**** File path ****";
        String keyName = "**** New object key name ****";
        String targetKeyName = "**** Key name for object copy ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                .withRegion(clientRegion)
                .withCredentials(new ProfileCredentialsProvider())
                .build();

            TransferManager tm = TransferManagerBuilder.standard()
                .withS3Client(s3Client)
                .build();

            // Create an object from a file.
            PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName,
            keyName, new File(fileToUpload));

            // Create an encryption key.
            KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
            keyGenerator.init(256, new SecureRandom());
```

```
        SSECustomerKey sseCustomerEncryptionKey = new
SSECustomerKey(keyGenerator.generateKey());

        // Upload the object. TransferManager uploads asynchronously, so this
call
        // returns immediately.
        putObjectRequest.setSSECustomerKey(sseCustomerEncryptionKey);
        Upload upload = tm.upload(putObjectRequest);

        // Optionally, wait for the upload to finish before continuing.
        upload.waitForCompletion();
        System.out.println("Object created.");

        // Copy the object and store the copy using SSE-C with a new key.
        CopyObjectRequest copyObjectRequest = new CopyObjectRequest(bucketName,
keyName, bucketName, targetKeyName);
        SSECustomerKey sseTargetObjectEncryptionKey = new
SSECustomerKey(keyGenerator.generateKey());
        copyObjectRequest.setSourceSSECustomerKey(sseCustomerEncryptionKey);

        copyObjectRequest.setDestinationSSECustomerKey(sseTargetObjectEncryptionKey);

        // Copy the object. TransferManager copies asynchronously, so this call
returns
        // immediately.
        Copy copy = tm.copy(copyObjectRequest);

        // Optionally, wait for the upload to finish before continuing.
        copy.waitForCompletion();
        System.out.println("Copy complete.");
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
```

.NET

Per caricare oggetti di grandi dimensioni, puoi utilizzare l'API di caricamento in più parti (vedi). [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#) AWS SDK for .NET fornisce API di alto o basso livello per caricare oggetti di grandi dimensioni. Queste API supportano l'uso di intestazioni correlate alla crittografia nella richiesta.

- Quando si utilizza l'API `Transfer-Utility` di alto livello, è necessario fornire le intestazioni specifiche della crittografia in `TransferUtilityUploadRequest` come mostrato. Per alcuni esempi di codice, consultare [Caricamento di un oggetto utilizzando il caricamento in più parti](#).

```
TransferUtilityUploadRequest request = new TransferUtilityUploadRequest()  
{  
    FilePath = filePath,  
    BucketName = existingBucketName,  
    Key = keyName,  
    // Provide encryption information.  
    ServerSideEncryptionCustomerMethod =  
    ServerSideEncryptionCustomerMethod.AES256,  
    ServerSideEncryptionCustomerProvidedKey = base64Key,  
};
```

- Quando si utilizza l'API di basso livello, è necessario fornire informazioni correlate alla crittografia nella richiesta di avvio del caricamento in più parti, seguite da informazioni di crittografia identiche nelle successive richieste di caricamento della parte. Non è necessario fornire alcuna intestazione specifica della crittografia nella richiesta di caricamento in più parti completa. Per alcuni esempi, consulta [Utilizzo di AWS SDK \(API di basso livello\)](#).

Di seguito è riportato un esempio di caricamento in più parti di basso livello in cui viene creata una copia di un oggetto di grandi dimensioni esistente. Nell'esempio, l'oggetto da copiare viene archiviato in Amazon S3 utilizzando SSE-C e si desidera salvare anche l'oggetto di destinazione utilizzando SSE-C. Inoltre, vengono effettuate le seguenti operazioni:

- Viene avviata una richiesta di caricamento in più parti specificando una chiave di crittografia e informazioni correlate.
- Vengono fornite chiavi di crittografia e informazioni correlate per gli oggetti di origine e di destinazione nella richiesta `CopyPartRequest`.
- Viene ottenuta la dimensione dell'oggetto di origine da copiare recuperando i metadata dell'oggetto.
- Caricamento degli oggetti in parti da 5 MB

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSECLowLevelMPUCopyObjectTest
    {
        private const string existingBucketName = "**** bucket name ****";
        private const string sourceKeyName      = "**** source object key name
****";
        private const string targetKeyName      = "**** key name for the target
object ****";
        private const string filePath           = @"**** file path ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CopyObjClientEncryptionKeyAsync().Wait();
        }

        private static async Task CopyObjClientEncryptionKeyAsync()
        {
            Aes aesEncryption = Aes.Create();
            aesEncryption.KeySize = 256;
            aesEncryption.GenerateKey();
            string base64Key = Convert.ToBase64String(aesEncryption.Key);

            await CreateSampleObjUsingClientEncryptionKeyAsync(base64Key,
s3Client);

            await CopyObjectAsync(s3Client, base64Key);
        }
    }
}
```



```

        private static async Task CopyObjectAsync(IAmazonS3 s3Client, string
base64Key)
        {
            List<CopyPartResponse> uploadResponses = new List<CopyPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = targetKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key,
            };

            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB
            long firstByte = 0;
            long lastByte = partSize;

            try
            {
                // First find source object size. Because object is stored
encrypted with
                // customer provided key you need to provide encryption
information in your request.
                GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest()
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                    ServerSideEncryptionCustomerProvidedKey = base64Key // " *
**source object encryption key ***"
                };

                GetObjectMetadataResponse getObjectMetadataResponse = await
s3Client.GetObjectMetadataAsync(getObjectMetadataRequest);

```

```

        long filePosition = 0;
        for (int i = 1; filePosition <
getObjectMetadataResponse.ContentLength; i++)
        {
            CopyPartRequest copyPartRequest = new CopyPartRequest
            {
                UploadId = initResponse.UploadId,
                // Source.
                SourceBucket = existingBucketName,
                SourceKey = sourceKeyName,
                // Source object is stored using SSE-C. Provide encryption
information.
                CopySourceServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                CopySourceServerSideEncryptionCustomerProvidedKey =
base64Key, //"***source object encryption key ***",
                FirstByte = firstByte,
                // If the last part is smaller then our normal part size
then use the remaining size.
                LastByte = lastByte >
getObjectMetadataResponse.ContentLength ?
                getObjectMetadataResponse.ContentLength - 1 :
lastByte,

                // Target.
                DestinationBucket = existingBucketName,
                DestinationKey = targetKeyName,
                PartNumber = i,
                // Encryption information for the target object.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };
            uploadResponses.Add(await
s3Client.CopyPartAsync(copyPartRequest));
            filePosition += partSize;
            firstByte += partSize;
            lastByte += partSize;
        }

        // Step 3: complete.
        CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
        {

```

```

        BucketName = existingBucketName,
        Key = targetKeyName,
        UploadId = initResponse.UploadId,
    };
    completeRequest.AddPartETags(uploadResponses);

    CompleteMultipartUploadResponse completeUploadResponse =
        await s3Client.CompleteMultipartUploadAsync(completeRequest);
}
catch (Exception exception)
{
    Console.WriteLine("Exception occurred: {0}", exception.Message);
    AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
    {
        BucketName = existingBucketName,
        Key = targetKeyName,
        UploadId = initResponse.UploadId
    };
    s3Client.AbortMultipartUpload(abortMPURequest);
}
}

private static async Task
CreateSampleObjUsingClientEncryptionKeyAsync(string base64Key, IAmazonS3
s3Client)
{
    // List to store upload part responses.
    List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();

    // 1. Initialize.
    InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
    {
        BucketName = existingBucketName,
        Key = sourceKeyName,
        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
        ServerSideEncryptionCustomerProvidedKey = base64Key
    };

    InitiateMultipartUploadResponse initResponse =
        await s3Client.InitiateMultipartUploadAsync(initiateRequest);

```

```
// 2. Upload Parts.
long contentLength = new FileInfo(filePath).Length;
long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

try
{
    long filePosition = 0;
    for (int i = 1; filePosition < contentLength; i++)
    {
        UploadPartRequest uploadRequest = new UploadPartRequest
        {
            BucketName = existingBucketName,
            Key = sourceKeyName,
            UploadId = initResponse.UploadId,
            PartNumber = i,
            PartSize = partSize,
            FilePosition = filePosition,
            FilePath = filePath,
            ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
            ServerSideEncryptionCustomerProvidedKey = base64Key
        };

        // Upload part and add response to our list.
        uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

        filePosition += partSize;
    }

    // Step 3: complete.
    CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
    {
        BucketName = existingBucketName,
        Key = sourceKeyName,
        UploadId = initResponse.UploadId,
        //PartETags = new List<PartETag>(uploadResponses)

    };
    completeRequest.AddPartETags(uploadResponses);

    CompleteMultipartUploadResponse completeUploadResponse =
        await s3Client.CompleteMultipartUploadAsync(completeRequest);
}
```

```
    }
    catch (Exception exception)
    {
        Console.WriteLine("Exception occurred: {0}", exception.Message);
        AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
        {
            BucketName = existingBucketName,
            Key = sourceKeyName,
            UploadId = initResponse.UploadId
        };
        await s3Client.AbortMultipartUploadAsync(abortMPURequest);
    }
}
}
```

Blocco o sblocco SSE-C per un bucket per uso generico

A partire da aprile 2026, Amazon S3 disabilita automaticamente la crittografia lato server con chiavi fornite dal cliente (SSE-C) per tutti i nuovi bucket generici. SSE-C Amazon S3 è inoltre disabilitato per i bucket esistenti negli account senza oggetti crittografati. Ciò significa che, per impostazione predefinita, le richieste di caricamento di oggetti utilizzando SSE-C vengono rifiutate con un errore HTTP AccessDenied 403.

SSE-C richiede di fornire la chiave di crittografia con ogni richiesta di lettura o scrittura di oggetti crittografati, rendendo difficile la condivisione dell'accesso con altri utenti, ruoli o AWS servizi che operano sui dati. La maggior parte dei carichi di lavoro utilizza invece la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) o chiavi AWS KMS (SSE-KMS).

Se il carico di lavoro lo richiede SSE-C, puoi abilitarlo esplicitamente aggiornando la configurazione di crittografia predefinita per il tuo bucket. Al contrario, se hai bucket esistenti in cui SSE-C è ancora consentito, puoi bloccarli per evitare nuovi caricamenti.

Se SSE-C è bloccato per un bucket PutObject CopyObject PostObject, qualsiasi richiesta di replica o caricamento in più parti che specifichi la SSE-C crittografia verrà rifiutata con un errore HTTP 403. AccessDenied Gli oggetti SSE-C crittografati esistenti nel bucket non sono interessati, puoi comunque leggerli con GetObject o fornendo le intestazioni richieste. HeadObject SSE-C

Questa impostazione è un parametro dell'`PutBucketEncryptionAPI` e può essere aggiornata anche utilizzando la console S3, la AWS CLI o gli SDK. AWS Deve disporre dell'autorizzazione `s3:PutEncryptionConfiguration`.

 Important

Amazon Simple Storage Service applica ora una nuova impostazione di sicurezza predefinita per i bucket che disabilita automaticamente la crittografia lato server con chiavi fornite dal cliente (SSE-C) per tutti i nuovi bucket generici. SSE-C Nell'aprile 2026, Amazon S3 ha implementato un aggiornamento in modo che tutti i nuovi bucket generici abbiano la crittografia disabilitata per tutte le nuove richieste di scrittura. SSE-C Per i bucket esistenti senza oggetti SSE-C crittografati, Amazon S3 è disabilitato SSE-C anche per tutte le nuove richieste di scrittura. Account AWS Con questa modifica, le applicazioni che richiedono SSE-C la crittografia devono essere abilitate deliberatamente SSE-C utilizzando l'operazione [PutBucketEncryption](#) API dopo aver creato un nuovo bucket. Per ulteriori informazioni su questa modifica, vedere [SSE-C Impostazione predefinita per i nuovi bucket \(domande frequenti\)](#).

Permissions

Usa l'`PutBucketEncryptionAPI` o la console S3, AWS gli SDK o la AWS CLI per bloccare o sbloccare i tipi di crittografia per un bucket generico. È necessario disporre delle seguenti autorizzazioni:

- `s3:PutEncryptionConfiguration`

Usa l'`GetBucketEncryptionAPI` o la console S3, AWS gli SDK o la AWS CLI per visualizzare i tipi di crittografia bloccati per un bucket generico. È necessario disporre delle seguenti autorizzazioni:

- `s3:GetEncryptionConfiguration`

Considerazioni prima di bloccare SSE-C la crittografia

Dopo aver bloccato SSE-C un bucket, si applica il seguente comportamento di crittografia:

- Non è stata apportata alcuna modifica alla crittografia degli oggetti che esistevano nel bucket prima del blocco SSE-C della crittografia.

- Dopo aver bloccato SSE-C la crittografia, è possibile continuare a effettuare GetObject HeadObject richieste su oggetti preesistenti crittografati SSE-C purché vengano fornite le SSE-C intestazioni richieste nelle richieste.
- Quando SSE-C è bloccata per un bucket PutObject CopyObjectPostObject, qualsiasi richiesta di caricamento in più parti che specifichi la SSE-C crittografia verrà rifiutata con un errore HTTP 403. AccessDenied
- Se un bucket di destinazione per la replica è SSE-C bloccato e gli oggetti di origine da replicare sono crittografati con SSE-C, la replica avrà esito negativo e verrà generato un errore HTTP 403. AccessDenied

Se desideri verificare se stai utilizzando la SSE-C crittografia in uno dei tuoi bucket prima di bloccare questo tipo di crittografia, puoi utilizzare strumenti come monitorare l'accesso [AWS CloudTrail](#) ai tuoi dati. Questo post [del blog](#) mostra come verificare i metodi di crittografia per il caricamento di oggetti in tempo reale. Puoi anche fare riferimento a questo articolo di [Re:POST](#) per guidarti nell'interrogazione dei report di S3 Inventory per vedere se hai oggetti crittografati. SSE-C

Fasi

Puoi bloccare o sbloccare la crittografia lato server con chiavi (SSE-C) fornite dal cliente per un bucket generico utilizzando la console Amazon S3, (), l'API REST di Amazon S3 e gli AWS Command Line Interface SDK.AWS CLI AWS

Utilizzo della console S3

Per bloccare o sbloccare la crittografia per un bucket utilizzando la console Amazon S3 SSE-C :

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, scegli bucket per uso generico.
3. Seleziona il bucket per il quale desideri bloccare la SSE-C crittografia.
4. Seleziona la scheda Proprietà per il bucket.
5. Accedi al pannello delle proprietà di crittografia predefinita per il bucket e seleziona Modifica.
6. Nella sezione Tipi di crittografia bloccati, seleziona la casella accanto alla Server-side crittografia con chiavi fornite dal cliente (SSE-C) per bloccare la SSE-C crittografia o deselecta questa casella per consentire. SSE-C
7. Seleziona Salva modifiche.

Utilizzo di AWS CLI

Per installare la AWS CLI, vedere [Installazione della AWS CLI nella Guida per l'utente](#). AWS Command Line Interface

Il seguente esempio CLI mostra come bloccare o sbloccare la SSE-C crittografia per un bucket generico utilizzando. AWS CLI Per utilizzare il comando, sostituisci il *user input placeholders* con le tue informazioni.

Richiesta di blocco della SSE-C crittografia per un bucket generico:

```
aws s3api put-bucket-encryption \
  --bucket amzn-s3-demo-bucket \
  --server-side-encryption-configuration '{
    "Rules": [{
      "BlockedEncryptionTypes": {
        "EncryptionType": ["SSE-C"]
      }
    }]
  }'
```

Richiesta di abilitare l'uso della SSE-C crittografia su un bucket generico:

```
aws s3api put-bucket-encryption \
  --bucket amzn-s3-demo-bucket \
  --server-side-encryption-configuration '{
    "Rules": [{
      "BlockedEncryptionTypes": {
        "EncryptionType": ["NONE"]
      }
    }]
  }'
```

Utilizzo di AWS SDK

SDK for Java 2.x

Gli esempi seguenti mostrano come bloccare o sbloccare le scritture SSE-C crittografiche nei bucket generici utilizzando gli SDK AWS

Esempio: PutBucketEncryption richiesta che imposta la configurazione di crittografia predefinita su e blocca SSE-S3 SSE-C


```

S3Client s3Client = ...;
ServerSideEncryptionByDefault defaultSse = ServerSideEncryptionByDefault
    .builder()
    .sseAlgorithm(ServerSideEncryption.AES256)
    .build();
BlockedEncryptionTypes blockedEncryptionTypes = BlockedEncryptionTypes
    .builder()
    .encryptionType(EncryptionType.SSE_C)
    .build();
ServerSideEncryptionRule rule = ServerSideEncryptionRule.builder()
    .applyServerSideEncryptionByDefault(defaultSse)
    .blockedEncryptionTypes(blockedEncryptionTypes)
    .build();
s3Client.putBucketEncryption(be -> be
    .bucket(bucketName)
    .serverSideEncryptionConfiguration(c -> c.rules(rule)));

```

Esempio: PutBucketEncryption richiesta di impostazione della configurazione di crittografia predefinita SSE-S3 e sblocco SSE-C

```

S3Client s3Client = ...;
ServerSideEncryptionByDefault defaultSse = ServerSideEncryptionByDefault
    .builder()
    .sseAlgorithm(ServerSideEncryption.AES256)
    .build();
BlockedEncryptionTypes blockedEncryptionTypes = BlockedEncryptionTypes
    .builder()
    .encryptionType(EncryptionType.NONE)
    .build();
ServerSideEncryptionRule rule = ServerSideEncryptionRule.builder()
    .applyServerSideEncryptionByDefault(defaultSse)
    .blockedEncryptionTypes(blockedEncryptionTypes)
    .build();
s3Client.putBucketEncryption(be -> be
    .bucket(bucketName)
    .serverSideEncryptionConfiguration(c -> c.rules(rule)));

```

SDK for Python Boto3

Esempio: PutBucketEncryption richiesta che imposta la configurazione di crittografia predefinita su SSE-S3 e blocca SSE-C

```
s3 = boto3.client("s3")
s3.put_bucket_encryption(
    Bucket="amzn-s3-demo-bucket",
    ServerSideEncryptionConfiguration={
        "Rules":[{
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            },
            "BlockedEncryptionTypes": {
                "EncryptionType": ["SSE-C"]
            }
        }]
    }
)
```

Esempio: PutBucketEncryption richiesta di impostazione della configurazione di crittografia predefinita SSE-S3 e sblocco SSE-C

```
s3 = boto3.client("s3")
s3.put_bucket_encryption(
    Bucket="amzn-s3-demo-bucket",
    ServerSideEncryptionConfiguration={
        "Rules":[{
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            },
            "BlockedEncryptionTypes": {
                "EncryptionType": ["NONE"]
            }
        }]
    }
)
```

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per bloccare o sbloccare la SSE-C crittografia per un bucket generico, consulta la seguente sezione nell'[Amazon Simple Storage Service API Reference](#):

- [BlockedEncryptionType](#) tipo di dati utilizzato nel tipo di [ServerSideEncryptionRule](#) dati [PutBucketEncryption](#) e [GetBucketEncryption](#) nelle operazioni API.

SSE-C Impostazione predefinita per i nuovi bucket (domande frequenti)

Important

Amazon Simple Storage Service applica ora una nuova impostazione di sicurezza predefinita per i bucket che disabilita automaticamente la crittografia lato server con chiavi fornite dal cliente (SSE-C) per tutti i nuovi bucket generici. Nell'aprile 2026, Amazon S3 ha implementato un aggiornamento in modo che tutti i nuovi bucket generici abbiano la crittografia disabilitata per tutte le nuove richieste di scrittura. SSE-C Per i bucket esistenti senza oggetti SSE-C crittografati, Amazon S3 è disabilitato SSE-C anche per tutte le nuove richieste di scrittura. Account AWS Con questa modifica, le applicazioni che richiedono SSE-C la crittografia devono essere abilitate deliberatamente SSE-C utilizzando l'operazione [PutBucketEncryption](#) API dopo aver creato un nuovo bucket.

Nelle sezioni seguenti vengono fornite le risposte alle domande su questo aggiornamento.

1. La nuova SSE-C impostazione ha effetto per tutti i bucket appena creati?

Sì. Questa distribuzione è stata completata in 37 AWS regioni, comprese le regioni AWS Cina e AWS GovCloud (Stati Uniti), nell'aprile 2026.

Note

Tutti i bucket appena creati in tutte le AWS regioni ad eccezione del Medio Oriente (Bahrain) e del Medio Oriente (Emirati Arabi Uniti) saranno disattivati per impostazione predefinita. SSE-C

2. Amazon S3 ha aggiornato le mie configurazioni di bucket esistenti?

Se il tuo AWS account non aveva oggetti SSE-C crittografati, AWS disabilita SSE-C la crittografia su tutti i bucket esistenti. Se un bucket del tuo AWS account conteneva oggetti SSE-C crittografati, non AWS hai modificato le configurazioni dei bucket su nessuno dei bucket di quell'account. La nuova impostazione predefinita si applica a tutti i nuovi bucket generici.

3. Posso disattivare SSE-C la crittografia per i miei bucket?

Sì. Puoi disabilitare SSE-C la crittografia per qualsiasi bucket chiamando l'operazione [PutBucketEncryption](#) API e specificando la nuova `BlockedEncryptionTypes` intestazione.

4. Posso usare SSE-C per crittografare i dati nei miei nuovi bucket?

Sì. La maggior parte dei casi d'uso moderni in Amazon S3 non viene più utilizzata SSE-C perché manca la flessibilità della crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3) o crittografia lato server con chiavi KMS (). AWS SSE-KMS Se devi utilizzare la SSE-C crittografia in un nuovo bucket, puoi creare il nuovo bucket e quindi abilitare l'uso della crittografia in una richiesta separata. SSE-C PutBucketEncryption

Esempio

```
aws s3api create-bucket \
bucket amzn-s3-demo-bucket \
region us-east-1 \

aws s3api put-bucket-encryption \
-- bucket amzn-s3-demo-bucket \
-- server-side-encryption-configuration \
'{ \Rules\: [{
  {
    \ApplyServerSideEncryptionByDefault\: {
      \SSEAlgorithm\: \AES256\,
    },
    \BlockedEncryptionTypes\: [
      \EncryptionType\: \NONE\
    ]
  }
}]
}'
```

Note

È necessario disporre dell'`s3:PutEncryptionConfiguration` autorizzazione per chiamare l'`PutBucketEncryptionAPI`.

5. In che modo il blocco SSE-C influisce sulle richieste al mio bucket?

Quando SSE-C è bloccato per un bucket `PutObject` `CopyObject` `PostObject`, qualsiasi richiesta di caricamento o replica in più parti che specificano la SSE-C crittografia verrà rifiutata con un errore HTTP 403. `AccessDenied`

Protezione dei dati con la crittografia lato client

Client-side la crittografia è l'atto di crittografare i dati a livello locale per garantirne la sicurezza in transito e a riposo. Per crittografare gli oggetti prima di inviarli ad Amazon S3, utilizza il client di crittografia Amazon S3. Quando i tuoi oggetti sono crittografati in questo modo, i tuoi oggetti non vengono esposti a terze parti, tra cui AWS. Amazon S3 riceve i tuoi oggetti già crittografati e non ha un ruolo nella crittografia o decrittografia degli oggetti. Puoi utilizzare sia il client di crittografia Amazon S3 che la [crittografia lato server](#) per crittografare i tuoi dati. Quando invii oggetti crittografati ad Amazon S3, non vengono riconosciuti come crittografati e vengono rilevati solo gli oggetti tipici.

Il client di crittografia Amazon S3 funge da intermediario tra te e Amazon S3. Dopo aver creato l'istanza del client di crittografia Amazon S3, i tuoi oggetti vengono automaticamente crittografati e decrittati come parte delle richieste PutObject e GetObject di Amazon S3. I tuoi oggetti sono tutti crittografati con una chiave di dati univoca. Il client di crittografia Amazon S3 non utilizza né interagisce con le chiavi bucket, anche se si specifica una chiave KMS come chiave di wrapping.

La Guida per gli sviluppatori del client di crittografia Amazon S3 si concentra sulle versioni 3.0 e successive del client di crittografia Amazon S3. Per ulteriori informazioni, consulta [Cos'è il client di crittografia Amazon S3](#) nella Guida per gli sviluppatori di Client di crittografia Amazon S3.

Per ulteriori informazioni sulle versioni precedenti del client Amazon S3 Encryption, consulta la AWS SDK Developer Guide per il tuo linguaggio di programmazione.

- [AWS SDK per Java](#)
- [AWS SDK per .NET](#)
- [AWS SDK per Go](#)
- [AWS SDK per PHP](#)
- [AWS SDK per Ruby](#)
- [AWS SDK per C++](#)

Protezione dei dati in transito con crittografia

Amazon S3 supporta i protocolli HTTP e HTTPS per la trasmissione dei dati. HTTP trasmette i dati in testo normale, mentre HTTPS aggiunge un livello di sicurezza crittografando i dati utilizzando Transport Layer Security (TLS). Il protocollo TLS protegge da intercettazioni, manomissioni di dati e attacchi man-in-the-middle. Sebbene il traffico HTTP sia accettato, la maggior parte delle

implementazioni utilizza la crittografia in transito con HTTPS e TLS per proteggere i dati mentre viaggiano tra i client e Amazon S3.

Supporto per TLS 1.2 e TLS 1.3

Amazon S3 supporta TLS 1.2 e TLS 1.3 per le connessioni HTTPS su tutti gli endpoint API per tutti. Regioni AWS S3 negozia automaticamente la protezione TLS più potente supportata dal software client e dall'endpoint S3 a cui stai accedendo. AWS Gli strumenti attuali (2014 o versioni successive), inclusi gli AWS SDK, utilizzano AWS CLI automaticamente TLS 1.3 senza che sia richiesta alcuna azione da parte dell'utente. È possibile ignorare questa negoziazione automatica tramite le impostazioni di configurazione del client per specificare una particolare versione TLS se è necessaria la retrocompatibilità con TLS 1.2. Quando si utilizza TLS 1.3, è possibile configurare facoltativamente un exchange ibrido di chiavi post-quantistiche (ML-KEM) per effettuare richieste di resistenza quantistica ad Amazon S3. Per ulteriori informazioni, consulta [the section called “ PQ-TLS Configurare il client”](#).

Note

TLS 1.3 è supportato in tutti gli endpoint S3, ad eccezione di Amazon S3 e Access Points. AWS PrivateLink Multi-Region

Monitoraggio dell'utilizzo di TLS

Puoi utilizzare i log di accesso al server Amazon S3 o AWS CloudTrail per monitorare le richieste ai bucket Amazon S3. Entrambe le opzioni di registrazione registrano la versione TLS e la suite di crittografia utilizzate in ciascuna richiesta.

- Log di accesso al server Amazon S3: la registrazione degli accessi al server fornisce record dettagliati per le richieste effettuate a un bucket. Ad esempio, le informazioni del log di accesso possono essere utili nei controlli di accesso e di sicurezza. Per ulteriori informazioni, consulta [Formato del log di accesso al server Amazon S3](#).
- AWS CloudTrail— [AWS CloudTrail](#) è un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o servizio. AWS CloudTrail acquisisce tutte le chiamate API per Amazon S3 come eventi. Per ulteriori informazioni, consulta [Eventi Amazon S3 CloudTrail](#).

Applicazione della crittografia in transito

È una best practice di sicurezza applicare la crittografia dei dati in transito verso Amazon S3. È possibile imporre la HTTPS-only comunicazione o l'uso di una versione TLS specifica tramite vari meccanismi di policy. Queste includono le politiche IAM basate sulle risorse per i bucket S3 ([politiche dei bucket](#)), le [politiche di controllo dei servizi \(SCP\)](#), le [politiche di controllo delle risorse \(RCP\)](#) e le politiche [sugli endpoint VPC](#).

Esempi di politiche bucket per l'applicazione della crittografia in transito

Puoi utilizzare la chiave [condizionale S3](#) `s3:TlsVersion` per limitare l'accesso ai bucket Amazon S3 in base alla versione TLS utilizzata dal client. Per ulteriori informazioni, consulta [Esempio 6: Richiesta di una versione TLS minima](#).

Example policy del bucket che applica TLS 1.3 utilizzando la chiave di condizione **S3:TlsVersion**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyInsecureConnections",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ],
      "Condition": {
        "NumericLessThan": {
          "s3:TlsVersion": "1.3"
        }
      }
    }
  ]
}
```

Puoi utilizzare la chiave di condizione `aws:SecureTransport` [globale](#) nella tua policy del bucket S3 per verificare se la richiesta è stata inviata tramite HTTPS (TLS). A differenza dell'esempio precedente, questa condizione non verifica una versione TLS specifica. Per ulteriori informazioni, consulta [Limitare l'accesso solo alle richieste HTTPS](#).

Example policy bucket che applica HTTPS utilizzando la chiave di condizione **aws: global SecureTransport**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictToTLSRequestsOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      },
      "Principal": "*"
    }
  ]
}
```

Politica di esempio basata su entrambe le chiavi e altri esempi

È possibile utilizzare entrambi i tipi di chiavi di condizione negli esempi precedenti in un'unica policy. Per ulteriori informazioni e approcci di applicazione aggiuntivi, consulta l'articolo del blog di AWS Storage [Enforcement encryption in transit with TLS1.2 or higher with Amazon S3](#).

Utilizzo del TLS post-quantistico ibrido con Amazon S3

Amazon S3 supporta un'opzione ibrida di scambio di chiavi post-quantistiche per il protocollo di crittografia di rete TLS. Puoi utilizzare questa opzione TLS quando effettui richieste agli endpoint Amazon S3 utilizzando TLS 1.3. Le classiche suite di crittografia supportate da S3 per le sessioni TLS rendono impossibili gli attacchi di forza bruta ai meccanismi di scambio di chiavi con la tecnologia attuale. Tuttavia, se in futuro un computer quantistico rilevante dal punto di vista crittografico diventerà pratico, le classiche suite di crittografia utilizzate nei meccanismi di scambio di chiavi TLS saranno suscettibili a questi attacchi. Al momento, il settore è orientato allo scambio ibrido di chiavi post-quantistico che combina elementi classici e post-quantistici per garantire che la connessione TLS sia almeno altrettanto forte di quanto lo sarebbe con le suite di crittografia

classiche. Amazon S3 supporta l'ibrido, in conformità con le specifiche standard del settore PQ-TLS, oggi. IANA

Se stai sviluppando applicazioni che si basano sulla riservatezza a lungo termine dei dati trasmessi tramite una connessione TLS, dovresti prendere in considerazione un piano di migrazione alla crittografia post-quantistica prima che i computer quantistici su larga scala diventino disponibili all'uso. Come parte del modello di responsabilità condivisa, S3 abilita la crittografia quantistica sicura sui nostri endpoint di servizio. Man mano che browser e applicazioni si PQ-TLS abilitano, S3 sceglierà la configurazione più potente possibile per proteggere i dati in transito.

Tipi di endpoint supportati e Regioni AWS

Post-quantum TLS per Amazon S3 è disponibile in tutti. Regioni AWS Per un elenco degli endpoint S3 per ciascuno Regione AWS, consulta gli endpoint e le quote di [Amazon Simple Storage Service nel](#). Riferimenti generali di Amazon Web Services

Note

Il TLS ibrido post-quantistico è supportato per tutti gli endpoint S3 ad eccezione di Amazon S3, Access Points e S3 AWS PrivateLink Vectors. Multi-Region

Utilizzo del TLS post-quantistico ibrido con Amazon S3

È necessario configurare il client che invia richieste ad Amazon S3 per supportare il TLS ibrido post-quantistico. Quando configuri l'ambiente di test o gli ambienti di produzione del tuo client HTTP, tieni presente le seguenti informazioni:

Crittografia in transito

Il TLS ibrido post-quantistico viene utilizzato solo per la crittografia in transito. Questo protegge i tuoi dati mentre viaggiano dal tuo client all'endpoint S3. Questo nuovo supporto, combinato con la crittografia lato server di Amazon S3 (di default) che utilizza AES-256 algoritmi, offre ai clienti la crittografia quantistica resistente sia in transito che a riposo. Per ulteriori informazioni sulla crittografia lato server in Amazon S3, consulta Proteggere i dati con la crittografia lato server. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html>

Client supportati

L'uso del TLS ibrido post-quantistico richiede l'utilizzo di un client che supporti questa funzionalità. AWS Gli SDK e gli strumenti hanno funzionalità e configurazioni crittografiche che differiscono

a seconda dei linguaggi e dei runtime. Per saperne di più sulla crittografia post-quantistica per strumenti specifici, vedi Abilitazione del TLS post-quantistico ibrido. <https://docs.aws.amazon.com/payment-cryptography/latest/userguide/pqtls-details.html>

 Note

PQ-TLS i dettagli sullo scambio delle chiavi per le richieste ad Amazon S3 non sono disponibili negli eventi o nei AWS CloudTrail log di accesso al server S3.

Scopri di più sul TLS post-quantistico

Per ulteriori informazioni sull'uso del TLS post-quantistico ibrido, consulta le seguenti risorse.

- Per ulteriori informazioni sulla crittografia post-quantistica AWS, inclusi collegamenti a post di blog e documenti di ricerca, vedi Cryptography for. [Post-Quantum AWS](#)
- Per informazioni su s2n-tls, consultare [Introduzione di s2n-tls, una nuova implementazione TLS open source](#) e [Utilizzo di s2n-tls](#).
- Per informazioni sul client HTTP AWS Common Runtime, consulta [Configurazione del client AWS CRT-based](#) HTTP nella Guida per gli sviluppatori. AWS SDK for Java 2.x
- Per informazioni sul progetto di crittografia post-quantistica presso il National Institute for Standards and Technology (NIST), vedere Cryptography. [Post-Quantum](#)
- Per informazioni sulla standardizzazione della crittografia post-quantistica del NIST, vedere NIST Cryptography Standardization. [Post-Quantum](#)

Configurazione del TLS ibrido post-quantistico per il tuo cliente

Per utilizzarlo PQ-TLS con Amazon S3, devi configurare il tuo client per supportare algoritmi di scambio di chiavi post-quantistico. Assicurati inoltre che il tuo cliente supporti l'approccio ibrido, che combina la tradizionale crittografia a curva ellittica con algoritmi post-quantistici come (Key Encapsulation Mechanism). ML-KEM Module-Lattice-Based

La configurazione specifica dipende dalla libreria client e dal linguaggio di programmazione. Per ulteriori informazioni, vedere [Abilitazione del TLS post-quantistico ibrido](#).

Esempio di configurazione del client: AWS SDK per Java 2

In questa procedura, aggiungi una dipendenza Maven per il client HTTP AWS Common Runtime. Quindi, configura un client HTTP che preferisca il protocollo TLS post-quantistico. Quindi, crea un client Amazon S3 che utilizzi il client HTTP.

Note

Il AWS Common Runtime HTTP Client, disponibile in anteprima, è diventato disponibile a livello generale nel febbraio 2023. In tale versione, la classe `TlsCipherPreference` e il parametro del metodo `tlsCipherPreference()` vengono sostituiti dal parametro del metodo `postQuantumTlsEnabled()`. Se stavi usando questo esempio durante l'anteprima, devi aggiornare il codice.

1. Aggiungi il client AWS Common Runtime alle tue dipendenze Maven. Si consiglia di utilizzare l'ultima versione disponibile.

Ad esempio, questa istruzione aggiunge la versione 2.30.22 del client AWS Common Runtime alle dipendenze Maven.

```
<dependency>
  <groupId>software.amazon.awssdk</groupId>
  <artifactId>aws-crt-client</artifactId>
  <version>2.30.22</version>
</dependency>
```

2. Per abilitare le suite ibride di cifratura post-quantistica, aggiungile al tuo progetto e inizializzalo. AWS SDK for Java 2.x Quindi abilita le suite di crittografia post-quantistica ibrida come mostrato nell'esempio seguente.

Questo codice utilizza il parametro `postQuantumTlsEnabled()` method per configurare un client HTTP di runtime [AWS comune](#) che preferisce la suite di crittografia post-quantistica ibrida consigliata, ECDH con. ML-KEM Quindi utilizza il client HTTP configurato per creare un'istanza del client asincrono Amazon S3, [S3AsyncClient](#). Una volta completato questo codice, tutte le [richieste API di](#) Amazon S3 sull'istanza utilizzano un TLS post-quantistico ibrido. `S3AsyncClient`

⚠ Important

A partire dalla versione 2.35.11, i chiamanti non devono più configurare per abilitare il TLS ibrido post-quantistico per il cliente `.postQuantumTlsEnabled(true)`. Tutte le versioni successive alla v2.35.11 abilitano il TLS post-quantistico per impostazione predefinita.

```
// Configure HTTP client
SdkAsyncHttpClient awsCrtHttpClient = AwsCrtAsyncHttpClient.builder()
    .postQuantumTlsEnabled(true)
    .build();

// Create the Amazon S3 async client
S3AsyncClient s3Async = S3AsyncClient.builder()
    .httpClient(awsCrtHttpClient)
    .build();
```

3. Testa le tue chiamate Amazon S3 con un TLS post-quantistico ibrido.

Quando chiami le operazioni API di Amazon S3 sul client Amazon S3 configurato, le chiamate vengono trasmesse all'endpoint Amazon S3 utilizzando un TLS post-quantistico ibrido. Per testare la tua configurazione, chiama un'API Amazon S3, ad esempio. [ListBuckets](#)

```
ListBucketsResponse reponse = s3Async.listBuckets();
```

Testa la tua configurazione TLS ibrida post-quantistica

Valuta la possibilità di eseguire i seguenti test con suite di crittografia ibride sulle tue applicazioni che chiamano Amazon S3.

- Eseguire test di carico e benchmark. Le suite di crittografia ibrida funzionano in modo diverso rispetto agli algoritmi di scambio di chiavi tradizionali. Potrebbe essere necessario modificare i timeout della connessione per consentire tempi di handshake più lunghi. Se stai eseguendo all'interno di una AWS Lambda funzione, estendi l'impostazione del timeout di esecuzione.
- Provare a connettersi da posizioni diverse. A seconda del percorso di rete utilizzato dalla richiesta, è possibile scoprire che host intermedi, proxy o firewall con deep packet inspection (DPI) bloccano

la richiesta. Ciò potrebbe derivare dall'utilizzo delle nuove suite di crittografia nella [ClientHello](#) parte dell'handshake TLS o dai messaggi di scambio di chiavi più grandi. In caso di difficoltà con la risoluzione di questi problemi, contattare il team di sicurezza o gli amministratori IT per aggiornare la configurazione pertinente e sbloccare le nuove suite di crittografia TLS.

Riservatezza del traffico Internet

Questo argomento descrive come Amazon S3 protegge le connessioni dal servizio ad altri percorsi.

Traffico tra servizio e applicazioni e client locali

Le seguenti connessioni possono essere combinate AWS PrivateLink per fornire connettività tra la rete privata e: AWS

- Una connessione AWS Site-to-Site VPN. Per ulteriori informazioni, vedi [Che cos'è AWS Site-to-Site VPN?](#)
- Una Direct Connect connessione. Per ulteriori informazioni, vedi [Che cos'è Direct Connect?](#)

L'accesso ad Amazon S3 tramite la rete avviene tramite API AWS pubblicate. I client devono supportare Transport Layer Security (TLS) 1.2. Consigliamo di utilizzare TLS 1.3 con scambio ibrido di chiavi post-quantistiche. I clienti devono inoltre supportare le suite di crittografia con Perfect Forward Secrecy (PFS), come Ephemeral (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman La maggior parte dei sistemi moderni come Java 7 e versioni successive, supporta tali modalità. Inoltre, è necessario firmare le richieste utilizzando un ID chiave di accesso e la chiave di accesso segreta associate a un principale IAM, oppure è possibile utilizzare [Servizio di token di sicurezza AWS \(STS\)](#) per generare le credenziali di sicurezza temporanee per firmare le richieste.

Traffico tra AWS risorse nella stessa regione

Un endpoint Virtual Private Cloud (VPC) Amazon S3 è un'entità logica all'interno di un VPC che consente la connettività solo ad Amazon S3 Il VPC instrada le richieste ad Amazon S3 e le risposte al VPC. Per ulteriori informazioni, consulta [Endpoint VPC](#) nella Guida per l'utente di VPC. Per policy del bucket di esempio che puoi utilizzare per controllare l'accesso ai bucket S3 da endpoint VPC, consulta [Controllo dell'accesso dagli endpoint VPC con policy di bucket](#).

AWS PrivateLink per Amazon S3

Con AWS PrivateLink Amazon S3, puoi effettuare il provisioning degli endpoint VPC di interfaccia (endpoint di interfaccia) nel tuo cloud privato virtuale (VPC). Questi endpoint sono direttamente accessibili dalle applicazioni locali tramite VPN e/o in un peering diverso Direct Connect tramite VPC. Regione AWS

Gli endpoint di interfaccia sono rappresentati da una o più interfacce di rete elastiche (ENI) a cui vengono assegnati indirizzi IP privati dalle sottoreti nel VPC. Le richieste ad Amazon S3 tramite gli endpoint di interfaccia rimangono nella rete Amazon. Puoi anche accedere agli endpoint di interfaccia nel tuo VPC da applicazioni locali tramite `or ()`. AWS Direct Connect AWS Virtual Private Network Site-to-Site VPN Per ulteriori informazioni su come connettere il VPC alla rete on-premises, consulta la [Guida per l'utente di Direct Connect](#) e la [Guida per l'utente di AWS Site-to-Site VPN](#).

Per informazioni sulla creazione di endpoint di interfaccia, consulta [Endpoint VPC di interfaccia \(AWS PrivateLink\)](#) nella Guida di AWS PrivateLink .

Argomenti

- [Tipi di endpoint VPC per Amazon S3](#)
- [Restrizioni e limitazioni di AWS PrivateLink per Amazon S3](#)
- [Creazione di un endpoint VPC](#)
- [Accesso agli endpoint di interfaccia di Amazon S3](#)
- [Tipi di indirizzi IP per endpoint VPC](#)
- [Tipi di IP di record DNS per endpoint VPC](#)
- [DNS privato](#)
- [Accesso ai bucket, ai punti di accesso e alle operazioni API di controllo Amazon S3 dagli endpoint di interfaccia S3](#)
- [Aggiornamento di una configurazione DNS locale](#)
- [Creazione di una policy per l'endpoint VPC per Amazon S3](#)

Tipi di endpoint VPC per Amazon S3

Puoi utilizzare due tipi di endpoint VPC per accedere ad Amazon S3: endpoint gateway ed endpoint di interfaccia (tramite). AWS PrivateLink Un endpoint gateway è un gateway specificato nella tabella di routing per accedere ad Amazon S3 dal tuo VPC tramite la rete. AWS Gli endpoint di interfaccia

estendono la funzionalità degli endpoint gateway utilizzando indirizzi IP privati per indirizzare le richieste ad Amazon S3 dall'interno del tuo VPC, in locale o da un VPC in un altro cloud utilizzando il peering VPC o. Regione AWS AWS Transit Gateway Per ulteriori informazioni, consulta [Che cos'è il peering di VPC?](#) e [Transit Gateway e peering di VPC](#).

Gli endpoint di interfaccia sono compatibili con gli endpoint gateway. Se disponi di un endpoint gateway nel VPC, puoi utilizzare entrambi i tipi di endpoint nello stesso VPC.

Endpoint gateway per Amazon S3	Endpoint di interfaccia per Amazon S3
In entrambi i casi, il traffico di rete rimane sulla rete. AWS	
Uso di indirizzi IP pubblici di Amazon S3	Uso di indirizzi IP privati del tuo VPC per accedere ad Amazon S3
Uso degli stessi nomi DNS di Simple Storage Service (Amazon S3)	Richiesta di nomi DNS di Simple Storage Service (Amazon S3) specifici per endpoint
Non consente l'accesso da on-premise	Consente l'accesso da On-Premise
Non consentire l'accesso da un altro Regione AWS	Consenti l'accesso da un VPC in un altro Regione AWS utilizzando il peering VPC o AWS Transit Gateway
Non fatturata	Fatturata

Per ulteriori informazioni, consulta Endpoint [Gateway](#) ed endpoint VPC di [interfaccia nella Guida](#). AWS PrivateLink

Restrizioni e limitazioni di AWS PrivateLink per Amazon S3

Le limitazioni del VPC si applicano AWS PrivateLink ad Amazon S3. Per ulteriori informazioni, consulta [Considerazioni di un endpoint di interfaccia](#) e [Quote di AWS PrivateLink](#) nella Guida di AWS PrivateLink . Inoltre, si applicano le limitazioni seguenti:

Gli endpoint di interfaccia per Amazon S3 non supportano quanto segue:

- [Endpoint FIPS \(Federal Information Processing Standard\)](#)
- [Endpoint del sito Web](#)

- [Endpoint globali legacy](#)
- [Endpoint S3 - Regione](#)
- Utilizzo [CopyObject](#) o [UploadPartCopy](#) tra bucket in diversi Regioni AWS
- Transport Layer Security (TLS) 1.0
- Transport Layer Security (TLS) 1.1
- Transport Layer Security (TLS) 1.3
- Transport Layer Security (TLS) ibrida post-quantistica

Creazione di un endpoint VPC

Per creare un endpoint di interfaccia VPC, consulta [Creazione di un endpoint VPC](#) nella Guida AWS PrivateLink . Per creare un endpoint gateway VPC, consulta [Create a gateway endpoint nella Guida. AWS PrivateLink](#)

Accesso agli endpoint di interfaccia di Amazon S3

Quando crei un endpoint di interfaccia, Amazon S3 genera due tipi di nomi DNS S3 specifici dell'endpoint: regionale e zonale.

- Un nome DNS regionale include un ID endpoint VPC univoco, un identificatore di servizio, e nel nome. Regione AWSvpce . amazonaws . com Ad esempio, per l'ID endpoint VPC *vpce-1a2b3c4d*, il nome DNS generato potrebbe essere simile a *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com*.
- I nomi DNS zionali includono la zona di disponibilità, ad esempio *vpce-1a2b3c4d-5e6f-us-east-1a.s3.us-east-1.vpce.amazonaws.com*. Puoi utilizzare questa opzione se l'architettura isola le zone di disponibilità. Ad esempio, puoi utilizzarla per il contenimento degli errori o per ridurre i costi di trasferimento dei dati a livello regionale.

Endpoint-specific I nomi DNS S3 possono essere risolti dal dominio DNS pubblico S3.

Gli endpoint VPC per Amazon S3 supportano diversi tipi di indirizzamento IP, tra cui: IPv4, IPv6 e Dualstack. Consulta [Tipi di indirizzi IP per endpoint VPC](#) e [Tipi di IP di record DNS per endpoint VPC](#).

Tipi di indirizzi IP per endpoint VPC

Gli endpoint VPC per Amazon S3 supportano diversi tipi di indirizzamento IP, tra cui:

- IPv4

Gli endpoint VPC possono essere configurati per utilizzare solo indirizzi IPv4 per la connettività.

- IPv6

Gli endpoint VPC possono essere configurati per utilizzare solo indirizzi IPv6 per la connettività.

- Dual-stack

Gli endpoint VPC possono essere configurati in modalità dual-stack, supportando contemporaneamente gli indirizzi IPv4 e IPv6. Ciò offre la flessibilità necessaria per accedere ad Amazon S3 tramite reti IPv4 o IPv6.

Il tipo di indirizzo IP scelto per l'endpoint VPC dipenderà dai requisiti di rete delle applicazioni e dell'infrastruttura. Le considerazioni possono includere gli schemi di indirizzamento IP utilizzati nel tuo VPC, nelle reti locali e nella connettività Internet verso Amazon S3. Per ulteriori informazioni, consulta i tipi di indirizzi IP per gli endpoint di [interfaccia](#) e gli endpoint [gateway](#) nella guida Amazon Virtual Private Cloud.

Tipi di IP di record DNS per endpoint VPC

A seconda del tipo di indirizzo IP, quando si chiama un endpoint VPC, questo Servizio AWS può restituire A record, record o entrambi AAAA i record. A AAAA È possibile personalizzare i tipi di record restituiti dal AWS servizio modificando il tipo IP del record DNS. La tabella seguente mostra i tipi IP di record DNS supportati e i tipi di indirizzo IP:

Tipi di indirizzo IP supportati	Tipi IP di record DNS
IPv4	IPv4
IPv6	IPv6
Dualstack	Dualstack, IPv4, IPv6, Service-defined

Configurazione del tipo IP di record DNS definito dal servizio per Amazon S3

Se crei un endpoint gateway per Amazon S3 e configuri il tipo di IP del record DNS come definito dal servizio e utilizzi l'endpoint di servizio regionale (ad esempio), Amazon S3 restituisce i record ai tuoi clienti. `s3.us-east-2.amazonaws.com` Al contrario, se crei un endpoint gateway e utilizzi

un endpoint di servizio dual-stack (ad esempio `s3.dualstack.us-east-2.amazonaws.com`) e selezioni il tipo di IP del record DNS come, Amazon S3 restituisce entrambi i record ai tuoi clienti. `service-defined A AAAA`

Allo stesso modo, se crei un endpoint di interfaccia con DNS privato abilitato e scegli il tipo di record DNS definito dal servizio, per l'endpoint di servizio regionale (ad esempio, `s3.us-east-2.amazonaws.com` A Invece, per un endpoint di servizio dualstack (ad esempio, `s3.dualstack.us-east-2.amazonaws.com` A AAAA Per ulteriori informazioni, consulta il tipo di IP del record DNS per gli endpoint di [interfaccia](#) e gli endpoint [gateway nella Guida per l'utente di VPC](#).

La tabella seguente mostra i tipi di IP di record DNS supportati per gli endpoint gateway e di interfaccia:

Tipo di indirizzo IP	Tipi IP di record DNS supportati per gli endpoint S3 Gateway	Tipi IP di record DNS supportati per gli endpoint dell'interfaccia S3
IPv4	IPv4, definito dal servizio*	IPv4
IPv6	IPv6, definito dal servizio*	IPv6
Dualstack	IPv4, IPv6, Dualstack, definito dal servizio*	Dualstack*, IPv4, IPv6, definito dal servizio

* Rappresenta il tipo IP di record DNS predefinito.

Per abilitare la connettività IPv6 su un gateway o endpoint di interfaccia S3 esistente, aggiorna il tipo di indirizzo IP dell'endpoint a **Dualstack**. Una volta aggiornato, Amazon S3 aggiorna automaticamente le tabelle di routing con gli indirizzi IPv6 per gli endpoint del gateway. Quindi puoi utilizzare l'endpoint del servizio dualstack, ad esempio, e Amazon S3 restituirà sia `s3.dualstack.us-east-2.amazonaws.com` i record per le query DNS S3 dualstack. A AAAA Se desideri utilizzare IPV6 con l'endpoint di servizio regionale, ad esempio, modifica il tipo di indirizzo IP dell'endpoint su `s3.us-east-2.amazonaws.com`; e il tipo IP del record DNS su **Dualstack**. **Dualstack** Quindi Amazon S3 restituirà entrambi i A AAAA record per le query DNS S3 regionali.

Considerazioni

- Se l'endpoint del gateway ha la configurazione predefinita del tipo di indirizzo IP as IPv4 e del record DNS come `IPservice-defined`, allora l'endpoint di servizio dualstack (ad esempio `s3.dualstack.us-east-2.amazonaws.com`), il traffico che utilizza i AAAA record non verrà indirizzato attraverso l'endpoint del gateway. Questo traffico verrà invece eliminato o indirizzato su un percorso, se presente. IPv6-compatible Ad esempio, se il tuo cloud privato virtuale (VPC) dispone di un gateway Internet, in questo scenario il traffico IPv6 verrà indirizzato sul gateway Internet del tuo VPC. Se desideri assicurarti che il traffico venga sempre indirizzato su un endpoint VPC, puoi utilizzare una policy sui bucket di Amazon S3 che limita l'accesso a un bucket specifico se non viene utilizzato un endpoint VPC specificato. Per ulteriori informazioni, consulta [Limitare l'accesso a un endpoint VPC specifico](https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html#example-bucket-policies-restrict-access-vpc-endpoint). <https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html#example-bucket-policies-restrict-access-vpc-endpoint>
- Se l'endpoint di interfaccia ha la configurazione predefinita del tipo di indirizzo IP, che è IPv4, e il tipo di IP del record DNS è IPv4, gli endpoint di servizio dualstack, ad esempio, `s3.dualstack.us-east-2.amazonaws.com` Il traffico che utilizza i AAAA record A o degli endpoint del servizio dualstack non verrà instradato attraverso l'endpoint dell'interfaccia. Questo traffico verrà invece eliminato o indirizzato su un altro percorso compatibile, se presente.
- La creazione o la modifica di un endpoint gateway con un tipo IP di record DNS diverso da quello definito dal servizio richiede che sia gli attributi VPC che quelli `enableDnsHostnames` VPC siano `enableDnsSupport` impostati su `true`.

DNS privato

Le opzioni DNS private per gli endpoint di interfaccia VPC semplificano l'instradamento del traffico S3 sugli endpoint VPC e consentono di sfruttare il percorso di rete più economico disponibile per l'applicazione. Puoi utilizzare le opzioni DNS private per indirizzare il traffico regionale S3 senza aggiornare i client S3 per usare i nomi DNS specifici degli endpoint di interfaccia o gestire l'infrastruttura DNS. Con i nomi DNS privati abilitati, le query DNS regionali S3 vengono risolte negli indirizzi IP privati dei seguenti endpoint: AWS PrivateLink

- Endpoint di bucket regionale (ad esempio, `s3.us-east-1.amazonaws.com`)
- Endpoint di controllo (ad esempio, `s3-control.us-east-1.amazonaws.com`)

- Endpoint di punto di accesso (ad esempio, `s3-accesspoint.us-east-1.amazonaws.com`)

Se hai un endpoint gateway nel tuo VPC, puoi indirizzare automaticamente le richieste in entrata nel VPC all'endpoint gateway S3 esistente e le richieste on-premise all'endpoint di interfaccia. Questo approccio consente di ottimizzare i costi di rete utilizzando gli endpoint gateway, che non vengono fatturati, per il traffico in entrata nel VPC. Le tue applicazioni locali possono essere utilizzate AWS PrivateLink con l'aiuto dell'endpoint Resolver in entrata. Amazon fornisce un server DNS chiamato il Route 53 Resolver per il tuo VPC. Un endpoint del resolver in entrata inoltra le query DNS dalla rete on-premise al Route 53 Resolver.

Important

Per sfruttare il percorso di rete più economico quando si utilizza Abilita DNS privato solo per gli endpoint in entrata, è necessario che nel cloud privato virtuale sia presente un endpoint gateway. La presenza di un endpoint gateway aiuta a garantire che il traffico in entrata nel VPC venga sempre indirizzato sulla rete privata AWS quando è selezionata l'opzione Abilita DNS privato solo per gli endpoint in entrata. È necessario mantenere questo endpoint gateway se è selezionata l'opzione Abilita DNS privato solo per gli endpoint in entrata. Se desideri eliminare l'endpoint gateway, devi prima deselezionare Abilita DNS privato solo per gli endpoint in entrata.

Se desideri aggiornare un endpoint di interfaccia esistente su Abilita DNS privato solo per gli endpoint in entrata verifica innanzitutto che il tuo VPC disponga di un endpoint gateway S3. Per ulteriori informazioni sugli endpoint gateway e sulla gestione dei nomi DNS privati, consulta rispettivamente [Endpoint gateway del VPC](#) e [Gestione dei nomi DNS](#) nella Guida di AWS PrivateLink .

Quando si abilita il DNS privato solo per il resolver in ingresso, l'endpoint del gateway deve corrispondere a quello `dnsRecordIpType` dell'endpoint di interfaccia o essere definito dal servizio.

L'opzione Abilita DNS privato solo per gli endpoint in entrata è disponibile solo per i servizi che supportano gli endpoint gateway.

Per ulteriori informazioni sulla creazione di un endpoint VPC che utilizza Abilita DNS privato solo per gli endpoint in entrata, consulta [Creare un endpoint di interfaccia](#) nella Guida di AWS PrivateLink .

Utilizzo della console VPC

Nella console sono disponibili due opzioni: Abilita nome DNS e Abilita DNS privato solo per gli endpoint in entrata. L'attivazione del nome DNS è un'opzione supportata da AWS PrivateLink. Con l'opzione Abilita nome DNS puoi utilizzare la connettività privata di Amazon ad Amazon S3, effettuando richieste ai nomi DNS predefiniti degli endpoint pubblici. Quando questa opzione è abilitata, i clienti possono sfruttare il percorso di rete più economico disponibile per la loro applicazione.

Quando abiliti i nomi DNS privati su un endpoint di interfaccia VPC esistente o nuovo per Amazon S3, l'opzione Abilita DNS privato solo per gli endpoint in entrata è selezionata per impostazione predefinita. Se questa opzione è selezionata, le applicazioni utilizzano solo gli endpoint di interfaccia per il traffico on-premise. Il traffico VPC in entrata utilizza automaticamente gli endpoint gateway più economici. In alternativa, puoi deselezionare Abilita DNS privato solo per gli endpoint in entrata per indirizzare tutte le richieste S3 sull'endpoint di interfaccia.

Usando il AWS CLI

Se non specifichi un valore per `PrivateDnsOnlyForInboundResolverEndpoint`, viene usata l'impostazione predefinita `true`. Tuttavia, prima che il cloud privato virtuale applichi le impostazioni, esegue un controllo per assicurarsi che nel cloud privato VPC sia presente un endpoint gateway. Se nel cloud privato virtuale è presente un endpoint gateway, la chiamata ha esito positivo. In caso contrario, viene visualizzato il seguente messaggio di errore:

Per `PrivateDnsOnlyForInboundResolverEndpoint` impostarlo su `true`, il VPC *vpce_id* deve disporre di un endpoint gateway per il servizio.

Per un nuovo endpoint di interfaccia VPC

Usa gli attributi `private-dns-enabled` e `dns-options` per abilitare il DNS privato tramite la linea di comando. L'opzione `PrivateDnsOnlyForInboundResolverEndpoint` nell'attributo `dns-options` deve essere impostata su `true`. Sostituisci *user input placeholders* con le informazioni appropriate.

```
aws ec2 create-vpc-endpoint \
--region us-east-1 \
--service-name s3-service-name \
--vpc-id client-vpc-id \
--subnet-ids client-subnet-id \
--vpc-endpoint-type Interface \
--private-dns-enabled \
```

```
--ip-address-type ip-address-type \  
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true \  
--security-group-ids client-sg-id
```

Per un endpoint VPC esistente

Se desideri utilizzare il DNS privato per un endpoint VPC esistente, usa il seguente comando di esempio e sostituisci *user input placeholders* con le tue specifiche informazioni.

```
aws ec2 modify-vpc-endpoint \  
--region us-east-1 \  
--vpc-endpoint-id client-vpc-id \  
--private-dns-enabled \  
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=false
```

Se desideri aggiornare un endpoint VPC esistente per abilitare il DNS privato solo per il risolutore in entrata, usa il seguente esempio e sostituisci i valori di esempio con le tue specifiche informazioni.

```
aws ec2 modify-vpc-endpoint \  
--region us-east-1 \  
--vpc-endpoint-id client-vpc-id \  
--private-dns-enabled \  
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true
```

Accesso ai bucket, ai punti di accesso e alle operazioni API di controllo Amazon S3 dagli endpoint di interfaccia S3

Puoi utilizzare gli AWS SDK AWS CLI o per accedere ai bucket, ai punti di accesso S3 e alle operazioni dell'API Amazon S3 Control tramite gli endpoint dell'interfaccia S3.

Nell'immagine seguente viene illustrata la scheda Dettagli della console VPC, in cui è possibile trovare il nome DNS di un endpoint VPC. In questo esempio, l'ID endpoint VPC (vpce-id) è `vpce-0e25b8cdd720f900e` e il nome DNS è `*.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com`.

Details	Subnets	Security Groups	Policy	Notifications	Tags
Endpoint ID vpce-0e25b8cdd720f900e Status available Creation time January 8, 2021 at 1:30:11 AM UTC-8 Endpoint type Interface					VPC ID vpc-0c0ccb9d87b1734bd VPCStack VPC Status message Service name com.amazonaws.us-east-1.s3 DNS names *.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com (Z7HUB22UULQXV)

Quando usi il nome DNS per accedere a una risorsa, sostituiscilo con il valore appropriato. * I valori appropriati da utilizzare al posto di * sono i seguenti:

- bucket
- accesspoint
- control

Ad esempio, per accedere a un bucket, usa un nome DNS simile al seguente:

`bucket.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com`

Per esempi di come utilizzare i nomi DNS per accedere a bucket, punti di accesso e operazioni API di controllo Amazon S3, consulta le sezioni [AWS CLI esempi](#) e [AWS Esempi di SDK](#).

Per ulteriori informazioni su come visualizzare i nomi DNS specifici degli endpoint, consulta [Visualizzazione della configurazione dei nomi DNS privati del servizio endpoint](#) nella Guida per l'utente di VPC.

AWS CLI esempi

Per accedere ai bucket S3, ai punti di accesso S3 o alle operazioni dell'API Amazon S3 Control tramite gli endpoint dell'interfaccia S3 nei AWS CLI comandi, utilizza i parametri `and. --region --endpoint-url`

Esempio: utilizzo dell'URL dell'endpoint per elencare gli oggetti nel bucket

Nell'esempio seguente, sostituisci il nome bucket *my-bucket*, Regione *us-east-1* e il nome DNS dell'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* con le tue informazioni.

```
aws s3 ls s3://my-bucket/ --region us-east-1 --endpoint-url
https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
```

Esempio: utilizzo dell'URL dell'endpoint per elencare gli oggetti da un punto di accesso

- Metodo 1: utilizzo del nome della risorsa Amazon (ARN) del punto di accesso con l'endpoint del punto di accesso

Sostituisci l'ARN *us-east-1:123456789012:accesspoint/accesspointexamplename*, la Regione *us-east-1* e l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* con le informazioni appropriate.

```
aws s3api list-objects-v2 --bucket arn:aws:s3:us-east-1:123456789012:accesspoint/
accesspointexamplename --region us-east-1 --endpoint-url
https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
```

Se non riesci a eseguire correttamente il comando, aggiorna la versione più recente e AWS CLI riprova. Per ulteriori informazioni sulle istruzioni di aggiornamento, consulta [Istruzioni per l'installazione o l'aggiornamento all'ultima versione della AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface .

- Metodo 2: utilizzo dell'alias del punto di accesso con l'endpoint bucket regionale

Nell'esempio seguente, sostituisci l'alias del punto di accesso *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*, la Regione *us-east-1* e l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* con le informazioni appropriate.

```
aws s3api list-objects-v2 --
bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias
--region us-east-1 --endpoint-url https://bucket.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com
```

- Metodo 3: utilizzo dell'alias del punto di accesso con l'endpoint del punto di accesso

Innanzitutto, per creare un endpoint S3 con il bucket incluso come parte del nome host, imposta lo stile di indirizzamento su `virtual` per `aws s3api`. Per ulteriori informazioni su AWS `configure`, consulta [File di configurazione e delle credenziali](#) nella Guida per l'utente di AWS Command Line Interface .

```
aws configure set default.s3.addressing_style virtual
```

Quindi, nell'esempio seguente, sostituisci l'alias del punto di accesso *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*, la Regione *us-east-1* e l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-*

east-1.vpce.amazonaws.com con le informazioni appropriate. Per ulteriori informazioni sull'alias del punto di accesso, consulta [Alias del punto di accesso](#).

```
aws s3api list-objects-v2 --  
bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias --  
region us-east-1 --endpoint-url https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-  
east-1.vpce.amazonaws.com
```

Esempio: utilizzo dell'URL dell'endpoint per elencare i processi con un'operazione API di controllo S3

Nell'esempio seguente, sostituisci la Regione *us-east-1*, l'ID endpoint VPC

vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com e l'ID account *12345678* con le informazioni appropriate.

```
aws s3control --region us-east-1 --endpoint-url  
https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com list-jobs --  
account-id 12345678
```

AWS Esempi di SDK

Per accedere ai bucket S3, ai punti di accesso S3 o alle operazioni dell'API Amazon S3 Control tramite gli endpoint dell'interfaccia S3 quando usi gli SDK, aggiorna i tuoi AWS SDK alla versione più recente. Quindi configura i client per utilizzare un URL endpoint per accedere a un bucket, un punto di accesso o un'operazione API di controllo Amazon S3 tramite gli endpoint di interfaccia S3.

SDK for Python (Boto3)

Esempio: utilizzo di un URL endpoint per accedere a un bucket S3

Nell'esempio seguente, sostituisci la Regione *us-east-1* e l'ID endpoint VPC

vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com con le informazioni appropriate.

```
s3_client = session.client(  
    service_name='s3',  
    region_name='us-east-1',  
    endpoint_url='https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'  
)
```

Esempio: utilizzare un URL endpoint per accedere a un punto di accesso S3

Nell'esempio seguente, sostituisci la Regione *us-east-1* e l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* con le informazioni appropriate.

```
ap_client = session.client(
    service_name='s3',
    region_name='us-east-1',
    endpoint_url='https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com'
)
```

Esempio: utilizzo di un URL endpoint per accedere all'API di controllo Amazon S3

Nell'esempio seguente, sostituisci la Regione *us-east-1* e l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* con le informazioni appropriate.

```
control_client = session.client(
    service_name='s3control',
    region_name='us-east-1',
    endpoint_url='https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
)
```

SDK for Java 1.x

Esempio: utilizzo di un URL endpoint per accedere a un bucket S3

Nell'esempio seguente, sostituisci l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* con le informazioni appropriate.

```
// bucket client
final AmazonS3 s3 = AmazonS3ClientBuilder.standard().withEndpointConfiguration(
    new AwsClientBuilder.EndpointConfiguration(
        "https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
        Regions.DEFAULT_REGION.getName()
    )
).build();
List<Bucket> buckets = s3.listBuckets();
```

Esempio: utilizzare un URL endpoint per accedere a un punto di accesso S3

Nell'esempio seguente, sostituisci l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e l'ARN *us-east-1:123456789012:accesspoint/prod* con le informazioni appropriate.

```
// accesspoint client
final AmazonS3 s3accesspoint =
    AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
            "https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
            Regions.DEFAULT_REGION.getName()
        )
    ).build();
ObjectListing objects = s3accesspoint.listObjects("arn:aws:s3:us-east-1:123456789012:accesspoint/prod");
```

Esempio: utilizzo di un URL endpoint per accedere all'operazione API di controllo Amazon S3

Nell'esempio seguente, sostituisci l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* con le informazioni appropriate.

```
// control client
final AWSS3Control s3control =
    AWSS3ControlClient.builder().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
            "https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
            Regions.DEFAULT_REGION.getName()
        )
    ).build();
final ListJobsResult jobs = s3control.listJobs(new ListJobsRequest());
```

SDK for Java 2.x

Esempio: utilizzo di un URL endpoint per accedere a un bucket S3

Nell'esempio seguente, sostituisci l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e la Regione *Region.US_EAST_1* con le informazioni appropriate.

```
// bucket client
Region region = Region.US_EAST_1;
```

```
s3Client = S3Client.builder().region(region)

    .endpointOverride(URI.create("https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com"))
    .build()
```

Esempio: utilizzare un URL endpoint per accedere a un punto di accesso S3

Nell'esempio seguente, sostituisci l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e la Regione *Region.US_EAST_1* con le informazioni appropriate.

```
// accesspoint client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

    .endpointOverride(URI.create("https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com"))
    .build()
```

Esempio: utilizzo di un URL endpoint per accedere all'API di controllo Amazon S3

Nell'esempio seguente, sostituisci l'ID endpoint VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* e la Regione *Region.US_EAST_1* con le informazioni appropriate.

```
// control client
Region region = Region.US_EAST_1;
s3ControlClient = S3ControlClient.builder().region(region)

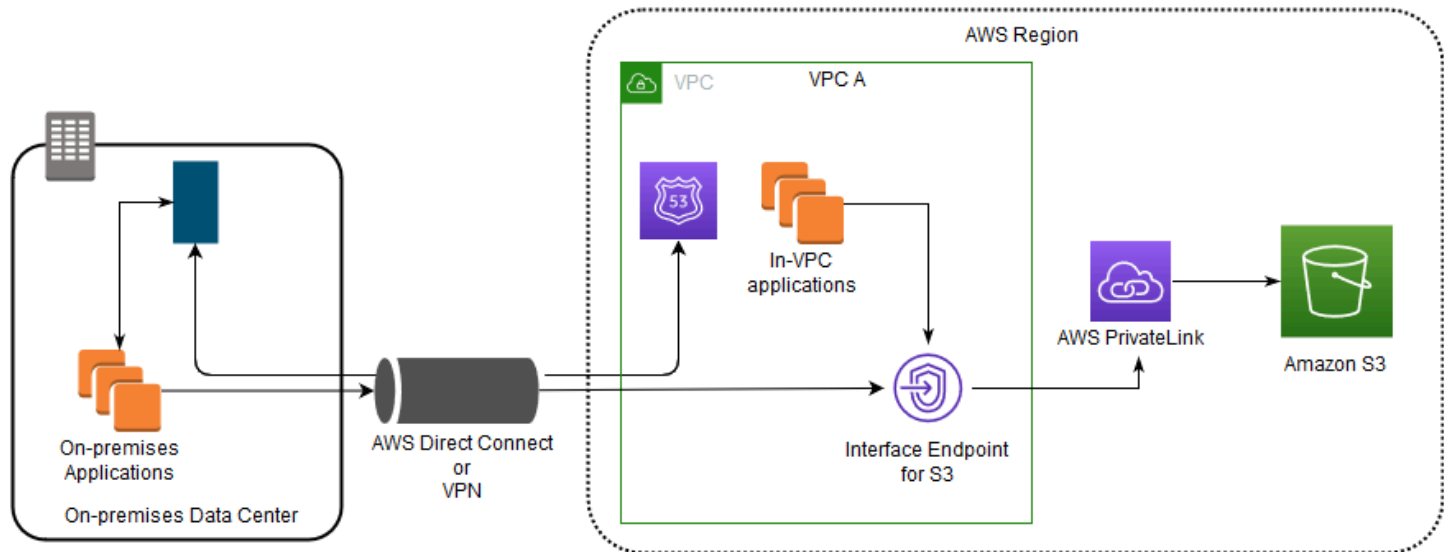
    .endpointOverride(URI.create("https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com"))
    .build()
```

Aggiornamento di una configurazione DNS locale

Quando si utilizzano nomi DNS specifici degli endpoint per accedere agli endpoint di interfaccia per Amazon S3, non è necessario aggiornare il resolver DNS locale. Puoi risolvere il nome DNS specifico dell'endpoint con l'indirizzo IP privato dell'endpoint di interfaccia dal dominio DNS Amazon S3 pubblico.

Utilizzo degli endpoint di interfaccia per accedere ad Amazon S3 senza un endpoint gateway o un gateway Internet nel VPC

Gli endpoint di interfaccia nel VPC possono instradare sia le applicazioni nel VPC che le applicazioni locali ad Amazon S3 sulla rete Amazon, come illustrato nel diagramma seguente.



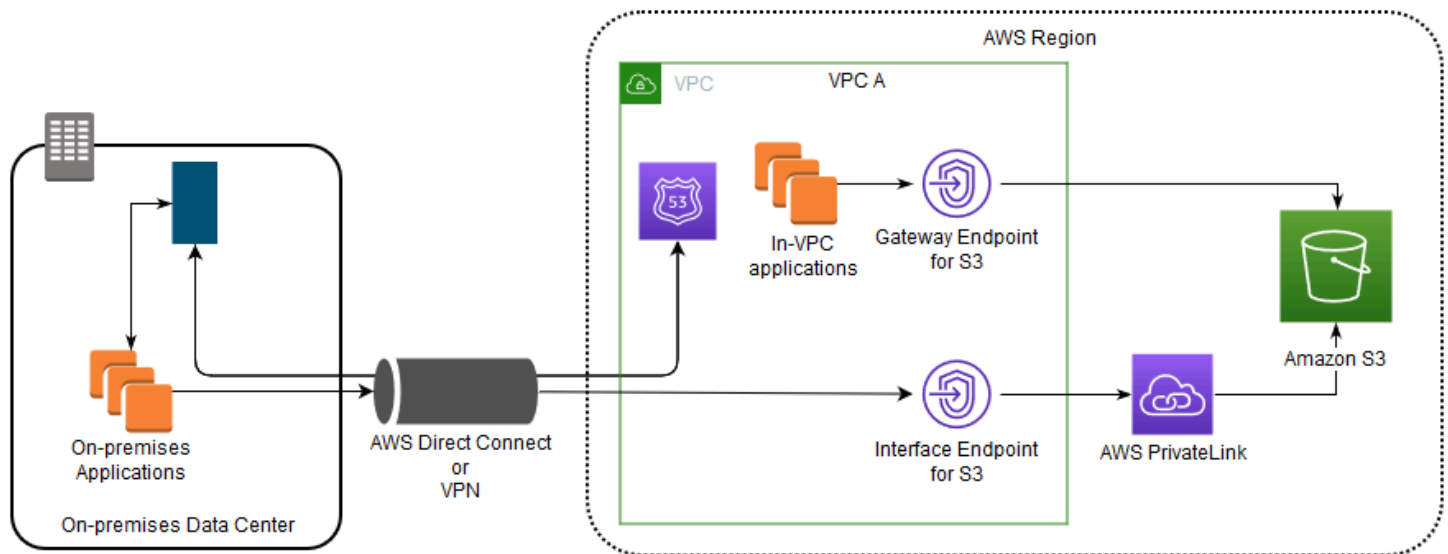
Il diagramma illustra quanto segue:

- La tua rete locale utilizza Direct Connect o si connette Site-to-Site VPN a VPC A.
- Le applicazioni in locale e in VPC A utilizzano nomi DNS specifici degli endpoint per accedere ad Amazon S3 tramite l'endpoint di interfaccia S3.
- On-premises le applicazioni inviano dati all'endpoint dell'interfaccia nel VPC tramite Direct Connect (o). Site-to-Site VPN AWS PrivateLink sposta i dati dall'endpoint dell'interfaccia ad Amazon S3 attraverso la rete. AWS
- In-VPC le applicazioni inviano anche traffico all'endpoint dell'interfaccia. AWS PrivateLink sposta i dati dall'endpoint dell'interfaccia ad Amazon S3 attraverso la rete. AWS

Utilizzo di endpoint gateway e endpoint di interfaccia insieme nello stesso VPC per accedere ad Amazon S3

Puoi creare endpoint di interfaccia e mantenere l'endpoint gateway esistente nello stesso VPC, come illustrato nel diagramma seguente. Con questo approccio consenti alle applicazioni nel VPC di continuare ad accedere ad Amazon S3 tramite l'endpoint gateway senza essere fatturate. Quindi, solo le applicazioni on-premise utilizzerebbero gli endpoint di interfaccia per accedere ad Amazon S3.

Per accedere ad Amazon S3 in questo modo, è necessario aggiornare le applicazioni On-Premise per utilizzare nomi DNS specifici degli endpoint per Amazon S3.



Il diagramma illustra quanto segue:

- On-premises le applicazioni utilizzano nomi DNS specifici degli endpoint per inviare dati all'endpoint dell'interfaccia all'interno del VPC tramite (o). Direct Connect Site-to-Site VPN AWS PrivateLink sposta i dati dall'endpoint dell'interfaccia ad Amazon S3 attraverso la rete. AWS
- Utilizzando i nomi regionali predefiniti di Amazon S3, le applicazioni in VPC inviano i dati all'endpoint gateway che si connette ad Amazon S3 tramite la rete. AWS

Per ulteriori informazioni sugli endpoint gateway, consulta [Endpoint VPC gateway](#) nella Guida per l'utente di VPC.

Creazione di una policy per l'endpoint VPC per Amazon S3

Puoi allegare una policy di endpoint all'endpoint VPC che controlla l'accesso ad Amazon S3. Questa policy specifica le informazioni riportate di seguito:

- Il principio AWS Identity and Access Management (IAM) in grado di eseguire azioni
- Le azioni che possono essere eseguite
- Le risorse sui cui si possono eseguire le azioni

Puoi utilizzare le policy del bucket di Amazon S3 anche per limitare l'accesso a bucket specifici da un endpoint VPC specifico utilizzando la condizione `aws:sourceVpce` nella policy del bucket. Negli esempi seguenti vengono illustrate le policy che limitano l'accesso a un bucket o a un endpoint.

Argomenti

- [Esempio: limitazione dell'accesso a un bucket specifico da un endpoint VPC](#)
- [Esempio: limitazione dell'accesso ai bucket in un account specifico da un endpoint VPC](#)
- [Esempio: limitazione dell'accesso a un endpoint VPC specifico nella policy del bucket S3](#)

Esempio: limitazione dell'accesso a un bucket specifico da un endpoint VPC

Puoi creare una policy di endpoint che limita l'accesso solo a bucket Amazon S3 specifici. Questo tipo di policy è utile se Servizi AWS nel tuo VPC ne sono presenti altri che utilizzano bucket. La seguente policy del bucket limita l'accesso solo a *amzn-s3-demo-bucket1*. Per utilizzare questa policy di endpoint, sostituisci *amzn-s3-demo-bucket1* con il nome del bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909151",
  "Statement": [
    { "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket1",
                  "arn:aws:s3:::amzn-s3-demo-bucket1/*"]
    }
  ]
}
```

Esempio: limitazione dell'accesso ai bucket in un account specifico da un endpoint VPC

Puoi creare una policy sugli endpoint che limiti l'accesso solo ai bucket S3 in uno specifico. Account AWS Per impedire ai client nel VPC di accedere ai bucket di cui non sei proprietario, utilizza la seguente istruzione nella policy di endpoint. Nell'esempio seguente viene creata una policy che limita l'accesso alle risorse di proprietà di un singolo ID Account AWS , **111122223333**.

```
{
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Note

Per specificare l' Account AWS ID della risorsa a cui si accede, puoi utilizzare la chiave `aws:ResourceAccount` o la `s3:ResourceAccount` chiave nella tua policy IAM. Tuttavia, tieni presente che alcuni Servizi AWS si basano sull'accesso ai bucket AWS gestiti. Pertanto, l'utilizzo della chiave `aws:ResourceAccount` o `s3:ResourceAccount` nelle policy IAM potrebbe influire sull'accesso a queste risorse.

Esempio: limitazione dell'accesso a un endpoint VPC specifico nella policy del bucket S3

La seguente policy del bucket Amazon S3 consente l'accesso a un bucket specifico, **amzn-s3-demo-bucket2**, solo dall'endpoint VPC **vpce-1a2b3c4d**. La policy nega l'accesso al bucket se l'endpoint specificato non è in uso. La condizione `aws:sourceVpce` viene utilizzata per specificare

l'endpoint e non richiede un nome della risorsa Amazon (ARN) per la risorsa dell'endpoint VPC, ma solo l'ID dell'endpoint. Per utilizzare questa politica del bucket, sostituisci *amzn-s3-demo-bucket2* e *vpce-1a2b3c4d* con il nome e l'endpoint del bucket.

 Important

- Quando applichi la seguente policy del bucket Amazon S3 per limitare l'accesso solo a determinati endpoint VPC, potresti senza volerlo bloccare l'accesso al bucket. Le policy del bucket che hanno lo scopo di limitare l'accesso del bucket a connessioni originate dall'endpoint VPC possono bloccare tutte le connessioni al bucket. Per informazioni su come risolvere questo problema, consulta [La policy del bucket ha l'ID del VPC o dell'endpoint VPC sbagliato. Come posso correggere la policy in modo da poter accedere al bucket? nel Knowledge Center di Supporto](#).
- Prima di utilizzare la policy di esempio seguente, sostituire l'ID endpoint VPC con un valore appropriato per il caso d'uso. In caso contrario, non sarà possibile accedere al bucket.
- Questa policy disabilita l'accesso alla console al bucket specificato in quanto le richieste della console non provengono dall'endpoint VPC specificato.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket2",
        "arn:aws:s3:::amzn-s3-demo-bucket2/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Per altri esempi di policy, consulta [Endpoint per Amazon S3](#) nella Guida per l'utente di VPC.

Per ulteriori informazioni sulla connettività VPC, consulta le opzioni di [Network-to-VPC connettività](#) nel AWS white paper [Amazon Virtual Private Cloud Connectivity Options](#).

Convalida della conformità per Amazon S3

La sicurezza e la conformità di Amazon S3 vengono valutate da revisori di terze parti nell'ambito di diversi programmi di AWS conformità, tra cui:

- System and Organization Controls (SOC)
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)

AWS fornisce un elenco aggiornato di AWS servizi nell'ambito di specifici programmi di conformità nell'ambito di [AWS Services in Scope by Compliance Program](#).

Third-party i rapporti di audit possono essere scaricati utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Download dei report in AWS Artifact](#).

Per ulteriori informazioni sui programmi di AWS conformità, vedere Programmi di [AWS conformità](#).

La responsabilità della conformità durante l'utilizzo di Amazon S3 è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'organizzazione e dalle leggi e normative in vigore. Se l'utilizzo di Amazon S3 è soggetto alla conformità a standard come HIPAA, PCI o FedRAMP, AWS fornisce alcune risorse utili:

- [Guide introduttive sulla sicurezza e la conformità](#) che illustrano le considerazioni sull'architettura e i passaggi per l'implementazione di ambienti di base incentrati sulla sicurezza e sulla conformità. AWS
- [Architecting for HIPAA Security and Compliance](#) delinea come le aziende utilizzano per aiutarle a soddisfare i requisiti HIPAA. AWS
- [AWS Le risorse sulla conformità](#) forniscono diverse cartelle di lavoro e guide che potrebbero essere applicate al tuo settore e alla tua sede.
- [AWS Config](#) è utile per valutare il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti del settore.
- [AWS Security Hub](#) offre una visione completa dello stato di sicurezza interno AWS e consente di verificare la conformità agli standard e alle best practice del settore della sicurezza.
- [Blocco di oggetti con Object Lock](#) consente di soddisfare i requisiti tecnici degli organi di regolamentazione finanziaria (ad esempio, SEC, FINRA e CFTC) che richiedono storage dei dati WORM (Write Once, Read Many) per alcuni tipi di informazioni su registri e record.

- [Catalogazione e analisi dei dati con Inventario S3](#) permette di svolgere revisioni e creare report sullo stato di replica e crittografia degli oggetti per esigenze aziendali, normative e di conformità.

Resilienza in Amazon S3

L'infrastruttura AWS globale è costruita attorno a regioni e zone di disponibilità. Regioni AWS forniscono zone di disponibilità multiple, fisicamente separate e isolate, collegate con una rete a bassa latenza, alta velocità effettiva e altamente ridondante. Queste zone di disponibilità offrono un modo efficace per progettare e gestire le applicazioni e i database. Sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali. Se hai specificamente bisogno di replicare i tuoi dati su distanze geografiche maggiori, puoi utilizzare [Replica di oggetti all'interno e tra le Regioni](#), che consente la copia automatica e asincrona di oggetti tra bucket in diversi bucket. Regioni AWS

Ciascuno ha più zone di disponibilità. Regione AWS Puoi distribuire le applicazioni tra più zone di disponibilità nella stessa regione per avere maggiore tolleranza ai guasti e una bassa latenza. Le zone di disponibilità sono collegate tra loro con velocissime reti in fibra ottica private, per consentire ai clienti di progettare applicazioni che eseguano il failover su diverse zone di disponibilità senza provocare interruzioni.

Per ulteriori informazioni sulle zone di disponibilità Regioni AWS e sulle zone di disponibilità, vedere Infrastruttura [AWS globale](#).

Oltre all'infrastruttura AWS globale, Amazon S3 offre diverse funzionalità per aiutare a supportare la resilienza dei dati e le esigenze di backup.

Configurazione del ciclo di vita

Una configurazione del ciclo di vita è un insieme di regole che definiscono le operazioni applicate da Amazon S3 a un gruppo di oggetti. Tramite le regole di configurazione del ciclo di vita, è possibile indicare ad Amazon S3 di trasferire gli oggetti in classi di storage meno costose, archivarli o eliminarli. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#).

Funzione Controllo delle versioni

La funzione Controllo delle versioni è un modo per conservare più versioni di un oggetto nello stesso bucket. La funzione Controllo delle versioni può essere impiegata per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Con la funzione Controllo delle versioni si può facilmente eseguire il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Blocco di oggetti in S3

Puoi utilizzare il blocco oggetti S3 per archiviare gli oggetti utilizzando il modello write once, read many (WORM). Utilizzando il blocco oggetti S3, puoi impedire che un oggetto venga eliminato o sovrascritto per un determinato periodo di tempo o in modo indefinito. Il blocco oggetti S3 consente di soddisfare i requisiti normativi che richiedono uno storage WORM o semplicemente di aggiungere un ulteriore livello di protezione contro le modifiche e l'eliminazione degli oggetti. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).

Classi di storage

Amazon S3 offre una gamma di classi di archiviazione tra cui scegliere in base ai requisiti del carico di lavoro. Le classi di Zone-IA storage S3 Standard-IA e S3 One sono progettate per i dati a cui si accede circa una volta al mese e richiedono un accesso in millisecondi. La classe di archiviazione S3 Glacier Instant Retrieval è progettata per i dati di archiviazione di lunga durata a cui si accede in millisecondi circa una volta al trimestre. Per i dati di archiviazione che non richiedono accesso immediato, come i backup, è possibile utilizzare le classi di archiviazione S3 Glacier Flexier Retrieval o S3 Glacier Deep Archive. Per ulteriori informazioni, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

Le best practice di sicurezza seguenti gestiscono anche la resilienza:

- [Enable versioning](#)
- [Consider Amazon S3 cross-region replication](#)
- [Identify and audit all your Amazon S3 buckets](#)

Crittografia dei backup di Amazon S3

Se si esegue l'archiviazione di backup utilizzando Amazon S3, la crittografia dei backup dipende dalla configurazione di tali bucket. Amazon S3 offre un modo per impostare il comportamento di crittografia predefinita per un bucket S3. Puoi configurare la crittografia predefinita di un bucket in modo che gli oggetti siano crittografati quando vengono memorizzati nel bucket. La crittografia predefinita supporta le chiavi memorizzate in (). AWS KMS SSE-KMS Per ulteriori informazioni, consulta [Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3](#).

Per ulteriori informazioni sulla funzione Controllo delle versioni e sul blocco oggetti, consulta i seguenti argomenti: [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#) [Blocco di oggetti con Object Lock](#)

Sicurezza dell'infrastruttura in Amazon S3

In quanto servizio gestito, Amazon S3 è protetto dalle procedure di sicurezza di rete AWS globali descritte nel pilastro della sicurezza del [AWS Well-Architected Framework](#).

L'accesso ad Amazon S3 tramite la rete avviene tramite API pubblicate AWS. I client devono supportare Transport Layer Security (TLS) 1.2. Consigliamo inoltre di supportare TLS 1.3 e lo scambio ibrido di chiavi post-quantistiche. Per ulteriori informazioni sulla crittografia post-quantistica AWS, inclusi collegamenti a post di blog e documenti di ricerca, vedi Cryptography for. [Post-Quantum AWS](#)

Note

TLS 1.3 è supportato in tutti gli endpoint S3, ad eccezione di Amazon S3 e Access Points. AWS PrivateLink Multi-Region

I clienti devono inoltre supportare suite di crittografia con Perfect Forward Secrecy (PFS) come Ephemeral (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman Inoltre, le richieste devono essere firmate utilizzando Signature V4 o Signature V2, richiedendo la fornitura di credenziali valide. AWS AWS

Queste API possono essere invocate da qualsiasi posizione di rete. Tuttavia, Amazon S3 supporta anche le policy di accesso basate sulle risorse, che possono includere limitazioni in base all'indirizzo IP di origine. È possibile utilizzare le policy del bucket Amazon S3 per controllare l'accesso ai bucket da endpoint Virtual Private Cloud (VPC) o da VPC specifici. In effetti, questo isola l'accesso alla rete a un determinato bucket Amazon S3 solo dallo specifico VPC all'interno della rete. AWS Per ulteriori informazioni, consulta [Controllo dell'accesso dagli endpoint VPC con policy di bucket](#).

Le best practice di sicurezza seguenti gestiscono anche la sicurezza dell'infrastruttura in Amazon S3:

- [Consider VPC endpoints for Amazon S3 access](#)
- [Identify and audit all your Amazon S3 buckets](#)

Analisi della configurazione e delle vulnerabilità in Amazon S3

AWS gestisce le attività di sicurezza di base come il sistema operativo (OS) guest e l'applicazione di patch al database, la configurazione del firewall e il disaster recovery. Queste procedure sono state riviste e certificate dalle terze parti appropriate. Per ulteriori dettagli, consulta le seguenti risorse :

- [Convalida della conformità per Amazon S3](#)
- [Modello di responsabilità condivisa](#)
- [Amazon Web Services: panoramica dei processi di sicurezza](#)

Le best practice di sicurezza seguenti gestiscono anche l'analisi di configurazione e vulnerabilità in Amazon S3:

- [Identify and audit all your Amazon S3 buckets](#)
- [Attiva AWS Config](#)

Gestione degli accessi

Amazon S3 offre una serie di strumenti di gestione degli accessi. Di seguito è riportato un elenco di queste funzioni e strumenti. Non è necessario disporre di tutti questi strumenti di gestione degli accessi, ma è necessario utilizzarne uno o più per concedere l'accesso ai bucket Amazon S3, agli oggetti e ad altri [Risorse S3](#). L'applicazione corretta di questi strumenti può aiutare a garantire che le risorse siano accessibili solo agli utenti previsti.

Lo strumento di gestione degli accessi più comunemente utilizzato è una policy di accesso. Una policy di accesso può essere una policy basata sulle risorse associata a una AWS risorsa, ad esempio una policy bucket per un bucket. Un policy di accesso può anche essere una policy basata sull'identità, collegata a un'identità AWS Identity and Access Management (IAM), come un utente, un gruppo o un ruolo IAM. Una policy di accesso descrive chi ha accesso a quali cose. Scrivi una policy di accesso per concedere a utenti, gruppi Account AWS e ruoli IAM il permesso di eseguire operazioni su una risorsa. Ad esempio, puoi concedere PUT Object l'autorizzazione a un altro account Account AWS in modo che l'altro account possa caricare oggetti nel tuo bucket.

Di seguito sono elencati gli strumenti di gestione degli accessi disponibili in Amazon S3. Per una guida più completa sul controllo degli accessi ad Amazon S3, consulta [Controllo degli accessi in Amazon S3](#).

Policy del bucket

Una policy sui bucket di Amazon S3 è una policy [basata sulle risorse JSON-formatted](#) AWS Identity and Access Management (IAM) collegata a un determinato bucket. Utilizza le politiche dei bucket per concedere altre autorizzazioni Account AWS o identità IAM per il bucket e gli oggetti in esso contenuti. Molti casi d'uso della gestione degli accessi S3 possono essere soddisfatti utilizzando una policy di bucket. Con le policy di bucket, è possibile personalizzare l'accesso ai bucket per assicurarsi che solo le identità approvate possano accedere alle risorse ed eseguire azioni al loro interno. Per ulteriori informazioni, consulta [Policy dei bucket per Amazon S3](#).

Identity-based policy

Una policy utente basata sull'identità o IAM è un tipo di [policy AWS Identity and Access Management \(IAM\)](#). Una policy basata sull'identità è una JSON-formatted policy allegata agli utenti, ai gruppi o ai ruoli IAM nel tuo account. AWS È possibile utilizzare le policy basate sull'identità per concedere a un'identità IAM l'accesso ai bucket o agli oggetti. È possibile creare utenti, gruppi e ruoli IAM nel proprio account e associare ad essi le policy di accesso. È quindi possibile concedere l'accesso alle risorse di AWS , comprese quelle di Amazon S3. Per ulteriori informazioni, consulta [Identity-based politiche per Amazon S3](#).

Sovvenzioni di accesso S3

Utilizza S3 Access Grants per creare i permessi di accesso ai dati di Amazon S3 sia per le identità nelle directory di identità aziendali, come Active Directory, sia per le identità AWS Identity and Access Management (IAM). S3 Access Grants aiuta a gestire le autorizzazioni dei dati su scala. Inoltre, S3 Access Grants registra l'identità dell'utente finale e l'applicazione utilizzata per accedere ai dati S3 in AWS CloudTrail. Questo fornisce una cronologia di audit dettagliata fino all'identità dell'utente finale per tutti gli accessi ai dati nei bucket S3. Per ulteriori informazioni, consulta [Gestione dell'accesso con S3 Access Grants](#).

Punti di accesso

Punti di accesso Amazon S3 semplifica la gestione dell'accesso ai dati su scala per le applicazioni che utilizzano set di dati condivisi su S3. I punti di accesso sono endpoint di rete denominati e collegati a un bucket. È possibile utilizzare i punti di accesso per eseguire operazioni sugli oggetti S3 in scala, come il caricamento e il recupero di oggetti. A un bucket possono essere collegati fino a 10.000 punti di accesso e per ogni punto di accesso è possibile applicare autorizzazioni e controlli di rete distinti per avere un controllo dettagliato sull'accesso agli oggetti S3. I punti di accesso S3 possono essere associati a bucket dello stesso account o di un altro account attendibile. Le policy dei

punti di accesso sono policy basate sulle risorse che vengono valutate insieme alla policy di bucket sottostante. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

Lista di controllo degli accessi (ACL)

Una ACL è un elenco di concessioni che identifica il beneficiario e l'autorizzazione concessa. Le ACL concedono permessi di base di lettura o scrittura ad altri Account AWS. Le liste ACL utilizzano uno schema XML specifico di Amazon S3. Una ACL è un tipo di [policy AWS Identity and Access Management \(IAM\)](#). Una ACL per oggetti viene utilizzata per gestire l'accesso a un oggetto e una ACL per bucket viene utilizzata per gestire l'accesso a un bucket. Con le policy di bucket, esiste una singola policy per l'intero bucket, ma le ACL degli oggetti sono specificate per ciascun oggetto. È consigliabile mantenere le ACL disattivate, tranne in circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Per ulteriori informazioni sulle ACL, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Warning

La maggior parte dei casi d'uso moderni di Amazon S3 non richiede l'uso di ACL.

Proprietà dell'oggetto

Per gestire l'accesso ai propri oggetti, è necessario essere il proprietario dell'oggetto. È possibile utilizzare l'impostazione Proprietà oggetto a livello di bucket per controllare la proprietà degli oggetti caricati nel bucket. Inoltre, utilizzare la proprietà dell'oggetto per attivare le ACL. Per impostazione predefinita, la proprietà dell'oggetto è impostata sul proprietario del bucket e tutte le ACL sono disattivate. Quando le ACL sono disattivate, il proprietario del bucket possiede tutti gli oggetti del bucket e gestisce esclusivamente l'accesso ai dati. Per gestire l'accesso, il proprietario del bucket utilizza le policy o un altro strumento di gestione degli accessi, escluse le ACL. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Per una guida più completa sul controllo degli accessi ad Amazon S3 e per ulteriori best practice, consulta [Controllo degli accessi in Amazon S3](#).

Inventario dei dati Amazon Simple Storage Service

Simple Storage Service (Amazon S3)

Amazon S3 fornisce uno storage di oggetti scalabile nel cloud. AWS Consente di archiviare e recuperare qualsiasi quantità di dati, ovunque sul web. Sulla base della sua architettura unica, S3 è progettato per superare la durabilità dei dati del 99,999999999% (11 nove). Inoltre, per impostazione predefinita, S3 archivia i dati in modo ridondante su un minimo di tre zone di disponibilità, garantendo una resilienza integrata contro disastri diffusi. I clienti possono archiviare i dati in un'unica zona di disponibilità per ridurre al minimo i costi o la latenza di archiviazione, in più zone di disponibilità per la resilienza contro la perdita permanente di un intero data center o in più Regioni AWS per soddisfare i requisiti di resilienza geografica.

Caratteristiche chiave

Posizione geografica

Amazon S3 è ospitato in più posizioni in tutto il mondo. Per i dati si selezionano le posizioni vicine ai clienti.

Bucket

Un bucket è un container per gli oggetti archiviati in Amazon S3. Ogni oggetto è contenuto in un bucket.

Oggetti

Entità fondamentali archiviate in Amazon S3, gli oggetti sono composti da dati e metadata.

Classi di storage

Amazon S3 offre diverse classi di archiviazione ottimizzate per diversi casi d'uso.

Gestione dello storage

Amazon S3 dispone di funzionalità di gestione dell'archiviazione utilizzabili per gestire i costi e rispettare i requisiti di conformità.

Gestione degli accessi e sicurezza

Amazon S3 offre caratteristiche per la verifica e la gestione degli accessi ai tuoi bucket e oggetti.

Posizione geografica

Amazon S3 è disponibile in tutto il mondo. Regione AWS Ciascuna regione è un'area geografica distinta.

Perché è importante

Dopo aver determinato dove archiviare i dati, è possibile decidere se implementare un'archiviazione funzionalmente equivalente nelle stesse posizioni o in località diverse, a seconda delle esigenze.

Come ottenere un riepilogo dei bucket Amazon S3 in tutte le Regioni

Usa il seguente AWS CLI comando:

```
aws s3api list-buckets /  
  --max-items 100 /  
  --page-size 100
```

Per ulteriori informazioni, vedere [list-buckets](#) nel Command Reference. AWS CLI

Bucket

I bucket Amazon S3 sono container di oggetti. Ogni bucket ha un nome univoco per tutti. AWS Amazon S3 supporta quattro tipi di bucket: bucket per uso generico, bucket di directory, bucket di tabelle e bucket vettoriali. Ogni tipo di bucket offre un set unico di funzionalità per diversi casi d'uso. Per ulteriori informazioni sui diversi tipi di bucket, consulta [Bucket](#) nella Guida per l'utente di Amazon S3.

Perché sono importanti

Dopo aver elencato i bucket, è possibile convalidare le impostazioni dei bucket per sistemi di archiviazione funzionalmente equivalenti esaminando le varie impostazioni di configurazione dei bucket.

Come elencare le configurazioni dei bucket

```
aws s3api get-bucket-versioning --bucket amzn-s3-demo-bucket1  
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1  
aws s3api get-bucket-logging --bucket amzn-s3-demo-bucket1
```

Per ulteriori informazioni, vedi <https://docs.aws.amazon.com/cli/latest/reference/s3api/get-bucket-versioning.html> get-bucket-versioning nel Command Reference. AWS CLI

Oggetti

Entità fondamentali archiviate in Amazon S3, gli oggetti Ciascun oggetto è formato dai dati, da una chiave (nome) e dai metadata.

Perché sono importanti

La comprensione delle caratteristiche degli oggetti aiuta a pianificare requisiti di capacità di archiviazione e prestazioni equivalenti in sistemi funzionalmente equivalenti.

Come elencare gli oggetti e le relative proprietà

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket1 /  
--query 'Contents[].{Key: Key, Size: Size, LastModified: LastModified}'
```

Per ulteriori informazioni, vedere <https://docs.aws.amazon.com/cli/latest/reference/s3api/list-objects-v2.html> list-objects-v2 nel Command Reference. AWS CLI

Classi di storage

- Amazon S3 Standard
- Amazon S3 Intelligent-Tiering
- Amazon S3 Standard-IA
- Amazon S3 Uno Zone-IA
- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- Amazon S3 Glacier Deep Archive
- Amazon S3 Express One Zone

Perché sono importanti

La comprensione dell'utilizzo della classe di archiviazione consente di determinare i livelli di archiviazione appropriati in sistemi funzionalmente equivalenti. Per maggiori informazioni, consulta

[Comprensione e gestione delle classi di archiviazione Amazon S3](#) nella Guida per l'utente di Amazon S3.

Come esaminare la selezione e l'utilizzo delle classi di archiviazione

Puoi utilizzare Amazon S3 Storage Lens per esaminare la selezione e l'utilizzo della classe di archiviazione. Per maggiori informazioni, consulta [Comprensione e gestione delle classi di archiviazione Amazon S3](#) nella Guida per l'utente di Amazon S3.

Gestione dello storage

Perché è importante

La comprensione dell'utilizzo della gestione dell'archiviazione aiuta a pianificare funzionalità equivalenti per gestire i costi e rispettare i requisiti di conformità in sistemi funzionalmente equivalenti.

Come esaminare la selezione e l'utilizzo delle funzionalità di gestione dell'archiviazione

Puoi utilizzare Amazon S3 Storage Lens per esaminare l'utilizzo delle funzionalità di gestione dell'archiviazione. Per maggiori informazioni, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#) nella Guida per l'utente di Amazon S3.

Gestione degli accessi e sicurezza

Perché sono importanti

La comprensione delle impostazioni di gestione degli accessi e della sicurezza consente di pianificare funzionalità equivalenti per gestire i requisiti di accesso e sicurezza in sistemi funzionalmente equivalenti.

Come esaminare le impostazioni di sicurezza e gestione degli accessi

Dopo aver elencato i bucket, è possibile convalidare le impostazioni di sicurezza e di accesso dei bucket per sistemi di archiviazione funzionalmente equivalenti esaminando le varie impostazioni di configurazione dei bucket.

```
aws s3api get-public-access-block --bucket amzn-s3-demo-bucket1
aws s3api get-bucket-acl --bucket amzn-s3-demo-bucket1
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

```
aws s3api get-bucket-policy --bucket amzn-s3-demo-bucket1
```

Trasferimento dati

È possibile trasferire i dati da Amazon S3 utilizzando diversi metodi:

- AWS CLI
- AWS SDK
- API REST di Amazon S3
- Third-party strumenti

Esempio di utilizzo AWS CLI

Per scaricare un intero bucket:

```
aws s3 sync s3://amzn-s3-demo-bucket1 /local/path
```

Per ulteriori informazioni, vedi [sync](#) nel AWS CLI Command Reference.

Per scaricare oggetti specifici:

```
aws s3 cp s3://amzn-s3-demo-bucket1/path/to/object /local/path
```

Per ulteriori informazioni, vedere [cp](#) nel AWS CLI Command Reference.

Risorse correlate

Di seguito sono riportate altre caratteristiche di Amazon S3:

- [Controllo degli accessi in Amazon S3](#)
- [Sicurezza in Amazon S3](#)
- [Protezione dei dati in Amazon S3](#)
- [Registrazione e monitoraggio in Amazon S3](#)

Protezione dei dati in Amazon S3

Oltre alla resilienza offerta dall'infrastruttura AWS globale, Amazon S3 offre una serie di funzionalità per proteggere i dati da eliminazioni accidentali o guasti regionali.

Replica di Amazon S3

La replica in tempo reale consente di abilitare la copia asincrona e automatica di oggetti tra bucket Amazon S3. I bucket configurati per la replica di oggetti possono essere di proprietà dello stesso account o di account diversi. Account AWS Puoi replicare gli oggetti in un singolo bucket o in più bucket di destinazione. I bucket di destinazione possono trovarsi in aree diverse Regioni AWS o all'interno della stessa regione del bucket di origine. Per abilitare i controlli di failover, è possibile configurare la replica affinché sia bidirezionale e i bucket di origine e di destinazione possano essere mantenuti sincronizzati durante un guasto a livello regionale. Per ulteriori informazioni, consulta [the section called “Replica di oggetti all'interno e tra le Regioni”](#).

Multi-Region Punti di accesso e controlli di failover

Gli Multi-Region access point Amazon S3 forniscono un endpoint globale che le applicazioni possono utilizzare per soddisfare le richieste provenienti da bucket S3 che si trovano in più bucket. Regioni AWS Puoi utilizzare gli Multi-Region Access Point per creare applicazioni multiregionali con la stessa architettura utilizzata in una singola regione e quindi eseguirle in qualsiasi parte del mondo. Invece di inviare richieste tramite la congestionata rete Internet pubblica, gli Multi-Region Access Point forniscono una resilienza di rete integrata con l'accelerazione delle richieste basate su Internet ad Amazon S3. Le richieste applicative effettuate a un endpoint globale di Multi-Region Access Point vengono instradate automaticamente sulla rete AWS globale [AWS Global Accelerator](#) verso il bucket S3 più vicino con uno stato di routing attivo. Per ulteriori informazioni sugli Access Point, vedere. Multi-Region [the section called “Gestione del traffico multi-regione ”](#)

Con i controlli di failover degli Multi-Region Access Point di Amazon S3, puoi mantenere la continuità aziendale durante le interruzioni del traffico regionale, fornendo allo stesso tempo alle tue applicazioni un'architettura multiregionale per soddisfare le esigenze di conformità e ridondanza. Se il traffico regionale viene interrotto, puoi utilizzare i controlli di failover degli Access Point per selezionare quale punto di Multi-Region accesso di Amazon S3 Multi-Region elaborerà Regioni AWS le richieste di accesso e storage ai dati.

Per supportare il failover, puoi configurare Multi-Region l'Access Point in una configurazione attiva-passiva, con il traffico che fluisce verso la regione attiva in condizioni normali e una regione

passiva in standby per il failover. Se hai abilitato S3 Cross-Region Replication (CRR) con regole di replica bidirezionale, puoi mantenere i bucket sincronizzati durante un failover. Per ulteriori informazioni sui controlli di failover, consulta [the section called “Configurazione di failover”](#).

Funzione Controllo delle versioni S3

La funzione Controllo delle versioni è un modo per conservare più versioni di un oggetto nello stesso bucket. La funzione Controllo delle versioni può essere impiegata per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Con la funzione Controllo delle versioni si può facilmente eseguire il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Blocco di oggetti in S3

Puoi utilizzare il blocco oggetti S3 per archiviare gli oggetti utilizzando il modello write once, read many (WORM). Utilizzando il blocco oggetti S3, puoi impedire che un oggetto venga eliminato o sovrascritto per un determinato periodo di tempo o in modo indefinito. Il blocco oggetti S3 consente di soddisfare i requisiti normativi che richiedono uno storage WORM o semplicemente di aggiungere un ulteriore livello di protezione contro le modifiche e l'eliminazione degli oggetti. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).

AWS Backup

Amazon S3 è integrato nativamente con AWS Backup un servizio completamente gestito e basato su policy che puoi utilizzare per definire centralmente le politiche di backup per proteggere i tuoi dati in Amazon S3. Dopo aver definito le politiche di backup e assegnato le risorse di Amazon S3 alle policy, AWS Backup automatizza la creazione dei backup di Amazon S3 e li archivia in modo sicuro in un deposito di backup crittografato indicato nel piano di backup. Per ulteriori informazioni, consulta [the section called “Backup dei dati”](#).

Per un tutorial sull'utilizzo di alcune di queste funzionalità per la protezione dei dati, consulta [Tutorial: Proteggere i dati su Amazon S3 dall'eliminazione accidentale o dai bug delle applicazioni utilizzando il Controllo delle versioni S3, S3 Object Lock e Replica S3](#).

Important

Oltre a utilizzare le funzionalità precedenti per la protezione dei dati, è opportuno consultare i suggerimenti contenuti in [the section called “Best practice di sicurezza”](#).

Argomenti

- [Replica di oggetti all'interno e tra le Regioni](#)
- [Gestione del traffico multiregionale con punti di Multi-Region accesso](#)
- [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#)
- [Blocco di oggetti con Object Lock](#)
- [Backup dei dati di Amazon S3](#)

Replica di oggetti all'interno e tra le Regioni

La replica consente di abilitare la copia asincrona e automatica di oggetti tra bucket di Amazon S3. I bucket configurati per la replica di oggetti possono essere di proprietà dello stesso Account AWS o di account diversi. Puoi replicare gli oggetti in un singolo bucket o in più bucket di destinazione. I bucket di destinazione possono trovarsi in aree diverse Regioni AWS o all'interno della stessa regione del bucket di origine.

Esistono due tipi di replica: la replica in tempo reale e la replica on demand.

- Replica in tempo reale: per replicare automaticamente oggetti nuovi e aggiornati durante la scrittura nel bucket di origine, utilizzare la replica in tempo reale. La replica in tempo reale non esegue la replica degli oggetti esistenti nel bucket prima della configurazione della replica. Per replicare oggetti esistenti prima della configurazione della replica, occorre ricorrere alla replica on demand.
- On-demand replica: per replicare oggetti esistenti dal bucket di origine a uno o più bucket di destinazione su richiesta, usa S3 Batch Replication. Per ulteriori informazioni sulla replica di oggetti esistenti, consulta la sezione [Quando utilizzare S3 Batch Replication](#).

Esistono due forme di replica live: Replication (CRR) e Cross-Region Replication (SRR). Same-Region

- Cross-Region Replica (CRR): puoi utilizzare il CRR per replicare oggetti su bucket Amazon S3 in diversi. Regioni AWS Per ulteriori informazioni sulla replica tra Regioni, consulta [the section called “Quando usare la replica Cross-Region”](#).
- Same-Region Replicazione (SRR): puoi utilizzare SRR per copiare oggetti tra bucket Amazon S3 nello stesso. Regione AWS Per ulteriori informazioni sulla replica nella stessa Regione, consulta [the section called “Quando utilizzare la replica Same-Region”](#).

Argomenti

- [Perché utilizzare la replica?](#)
- [Quando usare la replica Cross-Region](#)
- [Quando utilizzare la replica Same-Region](#)
- [Quando utilizzare la replica bidirezionale](#)
- [Quando utilizzare S3 Batch Replication](#)
- [Requisiti del carico di lavoro e replica in tempo reale](#)
- [Cosa replica Amazon S3?](#)
- [Requisiti e considerazioni sulla replica](#)
- [Panoramica della configurazione della replica in tempo reale](#)
- [Gestione o sospensione della replica in tempo reale](#)
- [Replica di oggetti esistenti con Replica in batch](#)
- [Risoluzione dei problemi nella replica](#)
- [Monitoraggio della replica con parametri, notifiche di eventi e stati](#)

Perché utilizzare la replica?

La replica può essere utile per gli scopi seguenti:

- **Replica di oggetti conservando i metadati:** puoi utilizzare la replica per creare copie degli oggetti che conservano tutti i metadati, ad esempio l'ora di creazione dell'oggetto originale e gli ID della versione. Questa funzionalità è importante se vuoi assicurarti che la replica sia identica all'oggetto di origine.
- **Replica di oggetti in classi di archiviazione diverse:** puoi utilizzare la replica per inserire direttamente gli oggetti in S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive o in un'altra classe di archiviazione nei bucket di destinazione. Puoi anche replicare i dati nella stessa classe di archiviazione e utilizzare configurazioni del ciclo di vita nei bucket di destinazione per spostare gli oggetti in una classe di archiviazione più inattiva col passare del tempo.
- **Mantieni le copie degli oggetti con proprietà diverse:** indipendentemente da chi possiede l'oggetto sorgente, puoi dire ad Amazon S3 di cambiare la proprietà della replica con quella proprietaria del Account AWS bucket di destinazione. Questa opzione è detta sostituzione del proprietario. Puoi utilizzare questa opzione per limitare l'accesso alle repliche degli oggetti.

- Conserva gli oggetti archiviati su più livelli Regioni AWS: per garantire le differenze geografiche in cui vengono conservati i dati, puoi impostare più bucket di destinazione su diversi. Regioni AWS Questa funzionalità potrebbe aiutarti a soddisfare determinati requisiti di conformità.
- Replica gli oggetti entro 15 minuti: per replicare i dati nella stessa regione Regione AWS o in diverse regioni entro un intervallo di tempo prevedibile, puoi utilizzare S3 Replication Time Control (S3 RTC). S3 RTC replica il 99,99% dei nuovi oggetti archiviati in Amazon S3 entro 15 minuti, secondo un Accordo sul Livello di Servizio (SLA). Per ulteriori informazioni, consulta [the section called “Utilizzo di S3 Replication Time Control”](#).

Note

S3 RTC non si applica a Batch Replication. Batch Replication è un processo di replica on demand e può essere monitorato con S3 Batch Operations. Per ulteriori informazioni, consulta [Monitoraggio dei rapporti sullo stato e sul completamento dei processi](#).

- Sincronizzazione di bucket, replica di oggetti esistenti e replica di oggetti falliti o replicati in precedenza: per sincronizzare i bucket e replicare oggetti esistenti, utilizza Batch Replication come operazione di replica on demand. Per ulteriori informazioni sul momento in cui è necessario utilizzare Batch Replication, consulta la sezione [Quando utilizzare S3 Batch Replication](#).
- Replica oggetti ed esegui il failover su un bucket in un altro Regione AWS: per mantenere sincronizzati tutti i metadati e gli oggetti tra i bucket durante la replica dei dati, utilizza le regole di replica bidirezionale (nota anche come replica bidirezionale) prima di configurare i controlli di failover di Amazon S3 Multi-Region Access Point. Two-way le regole di replica aiutano a garantire che quando i dati vengono scritti nel bucket S3 in cui il traffico viene trasferito, tali dati vengano poi replicati nuovamente nel bucket di origine.

Quando usare la replica Cross-Region

S3 Cross-Region Replication (CRR) viene utilizzato per copiare oggetti tra bucket Amazon S3 in diversi bucket. Regioni AWS La replica CRR consente di completare le seguenti operazioni:

- Rispetto dei requisiti di conformità: sebbene di default Amazon S3 archivi i dati in più zone di disponibilità geograficamente distanti, per soddisfare i requisiti di conformità potrebbe essere necessario archivarli a distanze ancora maggiori. Per soddisfare questi requisiti, utilizza Cross-Region Replication per replicare i dati tra loro distanti. Regioni AWS

- **Ridurre al minimo la latenza:** se i clienti si trovano in due aree geografiche, è possibile ridurre al minimo la latenza di accesso agli oggetti conservando le copie degli oggetti in Regioni AWS luoghi geograficamente più vicini agli utenti.
- **Aumenta l'efficienza operativa:** se disponi di due cluster di elaborazione diversi Regioni AWS che analizzano lo stesso set di oggetti, potresti scegliere di mantenere le copie degli oggetti in quelle regioni.

Quando utilizzare la replica Same-Region

Same-Region La replica (SRR) viene utilizzata per copiare oggetti tra bucket Amazon S3 nello stesso. Regione AWS La replica SRR consente di completare le seguenti operazioni:

- **Aggregazione dei registri in un solo bucket:** se archivi i registri in più bucket o in più account, puoi replicarli facilmente in un solo bucket nella tua regione. Questo semplifica l'elaborazione dei registri in una sola posizione.
- **Configurazione della replica in tempo reale tra gli account di produzione e test:** se tu o i tuoi clienti disponete di account di produzione e test che utilizzano gli stessi dati, potete replicare gli oggetti tra più account conservandone i metadati.
- **Rispetta le leggi sulla sovranità dei dati:** potrebbe essere necessario archiviare più copie dei dati separatamente all'interno di una determinata regione. Account AWS Same-Region La replica può aiutarti a replicare automaticamente i dati critici quando le normative di conformità non consentono ai dati di lasciare il tuo Paese.

Quando utilizzare la replica bidirezionale

- **Crea set di dati condivisi su più parti Regioni AWS:** con la sincronizzazione delle modifiche delle repliche, puoi replicare facilmente le modifiche ai metadati, come gli elenchi di controllo dell'accesso agli oggetti (ACL), i tag degli oggetti o i blocchi degli oggetti, sugli oggetti di replica. Questa replica bidirezionale è importante se si desidera mantenere sincronizzati tutti gli oggetti e le modifiche ai metadati degli oggetti. È possibile [abilitare la sincronizzazione delle modifiche delle repliche](#) su una regola di replica nuova o esistente quando si esegue una replica bidirezionale tra due o più bucket nella stessa o in diverse Regioni AWS.
- **Mantieni i dati sincronizzati tra le regioni durante il failover:** puoi sincronizzare i dati nei bucket tra loro configurando regole di replica bidirezionale con S3 Replication (CRR) direttamente Regioni AWS da un Access Point. Cross-Region Multi-Region Per prendere una decisione informata

su quando avviare il failover, puoi anche abilitare le metriche di replica S3 in modo da poter monitorare la replica in Amazon CloudWatch, in S3 Replication Time Control (S3 RTC) o dall' Multi-Region Access Point.

- Rendere la tua applicazione altamente disponibile: anche in caso di interruzione del traffico regionale, puoi utilizzare regole di replica bidirezionale per mantenere sincronizzati tutti i metadati e gli oggetti tra i bucket durante la replica dei dati.

Quando utilizzare S3 Batch Replication

Batch Replication replica gli oggetti esistenti in bucket diversi come opzione on demand. A differenza della replica in tempo reale, questi processi possono essere eseguiti all'occorrenza. Batch Replication può essere utile per gli scopi seguenti:

- Replica oggetti esistenti: puoi utilizzare Batch Replication per replicare oggetti aggiunti al bucket prima della configurazione di Replication o Replication. Same-Region Cross-Region
- Replica di oggetti che in precedenza non sono stati replicati: è possibile applicare un filtro a un processo Batch Replication per tentare di replicare gli oggetti con uno stato di replica FAILED (Fallito).
- Replica di oggetti già replicati: potrebbe essere necessario archiviare più copie dei dati in Account AWS o Regioni AWS separati. Batch Replication può replicare gli oggetti esistenti nelle destinazioni appena aggiunte.
- Replica di repliche di oggetti creati da una regola di replica: le configurazioni di replica creano repliche di oggetti nei bucket di destinazione. Le repliche di oggetti possono essere replicate solo con Batch Replication.

Requisiti del carico di lavoro e replica in tempo reale

A seconda dei requisiti del carico di lavoro, alcuni tipi di replica in tempo reale saranno più adatti a uno specifico caso d'uso rispetto ad altri. Utilizza la tabella seguente per determinare il tipo di replica da utilizzare in una specifica situazione e se utilizzare il controllo del tempo di replica di S3 (S3 RTC) per il carico di lavoro. S3 RTC replica il 99,99% dei nuovi oggetti archiviati in Amazon S3 entro 15 minuti, secondo un Accordo sul Livello di Servizio o SLA. Per ulteriori informazioni, consulta [the section called “Utilizzo di S3 Replication Time Control”](#).

Requisiti del carico di lavoro	S3 RTC (SLA di 15 minuti)	Cross-Region Replica (CRR)	Same-Region Replica (SRR)
Replica oggetti tra diversi Account AWS	Sì	Sì	Sì
Replica gli oggetti all'interno degli stessi Regione AWS entro 24-48 ore (senza supporto SLA)	No	No	Sì
Replica oggetti tra diversi Regioni AWS entro 24-48 ore (senza supporto SLA)	No	Sì	No
Tempo di replica prevedibile: supportato o dallo SLA per replicare il 99,9% degli oggetti entro 15 minuti	Sì	No	No

Cosa replica Amazon S3?

Amazon S3 replica solo elementi specifici nei bucket configurati per la replica.

Argomenti

- [Che cosa viene replicato con le configurazioni di replica?](#)
- [Che cosa non viene replicato con le configurazioni di replica?](#)

Che cosa viene replicato con le configurazioni di replica?

Di default, Amazon S3 replica quanto segue:

- Oggetti creati dopo l'aggiunta di una configurazione di replica.

- Oggetti non crittografati.
- Oggetti crittografati utilizzando chiavi fornite dal cliente (SSE-C), oggetti crittografati a riposo con una chiave gestita da Amazon S3 (SSE-S3) o una chiave KMS archiviata in (). AWS Key Management Service SSE-KMS Per ulteriori informazioni, consulta [the section called “Replica di oggetti crittografati”](#).
- Metadati dell'oggetto dagli oggetti di origine alle repliche. Per informazioni sulla replica dei metadati dalle repliche agli oggetti di origine, consulta [Replica delle modifiche ai metadati con la sincronizzazione delle modifiche alla replica](#).
- Solo gli oggetti nel bucket di origine per cui il proprietario del bucket dispone delle autorizzazioni di lettura degli oggetti e delle liste di controllo accessi (ACL).

Per ulteriori informazioni sulla proprietà delle risorse, consulta [Proprietà di bucket e oggetti di Amazon S3](#).

- Gli aggiornamenti delle liste di controllo accessi degli oggetti, a meno che non indichi ad Amazon S3 di modificare il proprietario della replica quando i bucket di origine e di destinazione non sono di proprietà degli stessi account.

Per ulteriori informazioni, consulta [Modifica del proprietario della replica](#).

Per la sincronizzazione delle due liste di controllo accessi da parte di Amazon S3 potrebbe essere necessario del tempo. Questa modifica di proprietà si applica solo agli oggetti creati dopo che è stata aggiunta una configurazione di replica al bucket.

- Eventuali tag degli oggetti.
- Annotazioni sugli oggetti, se presenti. Ogni annotazione viene replicata indipendentemente man mano che si verificano modifiche durante la replica in tempo reale. Durante S3 Batch Replication, le annotazioni vengono replicate indipendentemente accanto all'oggetto, ma non ci sono attività di lavoro separate per le singole annotazioni. Se la replica delle annotazioni ha esito negativo, il job task ha esito negativo, ma lo stato di replica dell'oggetto non riflette l'errore dell'annotazione.
- Eventuali informazioni sulla conservazione del blocco oggetti S3.

Quando Amazon S3 replica gli oggetti con informazioni sulla conservazione, applica gli stessi controlli di conservazione alle repliche, ignorando il periodo di conservazione predefinito configurato sui bucket di destinazione. Se non sono previsti controlli di conservazione applicati agli oggetti nel bucket di origine e la replica viene effettuata nei bucket di destinazione con un periodo di conservazione predefinito impostato, il periodo di conservazione predefinito dei bucket di

destinazione viene applicato alle repliche degli oggetti. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).

Effetto delle operazioni di eliminazione sulla replica

Se si elimina un oggetto dal bucket di origine, per impostazione predefinita si verificano le seguenti azioni:

- Se effettui una richiesta di eliminazione (DELETE) senza specificare l'ID della versione dell'oggetto, Amazon S3 aggiunge un contrassegno di eliminazione. Amazon S3 gestisce il contrassegno di eliminazione in questo modo:
 - Se usi la versione più recente della configurazione di replica (ovvero, se specifichi l'elemento `Filter` in una regola di configurazione di replica), Amazon S3 non replica automaticamente il contrassegno di eliminazione. Tuttavia, puoi aggiungere la replica del contrassegno di eliminazione a regole non basate su tag. Per ulteriori informazioni, consulta [Replica dei contrassegni di eliminazione tra i bucket](#).
 - Se non si specifica l'elemento `Filter`, Amazon S3 presuppone che la configurazione di replica sia la versione V1 e replica i contrassegni di eliminazione derivanti dalle azioni dell'utente. Tuttavia, se Amazon S3 elimina un oggetto a causa di un'azione del ciclo di vita, il contrassegno di eliminazione non viene replicato nei bucket di destinazione.
- Se nella richiesta DELETE specifichi l'ID della versione dell'oggetto da eliminare, Amazon S3 elimina la versione dell'oggetto nel bucket di origine, ma non replica l'eliminazione nei bucket di destinazione. In altre parole, non elimina la stessa versione dell'oggetto dai bucket di destinazione. Ciò permette di proteggere i dati da eliminazioni da parte di utenti malintenzionati.

Che cosa non viene replicato con le configurazioni di replica?

Di default, Amazon S3 non replica quanto segue:

- Gli oggetti nel bucket di origine che sono repliche create da un'altra regola di replica. Supponiamo, per esempio, di configurare una replica dove il bucket A è l'origine e il bucket B è la destinazione. Supponiamo ora di aggiungere un'altra configurazione di replica dove il bucket B è l'origine e il bucket C è la destinazione. In questo caso, gli oggetti nel bucket B che sono repliche di oggetti nel bucket A non vengono replicati nel bucket C.

Per replicare oggetti che sono repliche, utilizza Batch Replication. Per ulteriori informazioni sulla configurazione di Batch Replication, visita [Replica di oggetti esistenti](#).

- Oggetti nel bucket di origine che sono già stati replicati in una destinazione diversa. Se, ad esempio, modifichi il bucket di destinazione in una configurazione di replica esistente, Amazon S3 non replica di nuovo gli oggetti.

Per replicare oggetti replicati in precedenza, utilizza Batch Replication. Per ulteriori informazioni sulla configurazione di Batch Replication, visita [Replica di oggetti esistenti](#).

- La replica batch non supporta la ripetizione della replica di oggetti eliminati con l'ID versione dell'oggetto dal bucket di destinazione. Per replicare nuovamente questi oggetti è possibile copiare gli oggetti di origine presenti con un processo di copia in batch. La copia di tali oggetti crea nuove versioni dell'oggetto nel bucket di origine e avvia automaticamente la replica nella destinazione. Per ulteriori informazioni su come utilizzare la copia batch, consulta [Esempi che utilizzano operazioni in batch per copiare oggetti](#).
- Per impostazione predefinita, quando si esegue la replica da un altro Account AWS, i marker di eliminazione aggiunti al bucket di origine non vengono replicati.

Per informazioni su come replicare i contrassegni di eliminazione, consulta la sezione [Replica dei contrassegni di eliminazione tra i bucket](#).

- Oggetti archiviati nelle classi o nei livelli di storage S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Archive Access o S3 Deep Intelligent-Tiering Archive Access. Intelligent-Tiering Non è possibile replicare questi oggetti finché non vengono ripristinati e copiati in una classe di archiviazione diversa.

Per ulteriori informazioni su Recupero flessibile Amazon S3 Glacier e S3 Glacier Deep Archive, consulta [Classi di storage per oggetti con accesso non frequente](#).

Per saperne di più su S3, consulta. Intelligent-Tiering [Gestione dei costi di storage con il Piano intelligente Amazon S3](#)

- Oggetti nel bucket di origine per cui il proprietario del bucket non dispone di autorizzazioni sufficienti per eseguire la replica.

Per informazioni su come il proprietario di un oggetto può concedere le autorizzazioni al proprietario del bucket, consulta la sezione [Concedere autorizzazioni multi-account per il caricamento di oggetti a garanzia del controllo completo da parte del proprietario del bucket](#).

- Aggiornamenti alle risorse secondarie a livello di bucket.

Se, ad esempio, modifichi la configurazione del ciclo di vita o aggiungi una configurazione di notifica nel bucket di origine, tali modifiche non vengono applicate nel bucket di destinazione.

Questa funzionalità permette la presenza di configurazioni diverse nei bucket di origine e di destinazione.

- Operazioni eseguite dalla configurazione del ciclo di vita.

Ad esempio, se la configurazione del ciclo di vita è abilitata solo nel bucket di origine, Amazon S3 crea i contrassegni di eliminazione per gli oggetti scaduti, ma non replica i contrassegni. Per applicare al bucket di origine e a quello di destinazione la stessa configurazione del ciclo di vita, è sufficiente abilitare quest'ultima in entrambi. Per ulteriori informazioni sulla configurazione del ciclo di vita, consulta [Gestione del ciclo di vita degli oggetti](#).

- Quando si utilizzano regole di replica basate su tag con replica in tempo reale, occorre assegnare ai nuovi oggetti il tag della regola di replica corrispondente nell'operazione `PutObject`. In caso contrario, gli oggetti non verranno replicati. Non verranno replicati neanche gli oggetti a cui vengono assegnati tag dopo l'operazione `PutObject`.

Per replicare oggetti a cui sono stati assegnati tag dopo l'operazione `PutObject`, è necessario utilizzare Replica in batch S3. Per ulteriori informazioni su Batch Replication, consulta la sezione [Replica di oggetti esistenti](#).

- Le cancellazioni delle annotazioni nel bucket di origine non vengono replicate nella destinazione. Se si elimina un'annotazione sull'origine, l'annotazione persiste nella replica. Non è possibile escludere le annotazioni dalla replica utilizzando i filtri delle regole di replica. Quando la replica è configurata, tutte le creazioni e gli aggiornamenti delle annotazioni vengono replicati a meno che la politica del ruolo di replica non lo neghi esplicitamente. `s3:ReplicateObjectAnnotation`

Se le annotazioni vengono eliminate e ricreate ripetutamente sull'origine con nomi diversi, la replica di destinazione accumula annotazioni nel tempo perché le eliminazioni non vengono replicate. Questo accumulo può eventualmente far sì che la destinazione superi il limite di 1.000 annotazioni per versione dell'oggetto.

Le sovrascritture delle annotazioni (aggiornamenti a un nome di annotazione esistente) all'origine vengono replicate nella destinazione. Il contenuto dell'annotazione di destinazione rimane aggiornato con l'origine.

Requisiti e considerazioni sulla replica

La replica Amazon S3 richiede quanto segue:

- Il proprietario del bucket di origine deve avere l'origine e la destinazione Regioni AWS abilitate per il proprio account. La regione di destinazione deve essere abilitata per l'account del proprietario del bucket.

Per ulteriori informazioni sull'attivazione o la disabilitazione di un Regione AWS, consulta [Specificare quale Regioni AWS account può utilizzare](#) nella Guida di Gestione dell'account AWS riferimento.

- Sia per il bucket di origine che per quello di destinazione deve essere abilitata la funzione Controllo delle versioni. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).
- Amazon S3 deve disporre delle autorizzazioni necessarie per replicare gli oggetti dal bucket di origine a quelli di destinazione per tuo conto. Per ulteriori informazioni su queste autorizzazioni, consulta la sezione [Configurazione delle autorizzazioni per la replica in tempo reale](#).
- Se il proprietario del bucket di origine non possiede l'oggetto nel bucket, il proprietario dell'oggetto deve concedere al proprietario del bucket le autorizzazioni READ e READ_ACP con la lista di controllo degli accessi (ACL) dell'oggetto. Per ulteriori informazioni, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).
- Se il blocco oggetti S3 è abilitato nel bucket di origine, deve essere abilitato anche nei bucket di destinazione.

Per abilitare la replica su un bucket con Object Lock abilitato, devi utilizzare l' AWS Command Line Interface API REST o gli SDK. AWS Per ulteriori informazioni generali, consulta [Blocco di oggetti con Object Lock](#).

Note

È necessario concedere due nuove autorizzazioni sul bucket S3 di origine nel ruolo AWS Identity and Access Management (IAM) utilizzato per configurare la replica. Le due nuove autorizzazioni sono `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se il ruolo dispone di un'autorizzazione `s3:Get*`, soddisfa il requisito. Per ulteriori informazioni, consulta [Configurazione delle autorizzazioni per la replica in tempo reale](#).

Per ulteriori informazioni, consulta [Panoramica della configurazione della replica in tempo reale](#).

Quando imposti la configurazione di replica in uno scenario con più account, in cui il bucket di origine e quello di destinazione sono di proprietà di Account AWS diversi, si applica il seguente requisito aggiuntivo:

- Il proprietario dei bucket di destinazione deve concedere al proprietario del bucket di origine le autorizzazioni necessarie per replicare gli oggetti con una policy del bucket. Per ulteriori informazioni, consulta [\(Facoltativo\) Fase 3: concessione delle autorizzazioni quando i bucket di origine e di destinazione sono di proprietà di soggetti diversi Account AWS](#).
- I bucket di destinazione non possono essere configurati come bucket con pagamento a carico del richiedente. Per ulteriori informazioni, consulta [Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati](#).

Considerazioni sulla replica

Prima di creare una configurazione della replica, tenere presenti le considerazioni riportate di seguito.

Argomenti

- [Configurazione del ciclo di vita e repliche di oggetti](#)
- [Configurazione della funzione Controllo delle versioni e configurazione di replica](#)
- [Utilizzo della replica S3 con S3 Intelligent-Tiering](#)
- [Configurazione della registrazione e configurazione di replica](#)
- [CRR e regione di destinazione](#)
- [Replica in batch S3](#)
- [Controllo del tempo di replica di S3](#)

Configurazione del ciclo di vita e repliche di oggetti

Il tempo richiesto da Amazon S3 per la replica di un oggetto dipende dalle dimensioni dell'oggetto. Per gli oggetti di grandi dimensioni, questa operazione può richiedere anche diverse ore. Anche se la replica può richiedere tempo prima di diventare disponibile nella destinazione, il tempo necessario per creare la replica corrisponde a quello che è stato necessario per creare l'oggetto corrispondente nel bucket di origine. Se una configurazione del ciclo di vita è abilitata in un bucket di destinazione, le regole del ciclo di vita rispettano l'ora di creazione originale dell'oggetto, non l'ora in cui la replica è diventata disponibile nel bucket di destinazione.

La configurazione di replica richiede che nel bucket sia abilitata la funzione Controllo delle versioni. Quando si abilita tale funzione in un bucket, tenere presente quanto segue:

- Se è presente una configurazione del ciclo di vita di scadenza dell'oggetto, dopo avere abilitato la funzione Controllo delle versioni, è necessario aggiungere una policy `NonCurrentVersionExpiration` per mantenere lo stesso comportamento di eliminazione permanente presente prima dell'abilitazione della funzione.
- Se è presente una configurazione del ciclo di vita di transizione, dopo avere abilitato la funzione Controllo delle versioni, è consigliabile aggiungere una policy `NonCurrentVersionTransition`.

Configurazione della funzione Controllo delle versioni e configurazione di replica

Quando si configura la replica in un bucket, la funzione Controllo delle versioni deve essere abilitata sia nel bucket di origine che in quello di destinazione. Dopo avere abilitato la funzione Controllo delle versioni in entrambi i bucket di origine e di destinazione e avere configurato la replica nel bucket di origine, potrebbero verificarsi i problemi seguenti:

- Se si tenta di disabilitare la funzione Controllo delle versioni nel bucket di origine, Amazon S3 restituisce un errore. Prima di poter disabilitare la funzione Controllo delle versioni nel bucket di origine, è necessario rimuovere la configurazione di replica.
- Se si disabilita la funzione Controllo delle versioni nel bucket di destinazione, la replica ha esito negativo. Lo stato della replica dell'oggetto di origine è `FAILED`.

Utilizzo della replica S3 con S3 Intelligent-Tiering

S3 Intelligent-Tiering è una classe di storage progettata per ottimizzare i costi di storage spostando automaticamente i dati al livello di accesso più conveniente. Con un piccolo costo mensile per il monitoraggio e l'automazione degli oggetti, S3 Intelligent-Tiering monitora i modelli di accesso e sposta automaticamente gli oggetti a cui non è stato effettuato l'accesso ai livelli di accesso più economici.

Replicare gli oggetti archiviati in S3 Intelligent-Tiering con S3 Batch Replication o richiamare o costituire l'accesso. [CopyObject](#) [UploadPartCopy](#) In questi casi, gli oggetti di origine delle operazioni di copia o replica sono suddivisi su più livelli.

Per ulteriori informazioni su S3, vedere, [Intelligent-Tiering Gestione dei costi di storage con il Piano intelligente Amazon S3](#)

Configurazione della registrazione e configurazione di replica

Se Amazon S3 invia log a un bucket in cui è abilitata la replica, gli oggetti dei log vengono replicati.

Se nel bucket di origine o di destinazione sono abilitati i [log di accesso al server](#) o i [log di AWS CloudTrail](#), Amazon S3 include nei log le richieste correlate alla replica. Ad esempio, Amazon S3 include nei log ogni oggetto che replica.

CRR e regione di destinazione

Amazon S3 Cross-Region Replication (CRR) viene utilizzato per copiare oggetti tra bucket S3 in diversi. Regioni AWS Puoi scegliere la regione del bucket di destinazione in base alle esigenze aziendali o a considerazioni sui costi. Ad esempio, i costi di trasferimento dei dati tra regioni variano in base alle regioni scelte.

Supponiamo di scegliere Stati Uniti orientali (Virginia settentrionale) (us-east-1) come Regione per il bucket di origine. Se si sceglie Stati Uniti occidentali (Oregon) (us-west-2) come Regione per i bucket di destinazione, il costo sarà maggiore di quanto non sarebbe scegliendo la Regione Stati Uniti orientali (Ohio) (us-east-2). Per informazioni sui prezzi, consulta la sezione relativa ai prezzi per il trasferimento dati in [Prezzi di Amazon S3](#).

Non sono previsti costi di trasferimento dati associati Same-Region a Replication (SRR).

Replica in batch S3

Per informazioni sulle considerazioni relative a Replica in batch, consulta [Considerazioni su S3 Batch Replication](#).

Controllo del tempo di replica di S3

Per ulteriori informazioni sul controllo del tempo di replica di S3 (S3 RTC), consulta [Best practice e linee guida per S3 RTC](#).

Panoramica della configurazione della replica in tempo reale

Note

Gli oggetti esistenti prima della configurazione della replica non vengono replicati automaticamente. In altre parole, Amazon S3 non esegue la replica retroattiva di oggetti. Per replicare oggetti creati prima della configurazione della replica, utilizza S3 Batch Replication.

Per maggiori informazioni sulla configurazione di Replica in batch, consulta [Replica di oggetti esistenti](#).

Per abilitare la replica in tempo reale, Same-Region Replication (SRR) o Cross-Region Replication (CRR), aggiungi una configurazione di replica al bucket di origine. Questa configurazione indica ad Amazon S3 di replicare gli oggetti come specificato. Nella configurazione di replica, è necessario fornire le informazioni seguenti:

- I bucket di destinazione: uno o più bucket in cui desideri che Amazon S3 replichi gli oggetti.
- Gli oggetti da replicare: è possibile replicare tutti gli oggetti presenti nel bucket di origine o solo parte di essi. Puoi identificare un sottoinsieme specificando nella configurazione un [prefisso di nome di chiave](#), uno o più tag di oggetti oppure entrambi.

Se, ad esempio, configuri una regola di replica per replicare solo gli oggetti con il prefisso di nome di chiave Tax/, Amazon S3 replica gli oggetti con chiavi come Tax/doc1 o Tax/doc2. Ma non replica un oggetto con la chiave Legal/doc3. Se specifichi sia un prefisso sia uno o più tag, Amazon S3 replica solo gli oggetti con il prefisso della chiave e i tag specificati.

- Un ruolo AWS Identity and Access Management (IAM): Amazon S3 assume questo ruolo IAM per replicare gli oggetti per tuo conto. Per ulteriori informazioni sulla creazione di questo ruolo IAM e sulla gestione delle autorizzazioni, consulta [Configurazione delle autorizzazioni per la replica in tempo reale](#).

Oltre a questi requisiti minimi, puoi scegliere tra le opzioni seguenti:

- Classe di archiviazione della replica: di default, Amazon S3 archivia le repliche di oggetti utilizzando la stessa classe di archiviazione dell'oggetto di origine. È possibile specificare una classe di storage diversa per le repliche.
- Proprietà della replica: Amazon S3 presuppone che la replica di un oggetto continuerà ad appartenere al proprietario dell'oggetto di origine. Quindi, quando replica gli oggetti, ne replica anche la lista di controllo degli accessi (ACL) corrispondente o l'impostazione S3 Object Ownership. Se i bucket di origine e di destinazione sono di proprietà di Account AWS diversi, è possibile configurare la replica in modo da assegnare la proprietà di una replica all' Account AWS proprietario del bucket di destinazione. Per ulteriori informazioni, consulta [the section called "Modifica del proprietario della replica"](#).

Puoi configurare la replica utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3. Per istruzioni dettagliate su come configurare la replica, consulta [the section called “Procedure guidate di replica”](#).

Amazon S3 fornisce operazioni REST API per supportare la configurazione delle regole di replica. Per ulteriori informazioni, consulta i seguenti argomenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [PutBucketReplication](#)
- [GetBucketReplication](#)
- [DeleteBucketReplication](#)

Argomenti

- [Elementi del file di configurazione della replica](#)
- [Configurazione delle autorizzazioni per la replica in tempo reale](#)
- [Esempi di configurazione della replica in tempo reale](#)

Elementi del file di configurazione della replica

Amazon S3 archivia la configurazione di replica come file XML. Se la replica viene configurata a livello di codice tramite la REST API di Amazon S3, i vari elementi della configurazione della replica vengono specificati in questo file XML. Se la replica viene configurata tramite AWS Command Line Interface (AWS CLI), la configurazione della replica viene specificata utilizzando il formato JSON. Per gli esempi di JSON, consulta le procedure dettagliate in [the section called “Procedure guidate di replica”](#).

Note

La versione più recente del formato XML di configurazione della replica è V2. Le configurazioni di replica XML V2 sono quelle che contengono l'elemento `<Filter>` per le regole e le regole che specificano S3 Replication Time Control (S3 RTC). Per visualizzare la versione della configurazione di replica, puoi utilizzare l'operazione API `GetBucketReplication`. Per ulteriori informazioni, consulta [GetBucketReplication](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Per la compatibilità con le versioni precedenti, Amazon S3 continua a supportare il formato di configurazione della replica XML V1. Se è stato usato il formato di configurazione della replica XML V1, consulta [Considerazioni sulla compatibilità con le versioni precedenti](#) per le considerazioni relative alla compatibilità con le versioni precedenti.

Nel file XML di configurazione della replica, devi specificare un ruolo AWS Identity and Access Management (IAM) e una o più regole, come mostrato nell'esempio seguente:

```
<ReplicationConfiguration>
  <Role>IAM-role-ARN</Role>
  <Rule>
    ...
  </Rule>
  <Rule>
    ...
  </Rule>
  ...
</ReplicationConfiguration>
```

Amazon S3 non può replicare oggetti senza la tua autorizzazione. Le autorizzazioni vengono concesse ad Amazon S3 con il ruolo IAM specificato nella configurazione della replica. Amazon S3 assume questo ruolo IAM per replicare gli oggetti per conto dell'utente. È necessario innanzitutto concedere le autorizzazioni necessarie al ruolo IAM. Per ulteriori informazioni sulla gestione delle autorizzazioni, consulta la sezione [Configurazione delle autorizzazioni per la replica in tempo reale](#).

Una configurazione di replica di Amazon S3 può avere fino a 1.000 regole per bucket di origine. Questo limite non è regolabile.

È possibile aggiungere una sola regola a una configurazione della replica quando:

- Vuoi replicare tutti gli oggetti.
- Si desidera replicare solo un sottoinsieme di oggetti. Identifichi il sottoinsieme di oggetti aggiungendo un filtro alla regola. Nel filtro si specifica un prefisso di chiave o tag dell'oggetto o una combinazione di questi elementi, per identificare il sottoinsieme di oggetti a cui si applica la regola. I filtri si applicano agli oggetti che corrispondono ai valori esatti specificati.

Per replicare sottoinsiemi di oggetti diversi, aggiungere più regole a una configurazione della replica. In ogni regola è possibile specificare un filtro tramite il quale selezionare un sottoinsieme diverso.

Puoi ad esempio scegliere di replicare gli oggetti con prefissi della chiave `tax/` o `document/`. A tale scopo, aggiungi 2 regole, una che specifica il filtro del prefisso della `tax/` chiave e l'altra che specifica il prefisso della chiave `document/`. Per ulteriori informazioni sui prefissi della chiave dell'oggetto, consulta [Organizzazione degli oggetti utilizzando i prefissi](#).

Nelle sezioni seguenti vengono fornite informazioni aggiuntive.

Argomenti

- [Configurazione di base delle regole](#)
- [Facoltativo: specifica di un filtro](#)
- [Configurazioni di destinazione aggiuntive](#)
- [Esempi di configurazioni di replica](#)
- [Considerazioni sulla compatibilità con le versioni precedenti](#)

Configurazione di base delle regole

Ogni regola deve includere lo stato e la priorità della stessa. La regola deve anche indicare se replicare i contrassegni di eliminazione.

- L'elemento `<Status>` indica se la regola è abilitata o disabilitata utilizzando i valori `Enabled` o `Disabled`. Se una regola è disabilitata, Amazon S3 non esegue le operazioni in essa specificate.
- L'elemento `<Priority>` indica quale regola ha la precedenza ogni volta che 2 o più regole di replica sono in conflitto. Amazon S3 prova a replicare gli oggetti in base a tutte le regole di replica. Tuttavia, se sono presenti 2 o più regole con lo stesso bucket di destinazione, gli oggetti vengono replicati in base alla regola con la priorità più alta. Più elevato è il numero, maggiore è la priorità.
- L'elemento `<DeleteMarkerReplication>` indica se replicare i contrassegni di eliminazione tramite i valori `Enabled` o `Disabled`.

Nella configurazione dell'elemento `<Destination>` è necessario specificare il nome del bucket o dei bucket di destinazione in cui Amazon S3 deve replicare gli oggetti.

Nell'esempio seguente sono indicati i requisiti minimi per una regola V2. Per la compatibilità con le versioni precedenti, Amazon S3 continua a supportare il formato XML V1. Per ulteriori informazioni, consulta [Considerazioni sulla compatibilità con le versioni precedenti](#).

```
...  
<Rule>
```

```

    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
      <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
  <Rule>
    ...
  </Rule>
  ...
  ...

```

Puoi anche specificare altre opzioni di configurazione. Ad esempio, puoi scegliere di utilizzare una classe di storage per le repliche degli oggetti diversa dalla classe dell'oggetto di origine.

Facoltativo: specifica di un filtro

Per scegliere un sottoinsieme di oggetti a cui si applica la regola, aggiungi un filtro facoltativo. Puoi filtrare in base al prefisso della chiave dell'oggetto, ai tag dell'oggetto o a una combinazione di entrambi. Se applichi un filtro in base sia al prefisso della chiave sia ai tag dell'oggetto, Amazon S3 combina i filtri utilizzando un operatore logico AND. In altre parole, la regola si applica a un sottoinsieme di oggetti con uno specifico prefisso della chiave e tag specifici.

Filtro in base al prefisso della chiave oggetto

Per specificare una regola con un filtro basato su un prefisso della chiave di un oggetto, utilizzare l'XML seguente. È possibile specificare un solo prefisso per regola.

```

<Rule>
  ...
  <Filter>
    <Prefix>key-prefix</Prefix>
  </Filter>
  ...
</Rule>

```

...

Filtro basato su tag oggetto

Per specificare una regola con un filtro basato sui tag di un oggetto, utilizzare l'XML seguente. Puoi specificare uno o più tag dell'oggetto.

```
<Rule>
  ...
  <Filter>
    <And>
      <Tag>
        <Key>key1</Key>
        <Value>value1</Value>
      </Tag>
      <Tag>
        <Key>key2</Key>
        <Value>value2</Value>
      </Tag>
      ...
    </And>
  </Filter>
  ...
</Rule>
...
```

Filtro con un prefisso chiave e tag oggetto

Per specificare un filtro della regola con una combinazione di prefisso della chiave e tag di un oggetto, utilizzare l'XML seguente. I filtri vengono uniti in un elemento padre <And>. Amazon S3 esegue un'operazione logica AND per combinare questi filtri. In altre parole, la regola si applica a un sottoinsieme di oggetti con uno specifico prefisso della chiave e tag specifici.

```
<Rule>
  ...
  <Filter>
    <And>
      <Prefix>key-prefix</Prefix>
      <Tag>
        <Key>key1</Key>
        <Value>value1</Value>
      </Tag>
    </And>
  </Filter>
  ...
</Rule>
```

```
        <Tag>
          <Key>key2</Key>
          <Value>value2</Value>
        </Tag>
        ...
      </Filter>
      ...
    </Rule>
    ...
```

Note

- Se si specifica una regola con un elemento `<Filter>` vuoto, la regola verrà applicata a tutti gli oggetti nel bucket.
- Quando si utilizzano regole di replica basate su tag con replica in tempo reale, occorre assegnare ai nuovi oggetti il tag della regola di replica corrispondente nell'operazione `PutObject`. In caso contrario, gli oggetti non verranno replicati. Non verranno replicati neanche gli oggetti a cui vengono assegnati tag dopo l'operazione `PutObject`.

Per replicare oggetti a cui sono stati assegnati tag dopo l'operazione `PutObject`, è necessario utilizzare Replica in batch S3. Per ulteriori informazioni su Batch Replication, consulta la sezione [Replica di oggetti esistenti](#).

Configurazioni di destinazione aggiuntive

Nella configurazione di destinazione devi specificare il bucket in cui Amazon S3 deve replicare gli oggetti. Puoi configurare la replica per replicare gli oggetti da un bucket di origine a uno solo o a più bucket di destinazione.

```
...
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
</Destination>
...
```

Puoi aggiungere le seguenti opzioni nell'elemento `<Destination>`.

Argomenti

- [Specifica della classe di storage](#)
- [Aggiunta di più bucket di destinazione](#)
- [Specifica di parametri diversi per ogni regola di replica con più bucket di destinazione](#)
- [Modifica della proprietà della replica](#)
- [Abilitazione di S3 Replication Time Control](#)
- [Replica gli oggetti creati con la crittografia lato server utilizzando AWS KMS](#)

Specifica della classe di storage

È possibile specificare la classe di storage per le repliche degli oggetti. Per impostazione predefinita, Amazon S3 utilizza la classe di storage dell'oggetto di origine per creare le repliche degli oggetti, come nell'esempio seguente.

```
...  
<Destination>  
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>  
  <StorageClass>storage-class</StorageClass>  
</Destination>  
...
```

Aggiunta di più bucket di destinazione

Puoi aggiungere più bucket di destinazione in una singola configurazione di replica, come indicato di seguito.

```
...  
<Rule>  
  <ID>Rule-1</ID>  
  <Status>Enabled-or-Disabled</Status>  
  <Priority>integer</Priority>  
  <DeleteMarkerReplication>  
    <Status>Enabled-or-Disabled</Status>  
  </DeleteMarkerReplication>  
  <Destination>  
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>  
  </Destination>  
</Rule>  
<Rule>  
  <ID>Rule-2</ID>
```



```

<Status>Enabled-or-Disabled</Status>
<Priority>integer</Priority>
<DeleteMarkerReplication>
  <Status>Enabled-or-Disabled</Status>
</DeleteMarkerReplication>
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
</Destination>
</Rule>
...

```

Specifica di parametri diversi per ogni regola di replica con più bucket di destinazione

Quando si aggiungono più bucket di destinazione in una singola configurazione di replica, puoi specificare parametri diversi per ogni regola di replica, come indicato di seguito.

```

...
<Rule>
  <ID>Rule-1</ID>
  <Status>Enabled-or-Disabled</Status>
  <Priority>integer</Priority>
  <DeleteMarkerReplication>
    <Status>Disabled</Status>
  </DeleteMarkerReplication>
  <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
  </Destination>
</Rule>
<Rule>
  <ID>Rule-2</ID>
  <Status>Enabled-or-Disabled</Status>
  <Priority>integer</Priority>
  <DeleteMarkerReplication>
    <Status>Enabled</Status>
  </DeleteMarkerReplication>
  <Metrics>
    <Status>Enabled</Status>
  </Metrics>

```

```

    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
  <Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
  </Destination>
</Rule>
...

```

Modifica della proprietà della replica

Quando i bucket di origine e di destinazione non sono di proprietà degli stessi account, è possibile modificare la proprietà della replica con Account AWS quella proprietaria del bucket di destinazione. A questo scopo, aggiungi l'elemento `<AccessControlTranslation>`. Questo elemento assume il valore `Destination`.

```

...
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <Account>destination-bucket-owner-account-id</Account>
  <AccessControlTranslation>
    <Owner>Destination</Owner>
  </AccessControlTranslation>
</Destination>
...

```

Se non aggiungi l'elemento `<AccessControlTranslation>` alla configurazione di replica, le repliche sono di proprietà dello stesso proprietario dell'oggetto Account AWS sorgente. Per ulteriori informazioni, consulta [Modifica del proprietario della replica](#).

Abilitazione di S3 Replication Time Control

Puoi abilitare S3 Replication Time Control (S3 RTC) nella configurazione di replica. S3 RTC replica la maggior parte degli oggetti in pochi secondi e il 99,99% degli oggetti entro 15 minuti, secondo un Accordo sul Livello di Servizio (SLA).

 Note

Per gli elementi `<EventThreshold>` e `<Time>` è accettato solo un valore valido di `<Minutes>15</Minutes>`.

```
...
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
</Destination>
...
```

Per ulteriori informazioni, consulta [Soddisfazione dei requisiti di conformità con il controllo del tempo di replica di Amazon S3](#). Per esempi di API, consulta [PutBucketReplication](#) nella Guida di riferimento per l'API di Amazon Simple Storage Service.

Replica gli oggetti creati con la crittografia lato server utilizzando AWS KMS

Il bucket di origine potrebbe contenere oggetti creati con la crittografia lato server utilizzando AWS Key Management Service (AWS KMS) keys. Per impostazione predefinita, Amazon S3 non replica questi oggetti. Puoi facoltativamente indicare ad Amazon S3 di replicare questi oggetti. Per farlo, innanzitutto abilita esplicitamente questa funzionalità aggiungendo l'elemento `<SourceSelectionCriteria>`. Quindi fornisci il AWS KMS key (per il bucket Regione AWS di destinazione) da utilizzare per crittografare le repliche degli oggetti. I seguenti esempi mostrano come specificare questi elementi.

```
...
<SourceSelectionCriteria>
```

```

<SseKmsEncryptedObjects>
  <Status>Enabled</Status>
</SseKmsEncryptedObjects>
</SourceSelectionCriteria>
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <EncryptionConfiguration>
    <ReplicaKmsKeyID>AWS KMS key ID to use for encrypting object replicas</
ReplicaKmsKeyID>
  </EncryptionConfiguration>
</Destination>
...

```

Per ulteriori informazioni, consulta [Replica di oggetti crittografati \(,,,\) SSE-S3 SSE-KMS DSSE-KMS SSE-C](#).

Esempi di configurazioni di replica

Per iniziare, puoi aggiungere le configurazioni di replica di esempio seguenti al bucket, in base alle esigenze.

Important

Per aggiungere una configurazione di replica a un bucket, devi disporre dell'autorizzazione `iam:PassRole`. Questa autorizzazione permette di passare il ruolo IAM che concede le autorizzazioni di replica ad Amazon S3. Puoi specificare il ruolo IAM fornendo l'Amazon Resource Name (ARN) utilizzato nell'elemento `<Role>` nel file XML della configurazione di replica. Per ulteriori informazioni, consulta [Concessione di autorizzazioni utente per il passaggio di un ruolo a Servizio AWS](#) nella Guida per l'utente di IAM.

Example 1: Configurazione di replica con una regola

La configurazione di replica di base seguente specifica una regola. La regola specifica un ruolo IAM che Amazon S3 può assumere e un singolo bucket di destinazione per le repliche degli oggetti. Se il valore dell'elemento `<Status>` è `Enabled` significa che la regola è in vigore.

```

<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>

```

```
<Rule>
  <Status>Enabled</Status>

  <Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  </Destination>
</Rule>
</ReplicationConfiguration>
```

Per scegliere un sottoinsieme di oggetti da replicare, puoi aggiungere un filtro. Nella configurazione seguente il filtro specifica un prefisso della chiave di un oggetto. Questa regola si applica agli oggetti con il prefisso *Tax/* nel nome della chiave.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
      <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
      <Prefix>Tax/</Prefix>
    </Filter>

    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

Se specifichi l'elemento `<Filter>`, devi includere anche gli elementi `<Priority>` e `<DeleteMarkerReplication>`. In questo esempio, il valore impostato per l'elemento `<Priority>` non è rilevante perché è presente solo una regola.

Nella configurazione seguente, il filtro specifica 1 prefisso e 2 tag. La regola si applica al sottoinsieme di oggetti con il prefisso della chiave e i tag specificati. In particolare, si applica agli oggetti che hanno il *Tax/* prefisso nei nomi delle chiavi e i 2 tag oggetto specificati. In questo esempio, il valore impostato per l'elemento `<Priority>` non è rilevante perché è presente solo una regola.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
      <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
      <And>
        <Prefix>Tax</Prefix>
        <Tag>
          <Tag>
            <Key>tagA</Key>
            <Value>valueA</Value>
          </Tag>
          <Tag>
            <Key>tagB</Key>
            <Value>valueB</Value>
          </Tag>
        </And>
      </Filter>

      <Destination>
        <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
      </Destination>

    </Rule>
  </ReplicationConfiguration>
```

È possibile specificare una classe di storage per le repliche degli oggetti come illustrato di seguito:

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
```

```

<Status>Enabled</Status>
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <StorageClass>storage-class</StorageClass>
</Destination>
</Rule>
</ReplicationConfiguration>

```

È possibile specificare qualsiasi classe di storage supportata da Amazon S3.

Example 2: Configurazione della replica con 2 regole

Example

Nella seguente configurazione della replica, le regole specificano che:

- Ogni regola filtra in base a un prefisso della chiave diverso, per cui ogni regola si applica a un sottoinsieme di oggetti diverso. In questo esempio, Amazon S3 replica gli oggetti con i nomi di chiave *Tax/doc1.pdf* e *Project/project1.txt*, ma non gli oggetti con il nome di chiave *PersonalDoc/documentA*.
- Sebbene entrambe le regole specifichino un valore per l'<Priority>elemento, la priorità della regola è irrilevante perché le regole si applicano a 2 set distinti di oggetti. L'esempio successivo mostra cosa accade quando viene applicata la priorità delle regole.
- La seconda regola specifica la classe di Standard-IA archiviazione S3 per le repliche degli oggetti. Amazon S3 usa la classe di storage specificata per tali repliche.

```

<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
      <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
      <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
  </Rule>

```

```

    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
    ...
  </Rule>
<Rule>
  <Status>Enabled</Status>
  <Priority>2</Priority>
  <DeleteMarkerReplication>
    <Status>string</Status>
  </DeleteMarkerReplication>
  <Filter>
    <Prefix>Project</Prefix>
  </Filter>
  <Status>Enabled</Status>
  <Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    <StorageClass>STANDARD_IA</StorageClass>
  </Destination>
  ...
</Rule>

</ReplicationConfiguration>

```

Example 3: Configurazione della replica con 2 regole con prefissi sovrapposti

In questa configurazione, le 2 regole specificano i filtri con prefissi di chiave sovrapposti e. *star* *starship* Entrambe le regole si applicano agli oggetti con il nome di chiave *starship-x*. In questo caso, Amazon S3 utilizza la priorità delle regole per determinare quale regola applicare. Più elevato è il numero, maggiore è la priorità.

```

<ReplicationConfiguration>

  <Role>arn:aws:iam::account-id:role/role-name</Role>

  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
      <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>

```



```

    <Prefix>star</Prefix>
  </Filter>
  <Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  </Destination>
</Rule>
<Rule>
  <Status>Enabled</Status>
  <Priority>2</Priority>
  <DeleteMarkerReplication>
    <Status>string</Status>
  </DeleteMarkerReplication>
  <Filter>
    <Prefix>starship</Prefix>
  </Filter>
  <Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  </Destination>
</Rule>
</ReplicationConfiguration>

```

Example 4: Procedure dettagliate di esempio

Per le procedure dettagliate di esempio, consulta [Esempi di configurazione della replica in tempo reale](#).

Per ulteriori informazioni sulla struttura XML della configurazione di replica, consulta Amazon Simple Storage [PutBucketReplication](#) Service API Reference.

Considerazioni sulla compatibilità con le versioni precedenti

La versione più recente del formato XML di configurazione della replica è V2. Le configurazioni di replica XML V2 sono quelle che contengono l'elemento `<Filter>` per le regole e le regole che specificano S3 Replication Time Control (S3 RTC).

Per visualizzare la versione della configurazione di replica, puoi utilizzare l'operazione API `GetBucketReplication`. Per ulteriori informazioni, consulta [GetBucketReplication](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Per la compatibilità con le versioni precedenti, Amazon S3 continua a supportare il formato di configurazione della replica XML V1. Se si è utilizzato il formato di configurazione della replica XML V1, tenere presenti i seguenti problemi relativi alla compatibilità con le versioni precedenti:

- Il formato di configurazione della replica XML V2 include l'elemento `<Filter>` per le regole. Con l'elemento `<Filter>`, puoi specificare filtri di oggetti basati sul prefisso della chiave o sui tag dell'oggetto, oppure su entrambi gli elementi, per specificare gli oggetti a cui si applica la regola. Il formato di configurazione della replica XML V1 supporta il filtro solo in base al prefisso della chiave. In tal caso, aggiungere l'elemento `<Prefix>` direttamente come elemento figlio dell'elemento `<Rule>`, come nell'esempio seguente:

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

- Quando elimini un oggetto dal bucket di origine senza specificare un ID versione, Amazon S3 aggiunge un contrassegno di eliminazione. Se si utilizza il formato di configurazione della replica XML V1, le repliche Amazon S3 eliminano solo i contrassegni derivanti dalle operazioni dell'utente. In altre parole, Amazon S3 esegue la replica del contrassegno di eliminazione solo se un utente elimina un oggetto. Se un oggetto scaduto viene rimosso da Amazon S3 (come parte di un'operazione del ciclo di vita), Amazon S3 non replicherà il contrassegno di eliminazione.

Nel formato di configurazione della replica XML V2, è possibile abilitare la replica dei contrassegni di eliminazione per le regole non basate su tag. Per ulteriori informazioni, consulta [Replica dei contrassegni di eliminazione tra i bucket](#).

Configurazione delle autorizzazioni per la replica in tempo reale

Per la configurazione della replica in tempo reale in Amazon S3, occorre acquisire le autorizzazioni necessarie, come indicato di seguito:

- È necessario concedere al principale AWS Identity and Access Management (IAM) (utente o ruolo) che creerà le regole di replica un determinato set di autorizzazioni.

- Amazon S3 necessita delle autorizzazioni per replicare gli oggetti per tuo conto. Queste autorizzazioni vengono concesse creando un ruolo IAM e specificandolo nella configurazione di replica.
- Quando i bucket di origine e di destinazione non sono di proprietà degli stessi account, il proprietario del bucket di destinazione deve concedere al proprietario del bucket di origine anche le autorizzazioni per archiviare le repliche.

Note

Se si utilizza Operazioni in batch S3 per replicare gli oggetti on demand anziché configurare la replica in tempo reale, le policy e un ruolo IAM diversi sono necessari per Replica in batch S3. Per esempi di policy e ruoli IAM di Replica in batch, consulta [Configurazione di un ruolo IAM per Replica in batch S3](#).

Argomenti

- [Fase 1. Concessione di autorizzazioni al principale IAM che crea le regole di replica](#)
- [Fase 2. Creazione di un ruolo IAM per Amazon S3](#)
- [\(Facoltativo\) Fase 3: concessione delle autorizzazioni quando i bucket di origine e di destinazione sono di proprietà di soggetti diversi Account AWS](#)
- [\(Facoltativo\) Fase 4. Concessione di autorizzazioni per modificare la proprietà della replica](#)

Fase 1. Concessione di autorizzazioni al principale IAM che crea le regole di replica

L'utente o il ruolo IAM da utilizzare per creare le regole di replica necessita delle autorizzazioni per creare regole per repliche unidirezionali o bidirezionali. Se l'utente o il ruolo non dispone di queste autorizzazioni, non è possibile creare regole di replica. Per ulteriori informazioni, consulta [Identità IAM](#) nella Guida per l'utente IAM.

L'utente o il ruolo necessita delle seguenti azioni:

- iam:AttachRolePolicy
- iam:CreatePolicy
- iam:CreateServiceLinkedRole
- iam:PassRole

- iam:PutRolePolicy
- s3:GetBucketVersioning
- s3:GetObjectVersionAcl
- s3:GetObjectVersionForReplication
- s3:GetReplicationConfiguration
- s3:PutReplicationConfiguration

Di seguito è riportato un esempio di policy IAM che include queste azioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetAccessPoint",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:PutReplicationConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:GetBucketVersioning",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionAcl",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetObjectVersion",
        "s3:GetBucketOwnershipControls",
        "s3:PutBucketOwnershipControls",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetBucketObjectLockConfiguration"
      ]
    }
  ],
}
```

```

        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1-*",
            "arn:aws:s3:::amzn-s3-demo-bucket2-*/*"
        ],
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:List*AccessPoint*",
            "s3:GetMultiRegion*"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:Get*",
            "iam:CreateServiceLinkedRole",
            "iam:CreateRole",
            "iam:PassRole"
        ],
        "Resource": "arn:aws:iam::*:role/service-role/s3*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:List*"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:PutRolePolicy",
            "iam:CreatePolicy"
        ],
        "Resource": [
            "arn:aws:iam::*:policy/service-role/s3*",
            "arn:aws:iam::*:role/service-role/s3*"
        ]
    }
]
}

```

Fase 2. Creazione di un ruolo IAM per Amazon S3

Di default, tutte le risorse di Amazon S3, ossia bucket, oggetti e risorse secondarie correlate, sono private e solo il proprietario vi può accedere. Amazon S3 ha bisogno di autorizzazioni per leggere e replicare gli oggetti dal bucket di origine. Queste autorizzazioni vengono concesse creando un ruolo IAM e specificandolo nella configurazione della replica.

In questa sezione vengono illustrate la policy di attendibilità e la policy di autorizzazione minima richiesta associate a questo ruolo IAM. Le procedure dettagliate di esempio forniscono istruzioni dettagliate per la creazione di un ruolo IAM. Per ulteriori informazioni, consulta [Esempi di configurazione della replica in tempo reale](#).

Note

Se si utilizza la console per creare la configurazione di replica, è consigliabile saltare questa sezione e lasciare che sia invece la console a creare automaticamente questo ruolo IAM e le policy di attendibilità e autorizzazione necessarie.

La policy di attendibilità identifica le identità principali che possono assumere il ruolo IAM. La policy di autorizzazione specifica le azioni che il ruolo IAM può eseguire, su quali risorse e in quali condizioni.

- L'esempio seguente mostra una politica di fiducia in cui si identifica Amazon S3 come il Servizio AWS principale che può assumere il ruolo:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
}
```

- Di seguito viene mostrata una policy di attendibilità esemplificativa in cui si identifica Amazon S3 e Operazioni in batch S3 come principali del servizio che può assumere il ruolo. Usare questo approccio quando si crea un processo Replica in batch. Per ulteriori informazioni, consulta [Creazione di un processo Replica in batch per nuove destinazioni o regole di replica](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "s3.amazonaws.com",
          "batchoperations.s3.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Per ulteriori informazioni sui ruoli IAM, consulta [Ruoli IAM](#) nella Guida per l'utente di IAM.

- Di seguito viene mostrata una policy di autorizzazioni esemplificativa in cui si concedono al ruolo IAM le autorizzazioni per eseguire attività di replica per proprio conto. Quando Amazon S3 assume il ruolo, dispone delle autorizzazioni che sono state specificate in questa policy. In questa politica, *amzn-s3-demo-source-bucket* è il bucket di origine e *amzn-s3-demo-destination-bucket* è il nome del bucket di destinazione.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetReplicationConfiguration",
        "s3:ListBucket"
      ]
    }
  ]
}
```

```
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
]
```

La policy di autorizzazioni concede le autorizzazioni per le seguenti azioni:

- `s3:GetReplicationConfiguration` e `s3:ListBucket`: le autorizzazioni per queste azioni sul bucket *amzn-s3-demo-source-bucket* consentono ad Amazon S3 di recuperare la configurazione della replica ed elencare il contenuto del bucket. (Il modello di autorizzazioni corrente richiede l'autorizzazione `s3:ListBucket` per l'accesso ai contrassegni di eliminazione.)
- `s3:GetObjectVersionForReplication` e `s3:GetObjectVersionAcl`: le autorizzazioni per queste operazioni concesse su tutti gli oggetti permettono ad Amazon S3 di ottenere una versione dell'oggetto specifica e la lista di controllo degli accessi (ACL) associata agli oggetti.
- `s3:ReplicateObject` e `s3:ReplicateDelete`: le autorizzazioni per queste operazioni sugli oggetti nel bucket di *amzn-s3-demo-destination-bucket* permettono ad Amazon S3 di replicare gli oggetti o i contrassegni di eliminazione nel bucket di destinazione. Per informazioni

sui contrassegni di eliminazione, consulta la sezione [Effetto delle operazioni di eliminazione sulla replica](#).

Note

Le autorizzazioni per l'azione `s3:ReplicateObject` nel bucket *amzn-s3-demo-destination-bucket* consentono anche la replica dei metadati, come i tag degli oggetti e le liste di controllo degli accessi. Pertanto non è necessario concedere esplicitamente l'autorizzazione per l'operazione `s3:ReplicateTags`.

- `s3:GetObjectVersionTagging`: le autorizzazioni per questa azione sugli oggetti nel bucket *amzn-s3-demo-source-bucket* permettono ad Amazon S3 di leggere i tag degli oggetti per la replica. Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#). Se non dispone dell'autorizzazione `s3:GetObjectVersionTagging`, Amazon S3 replica gli oggetti ma non i relativi tag.
- `s3:GetObjectVersionAnnotationForReplication`— Le autorizzazioni per questa azione sugli oggetti nel bucket di origine consentono ad Amazon S3 di leggere le annotazioni per la replica. Se Amazon S3 non dispone di questa autorizzazione, la replica delle annotazioni ha esito negativo. Per ulteriori informazioni sulle annotazioni, consulta [Annotazione degli oggetti](#)

Per visualizzare un elenco di operazioni Amazon S3, consulta [Operazioni, risorse e chiavi di condizione per Amazon S3](#) nella Guida di riferimento per l'autorizzazione al servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Important

Il Account AWS proprietario del ruolo IAM deve disporre delle autorizzazioni per le azioni che concede al ruolo IAM.

Supponiamo ad esempio che il bucket di origine contenga oggetti di proprietà di un altro Account AWS. Il proprietario degli oggetti deve concedere esplicitamente al proprietario del ruolo IAM Account AWS le autorizzazioni richieste tramite gli elenchi di controllo degli accessi (ACL) degli oggetti. In caso contrario, Amazon S3 non può accedere agli oggetti e la replica degli oggetti ha esito negativo. Per informazioni sulle autorizzazioni ACL, consulta la sezione [Panoramica delle liste di controllo accessi \(ACL\)](#).

Le autorizzazioni descritte si riferiscono alla configurazione di replica minima. Se scegli di aggiungere configurazioni di replica facoltative, è necessario fornire ulteriori autorizzazioni ad Amazon S3:

- Per replicare oggetti crittografati, è necessario anche fornire le autorizzazioni per la chiave AWS Key Management Service (AWS KMS) necessarie. Per ulteriori informazioni, consulta [the section called “Replica di oggetti crittografati”](#).
- Per utilizzare Object Lock con la replica, devi concedere 2 autorizzazioni aggiuntive sul bucket S3 di origine nel ruolo AWS Identity and Access Management (IAM) utilizzato per configurare la replica. Le 2 autorizzazioni aggiuntive sono `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se il ruolo dispone di un'istruzione di autorizzazione `s3:Get*`, tale istruzione soddisfa il requisito. Per ulteriori informazioni, consulta [the section called “Utilizzo di Object Lock con la replica S3”](#).

(Facoltativo) Fase 3: concessione delle autorizzazioni quando i bucket di origine e di destinazione sono di proprietà di soggetti diversi Account AWS

Quando i bucket di origine e di destinazione non sono di proprietà degli stessi account, il proprietario del bucket di destinazione deve aggiungere anche una policy di bucket per concedere al proprietario del bucket di origine le autorizzazioni per eseguire le operazioni di replica, come mostrato nel seguente esempio. In questa policy di esempio, *amzn-s3-demo-destination-bucket* è il nome del bucket di destinazione.

È possibile utilizzare la console Amazon S3 anche per generare automaticamente questa policy di bucket. Per ulteriori informazioni, consulta [Abilita la ricezione di oggetti replicati da un bucket di origine](#).

Note

Il formato ARN del ruolo può apparire diverso. Se il ruolo è stato creato utilizzando la console, il formato ARN è `arn:aws:iam::account-ID:role/service-role/role-name`. Se il ruolo è stato creato utilizzando il AWS CLI, il formato ARN è `arn:aws:iam::account-ID:role/role-name`. Per ulteriori informazioni, consulta [Ruoli IAM](#) nella Guida per l'utente IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PolicyForDestinationBucket",
  "Statement": [
    {
      "Sid": "Permissions on objects",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/service-role/source-account-IAM-role"
      },
      "Action": [
        "s3:ReplicateDelete",
        "s3:ReplicateObject"
      ],
      "Resource": "arn:aws:s3::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Sid": "Permissions on bucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/service-role/source-account-IAM-role"
      },
      "Action": [
        "s3:List*",
        "s3:GetBucketVersioning",
        "s3:PutBucketVersioning"
      ],
      "Resource": "arn:aws:s3::amzn-s3-demo-destination-bucket"
    }
  ]
}
```

Per un esempio, consulta [Configurazione della replica per i bucket in account diversi](#).

In presenza di oggetti con tag nel bucket di origine, tenere in considerazione quanto segue:

- Se il proprietario del bucket di origine concede ad Amazon S3 l'autorizzazione per le operazioni `s3:GetObjectVersionTagging` e `s3:ReplicateTags` per replicare i tag degli oggetti (tramite il ruolo IAM), Amazon S3 replica i tag insieme agli oggetti. Per informazioni sul ruolo IAM, consulta [Fase 2. Creazione di un ruolo IAM per Amazon S3](#).
- Se il proprietario del bucket di destinazione non desidera replicare i tag, può aggiungere l'istruzione seguente alla policy del bucket di destinazione per rifiutare esplicitamente l'autorizzazione per l'operazione `s3:ReplicateTags`. In questa politica, *amzn-s3-demo-destination-bucket* è il nome del bucket di destinazione.

```
...
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::source-bucket-account-id:role/service-role/source-account-IAM-role"
      },
      "Action": "s3:ReplicateTags",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
  ...
```

- Allo stesso modo, se il proprietario del bucket di origine concede ad Amazon S3 l'autorizzazione per l'`s3:GetObjectVersionAnnotationForReplication` di replica delle annotazioni (tramite il ruolo IAM), Amazon S3 replica le annotazioni insieme agli oggetti. Per informazioni sul ruolo IAM, consulta [Fase 2. Creazione di un ruolo IAM per Amazon S3](#).

Se il proprietario del bucket di destinazione non desidera replicare le annotazioni, può aggiungere la seguente dichiarazione alla policy del bucket di destinazione per negare esplicitamente l'autorizzazione all'azione. `s3:ReplicateObjectAnnotation` In questa policy, *amzn-s3-demo-destination-bucket* è il nome del bucket di destinazione.

```
...
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::source-bucket-account-id:role/service-role/source-account-IAM-role"
      },
      "Action": "s3:ReplicateObjectAnnotation",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
  ...
```

```
    },  
    "Action": "s3:ReplicateObjectAnnotation",  
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"  
  }  
]  
...
```

Note

- Se si desidera replicare oggetti crittografati, è opportuno anche concedere le autorizzazioni chiave AWS Key Management Service (AWS KMS) necessarie. Per ulteriori informazioni, consulta [the section called “Replica di oggetti crittografati”](#).
- Per utilizzare Object Lock con la replica, devi concedere 2 autorizzazioni aggiuntive sul bucket S3 di origine nel ruolo AWS Identity and Access Management (IAM) che utilizzi per configurare la replica. Le 2 autorizzazioni aggiuntive sono e. `s3:GetObjectRetention` `s3:GetObjectLegalHold` Se il ruolo dispone di un'istruzione di autorizzazione `s3:Get*`, tale istruzione soddisfa il requisito. Per ulteriori informazioni, consulta [the section called “Utilizzo di Object Lock con la replica S3”](#).

Abilitare la ricezione di oggetti replicati da un bucket di origine

Anziché aggiungere manualmente la policy precedente al bucket di destinazione, è possibile generare rapidamente le policy necessarie per abilitare la ricezione di oggetti replicati da un bucket di origine tramite la console Amazon S3.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckete, scegliere il bucket da utilizzare come bucket di destinazione.
4. Seleziona la scheda Gestione, quindi scorri verso il basso fino a Regole di replica.
5. Per Operazioni, scegliere Ricevi oggetti replicati.

Segui le istruzioni e inserisci l' Account AWS ID dell'account bucket di origine, quindi scegli Genera policy. La console genera una policy del bucket Amazon S3 e una policy della chiave KMS.

6. Per aggiungere questa policy alla policy del bucket esistente, scegli **Applica le impostazioni** oppure scegli **Copia** per copiare manualmente le modifiche.
7. (Facoltativo) Copia la AWS KMS policy nella policy chiave KMS desiderata nella console. AWS Key Management Service

(Facoltativo) Fase 4. Concessione di autorizzazioni per modificare la proprietà della replica

Se Account AWS i bucket di origine e di destinazione sono diversi, puoi dire ad Amazon S3 di cambiare la proprietà della replica con Account AWS quella proprietaria del bucket di destinazione. Per ignorare la proprietà delle repliche, è necessario fornire alcune autorizzazioni aggiuntive o modificare le impostazioni **Proprietà dell'oggetto S3** per il bucket di destinazione. Per ulteriori informazioni sulla sovrascrittura del proprietario, consulta [Modifica del proprietario della replica](#).

Esempi di configurazione della replica in tempo reale

Nei seguenti esempi vengono fornite istruzioni dettagliate che mostrano come configurare la replica in tempo reale per i casi d'uso comuni.

Note

La replica in tempo reale si riferisce alla Same-Region replica (SRR) e Cross-Region alla replica (CRR). La replica in tempo reale non esegue la replica degli oggetti esistenti nel bucket prima della configurazione della replica. Per replicare oggetti esistenti prima della configurazione della replica, occorre ricorrere alla replica on demand. Per sincronizzare bucket e replicare gli oggetti esistenti on demand, consulta [Replica di oggetti esistenti](#).

Questi esempi dimostrano come creare una configurazione di replica utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e gli AWS SDK (e vengono mostrati alcuni esempi).AWS SDK per Java AWS SDK per .NET

Per informazioni sull'installazione e la configurazione di AWS CLI, consulta i seguenti argomenti nella Guida per l'utente: AWS Command Line Interface

- [Inizia con AWS CLI](#)
- [Configura AWS CLI](#): è necessario impostare almeno un profilo. Se stai esplorando scenari per più account, devi impostare due profili.

Per informazioni sugli AWS SDK, consulta [AWS SDK per Java](#) e [AWS SDK per .NET](#).

 Tip

Per un tutorial dettagliato che dimostra come utilizzare la replica in tempo reale per replicare i dati, vedi [Tutorial: Replicating data within and between using S3 Replication. Regioni AWS](#)

Argomenti

- [Configurazione della replica per i bucket nello stesso account](#)
- [Configurazione della replica per i bucket in account diversi](#)
- [Soddisfazione dei requisiti di conformità con il controllo del tempo di replica di Amazon S3](#)
- [Replica di oggetti crittografati \(,,,\) SSE-S3 SSE-KMS DSSE-KMS SSE-C](#)
- [Replica delle modifiche ai metadati con la sincronizzazione delle modifiche alla replica](#)
- [Replica dei contrassegni di eliminazione tra i bucket](#)
- [Replica delle annotazioni](#)

Configurazione della replica per i bucket nello stesso account

La replica in tempo reale è la copia automatica e asincrona di oggetti su bucket generici, uguali o diversi. Regioni AWS La replica in tempo reale copia gli oggetti appena creati e gli aggiornamenti degli oggetti da un bucket di origine in uno o più bucket di destinazione. Per ulteriori informazioni, consulta [Replica di oggetti all'interno e tra le Regioni](#).

Quando si configura la replica, vengono aggiunte le regole di replica al bucket di origine. Le regole di replica definiscono gli oggetti del bucket di origine da replicare e i bucket di destinazione in cui vengono archiviati gli oggetti replicati. È possibile creare una regola per replicare tutti gli oggetti in un bucket o un sottoinsieme di oggetti con un prefisso di nome di chiave specifico, uno o più tag di oggetto o entrambi gli elementi. Un bucket di destinazione può trovarsi nello stesso bucket Account AWS di origine oppure in un account diverso.

Se specifichi l'ID della versione dell'oggetto da eliminare, Amazon S3 elimina la versione dell'oggetto nel bucket di origine. Ma non replica l'eliminazione nel bucket di destinazione. In altre parole, non elimina la stessa versione dell'oggetto dal bucket di destinazione. Ciò permette di proteggere i dati da eliminazioni da parte di utenti malintenzionati.

Quando si aggiunge una regola di replica a un bucket, la regola viene abilitata per impostazione predefinita e pertanto inizia a funzionare non appena viene salvata.

In questo esempio viene configurata la replica per i bucket di origine e di destinazione di proprietà dello stesso Account AWS. Vengono forniti esempi per l'utilizzo della console Amazon S3, the AWS Command Line Interface (AWS CLI) e and. AWS SDK per Java AWS SDK per .NET

Prerequisiti

Prima di utilizzare le seguenti procedure, assicurati di aver impostato le autorizzazioni necessarie per la replica, a seconda che i bucket di origine e destinazione siano di proprietà dello stesso account o di account diversi. Per ulteriori informazioni, consulta [the section called “Impostazione delle autorizzazioni”](#).

Note

- Se si desidera replicare oggetti crittografati, è opportuno anche concedere le autorizzazioni chiave AWS Key Management Service (AWS KMS) necessarie. Per ulteriori informazioni, consulta [the section called “Replica di oggetti crittografati”](#).
- Per utilizzare Object Lock con la replica, devi concedere due autorizzazioni aggiuntive sul bucket S3 di origine nel ruolo AWS Identity and Access Management (IAM) utilizzato per configurare la replica. Le due nuove autorizzazioni aggiuntive sono `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se il ruolo dispone di un'istruzione di autorizzazione `s3:Get*`, tale istruzione soddisfa il requisito. Per ulteriori informazioni, consulta [the section called “Utilizzo di Object Lock con la replica S3”](#).

Utilizzo della console S3

Per configurare una regola di replica quando il bucket di destinazione è nello stesso bucket di origine, segui Account AWS questi passaggi.

Se il bucket di destinazione si trova in un account diverso rispetto al bucket di origine, è necessario aggiungere al bucket di destinazione una policy di bucket per concedere al proprietario dell'account del bucket di origine l'autorizzazione per replicare gli oggetti nel bucket di destinazione. Per ulteriori informazioni, consulta [\(Facoltativo\) Fase 3: concessione delle autorizzazioni quando i bucket di origine e di destinazione sono di proprietà di soggetti diversi Account AWS](#).

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket desiderato.
4. Seleziona la scheda Gestione, scorri verso il basso fino a Regole di replica e quindi scegli Crea regola di replica.
5. Nella sezione Configurazione della regola di replica, in Nome della regola di replica, specifica il nome della regola per semplificarne l'identificazione in un secondo momento. Il nome è obbligatorio e deve essere univoco all'interno del bucket.
6. In Status (Stato), l'opzione Enabled (Abilitata) è selezionata per impostazione predefinita. Una regola abilitata inizia a funzionare non appena viene salvata. Se desideri abilitare la regola in un secondo momento, scegli Disabilitata.
7. Se il bucket dispone di regole di replica esistenti, viene chiesto di impostare una priorità per la regola. È necessario impostare una priorità per la regola per evitare i conflitti causati dagli oggetti inclusi nell'ambito di più regole. In caso di regole sovrapposte, Amazon S3 utilizza la priorità delle regole per determinare quale regola applicare. Più elevato è il numero, maggiore è la priorità. Per ulteriori informazioni sulla priorità delle regole, consulta [Elementi del file di configurazione della replica](#).
8. In Bucket di origine sono disponibili le seguenti opzioni per l'impostazione dell'origine della replica:
 - Per replicare l'intero bucket, scegli Apply to all objects in the bucket (Applica a tutti gli oggetti nel bucket).
 - Per replicare tutti gli oggetti con lo stesso prefisso, scegli Limita l'ambito di questa regola utilizzando uno o più filtri. Ciò limita la replica a tutti gli oggetti con nomi che iniziano il prefisso specificato, ad esempio pictures. Immetti un prefisso nella casella Prefisso.

 Note

Se si immette un prefisso corrispondente al nome di una cartella, è necessario utilizzare / (barra) come ultimo carattere (ad esempio, pictures/).

- Per replicare tutti gli oggetti con uno o più tag oggetto, scegli Aggiungi tag e specifica la coppia chiave-valore nelle caselle. Per aggiungere un altro tag, ripetere la procedura. È possibile

combinare un prefisso con i tag. Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#).

Il nuovo schema XML della configurazione della replica supporta il filtro basato su prefissi e tag e l'impostazione della priorità delle regole. Per ulteriori informazioni sul nuovo schema, consulta [Considerazioni sulla compatibilità con le versioni precedenti](#). Per ulteriori informazioni sull'XML utilizzato con l'API Amazon S3 che funziona con l'interfaccia utente, consulta [Elementi del file di configurazione della replica](#). Il nuovo schema è descritto come configurazione di replica XML V2.

9. In Destinazione, scegli il bucket in cui desideri che Amazon S3 esegui la replica degli oggetti.

 Note

Il numero di bucket di destinazione è limitato al numero di bucket Regioni AWS presenti in una determinata partizione. Una partizione è un raggruppamento di regioni. AWS attualmente ha tre partizioni: aws (Regioni standard), aws-cn (Regioni cinesi) e aws-us-gov (AWS GovCloud (US) Regioni). È possibile utilizzare le [Service Quotas](#) per richiedere un aumento del limite per i bucket di destinazione.

- Per eseguire la replica in un periodo fisso nel tuo account, seleziona Scegli un bucket in questo account e digita o cerca i bucket di destinazione.
- Per eseguire la replica su uno o più bucket in un altro account Account AWS, scegli Specifica un bucket in un altro account e inserisci l'ID dell'account del bucket di destinazione e il nome del bucket.

Se il bucket di destinazione si trova in un account diverso rispetto al bucket di origine, dovrai aggiungere ai bucket di destinazione una policy di bucket per concedere al proprietario dell'account del bucket di origine l'autorizzazione per replicare gli oggetti nei bucket di destinazione. Per ulteriori informazioni, consulta [\(Facoltativo\) Fase 3: concessione delle autorizzazioni quando i bucket di origine e di destinazione sono di proprietà di soggetti diversi Account AWS](#).

Facoltativamente, se desideri standardizzare la proprietà dei nuovi oggetti nel bucket di destinazione, seleziona Assegna la proprietà degli oggetti al proprietario del bucket di destinazione. Per ulteriori informazioni su questa opzione, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

 Note

Se la funzione Controllo delle versioni non è abilitata nel bucket di destinazione, viene visualizzato un messaggio di avviso contenente un pulsante **Abilita Controllo delle versioni**. Seleziona questo pulsante per abilitare la funzione Controllo delle versioni nel bucket.

10. Configura un ruolo AWS Identity and Access Management (IAM) che Amazon S3 può assumere per replicare gli oggetti per tuo conto.

Per impostare un ruolo IAM, nella sezione **Ruolo IAM** seleziona uno dei seguenti valori nell'elenco a discesa **Ruolo IAM**:

- Consigliamo di scegliere **Crea nuovo ruolo per fare in modo che Amazon S3 crei un nuovo ruolo IAM per l'utente**. Quando salvi la regola, viene generata una nuova policy per il ruolo IAM corrispondente ai bucket di origine e di destinazione scelti.
- Puoi decidere di utilizzare un ruolo IAM esistente. In tal caso, è necessario scegliere un ruolo che conceda ad Amazon S3 le autorizzazioni necessarie per la replica. Se questo ruolo non concede autorizzazioni sufficienti ad Amazon S3 per seguire la regola di replica, la replica non riesce.

 Important

Quando si aggiunge una regola di replica a un bucket, si deve disporre dell'autorizzazione `iam:PassRole` per poter passare il ruolo IAM che concede le autorizzazioni di replica Amazon S3. Per ulteriori informazioni, consulta [Concessione di autorizzazioni utente per il passaggio di un ruolo a un Servizio AWS](#) nella Guida per l'utente di IAM.

11. Per replicare oggetti nel bucket di origine crittografati con crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS), in **Crittografia**, seleziona **Replica oggetti crittografati con**. AWS KMS In **Chiavi AWS KMS per crittografare gli oggetti di destinazione** sono disponibili le chiavi di origine che consentono la replica da utilizzare. Tutte le chiavi KMS di origine sono incluse per impostazione predefinita. Per limitare la selezione delle chiavi KMS, puoi scegliere un alias o un ID chiave.

Gli oggetti crittografati con AWS KMS keys quelli non selezionati non vengono replicati.

Viene scelta una chiave KMS o un gruppo di chiavi KMS, ma se lo desideri puoi scegliere le chiavi KMS. Per informazioni sull'utilizzo AWS KMS con la replica, vedere. [Replica di oggetti crittografati \(,,,\) SSE-S3 SSE-KMS DSSE-KMS SSE-C](#)

 Important

Quando si replicano oggetti crittografati con AWS KMS, la frequenza delle AWS KMS richieste raddoppia nella regione di origine e aumenta della stessa quantità nella regione di destinazione. L'aumento delle velocità di chiamata è dovuto anche al modo in cui i dati AWS KMS vengono nuovamente crittografati utilizzando la chiave KMS definita per la regione di destinazione della replica. AWS KMS ha una quota di richieste per account chiamante e per regione. Per informazioni sulle quote predefinite, consulta la sezione [Quote di AWS KMS - richieste al secondo: variabili](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Se l'attuale percentuale di richieste di PUT oggetti Amazon S3 durante la replica è superiore alla metà del limite predefinito AWS KMS per il tuo account, ti consigliamo di richiedere un aumento della quota di AWS KMS richieste. Per richiedere un incremento, invia una richiesta tramite il Supporto Center nella sezione [Contatti](#). Ad esempio, supponiamo che il tuo attuale tasso di richieste di PUT oggetti sia di 1.000 richieste al secondo e che tu lo usi per AWS KMS crittografare i tuoi oggetti. In questo caso, ti consigliamo di chiedere Supporto di aumentare il limite AWS KMS di velocità a 2.500 richieste al secondo, nelle regioni di origine e di destinazione (se diverse), per assicurarti che non vi siano limitazioni. AWS KMS

Per visualizzare la frequenza di richieste di PUT oggetti nel bucket di origine, consulta le metriche delle CloudWatch richieste PutRequests di Amazon per Amazon S3. Per informazioni sulla visualizzazione delle CloudWatch metriche, consulta. [Utilizzo della console S3](#)

Se hai scelto di replicare oggetti crittografati con AWS KMS, procedi come segue:

- In AWS KMS key per crittografare gli oggetti di destinazione, specifica la tua chiave KMS in uno dei seguenti modi:
 - Per effettuare una selezione in un elenco di chiavi KMS disponibili, seleziona Scegli tra le chiavi AWS KMS keys e quindi scegli una chiave KMS dell'elenco delle chiavi disponibili.

In questo elenco vengono visualizzate sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente. Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta [Chiavi gestite dal cliente e chiavi AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Per inserire il nome della risorsa Amazon (ARN) della chiave KMS, scegli Inserisci ARN AWS KMS key e specifica l'ARN della chiave KMS nel campo visualizzato. In questo modo vengono crittografate le repliche nel bucket di destinazione. È possibile trovare l'ARN per la chiave KMS nella [console IAM](#) in Chiavi di crittografia.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creazione di chiavi](#) nella Guida per gli AWS Key Management Service sviluppatori.

 Important

È possibile utilizzare solo le chiavi KMS abilitate contemporaneamente Regione AWS al bucket. Quando selezioni Scegli tra le chiavi KMS, la console S3 elenca solo 100 chiavi KMS per regione. Se hai oltre 100 chiavi KMS nella stessa regione, puoi vedere solo i primi le prime 100 nella console S3. Per utilizzare una chiave KMS non elencata nella console, seleziona Inserisci ARN AWS KMS key e specifica l'ARN della chiave KMS.

Quando utilizzi una AWS KMS key crittografia lato server in Amazon S3, devi scegliere una chiave KMS di crittografia simmetrica. Amazon S3 supporta solo chiavi KMS di crittografia simmetriche e non chiavi KMS asimmetriche. Per ulteriori informazioni, consulta [Identificazione delle chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni sulla creazione di una AWS KMS key, consulta [Creating keys nella Developer Guide](#). AWS Key Management Service Per ulteriori informazioni sull'utilizzo AWS KMS con Amazon S3, consulta [Utilizzo della crittografia lato server con AWS KMS chiavi \(\) SSE-KMS](#).

12. In Classe di storage di destinazione, per replicare i dati in una classe di archiviazione specifica nel bucket di destinazione, seleziona Modifica classe di archiviazione per gli oggetti replicati.

Scegli quindi la classe di storage che desideri utilizzare per gli oggetti replicati nel bucket di destinazione. Se non selezioni questa opzione, la classe di storage per gli oggetti replicati sarà la stessa degli oggetti originali.

13. Durante l'impostazione dei valori in Opzioni di replica aggiuntive, sono disponibili le seguenti opzioni aggiuntive:

- Se desideri abilitare la funzionalità di controllo del tempo di replica di S3 (S3 RTC) nella configurazione della replica, seleziona Controllo del tempo di replica (RTC). Per ulteriori informazioni su questa opzione, consulta [Soddisfazione dei requisiti di conformità con il controllo del tempo di replica di Amazon S3](#).
- Se desideri abilitare i parametri di replica S3 nella configurazione di replica, seleziona Replication metrics and events (Parametri ed eventi di replica). Per ulteriori informazioni, consulta [Monitoraggio della replica con parametri, notifiche di eventi e stati](#).
- Se desideri abilitare la replica del contrassegno di eliminazione nella configurazione di replica, seleziona Replica del contrassegno di eliminazione. Per ulteriori informazioni, consulta [Replica dei contrassegni di eliminazione tra i bucket](#).
- Se desideri abilitare la sincronizzazione delle modifiche alla replica di Amazon S3 nella configurazione di replica, seleziona Sincronizzazione delle modifiche alla replica. Per ulteriori informazioni, consulta [Replica delle modifiche ai metadati con la sincronizzazione delle modifiche alla replica](#).

Note

Quando si utilizzano i parametri di replica S3 RTC o S3, si applicano costi aggiuntivi.

14. Per terminare, seleziona Salva.

15. Dopo aver salvato la regola, potrai modificare, abilitare, disabilitare o eliminare la regola selezionando la regola e scegliendo Modifica regola.

Utilizzo di AWS CLI

AWS CLI Per configurare la replica quando i bucket di origine e destinazione sono di proprietà dello stesso Account AWS, procedi come segue:

- Creare bucket di origine e di destinazione.
- Abilitare il controllo delle versioni sui bucket.

- Crea un ruolo AWS Identity and Access Management (IAM) che conceda ad Amazon S3 il permesso di replicare oggetti.
- Aggiungere la configurazione della replica al bucket di origine.

Per verificare l'impostazione, testarla.

Per configurare la replica quando i bucket di origine e destinazione sono di proprietà della stessa Account AWS

1. Impostare un profilo di credenziali per la AWS CLI. In questo esempio si utilizza il nome del profilo `acctA`. Per informazioni sull'impostazione di profili con credenziali e sull'uso di profili denominati, consulta [Impostazioni del file di configurazione e delle credenziali](#) nella Guida per l'utente di AWS Command Line Interface .

 Important

Il profilo utilizzato per questo esempio deve disporre delle autorizzazioni necessarie. Ad esempio, nella configurazione di replica dovrai specificare il ruolo IAM che Amazon S3 può assumere. È possibile effettuare questa operazione solo se il profilo utilizzato dispone dell'autorizzazione `iam:PassRole`. Per ulteriori informazioni, consulta [Concedere le autorizzazioni utente per il passaggio di un ruolo a un Servizio AWS](#) nella Guida per l'utente IAM. Se utilizzi le credenziali di amministratore per creare un profilo con nome, puoi eseguire tutte le attività.

2. Creare un bucket di origine e abilitare su di esso il controllo delle versioni utilizzando i seguenti comandi di AWS CLI . Per utilizzare questi comandi, sostituire *user input placeholders* con le proprie informazioni.

Il seguente comando `create-bucket` crea un bucket di origine denominato *amzn-s3-demo-source-bucket* nella Regione Stati Uniti orientali (Virginia settentrionale) (`us-east-1`).

```
aws s3api create-bucket \  
--bucket amzn-s3-demo-source-bucket \  
--region us-east-1 \  
--profile acctA
```

Il seguente comando `put-bucket-versioning` abilita il controllo delle versioni S3 sul bucket *amzn-s3-demo-source-bucket*:

```
aws s3api put-bucket-versioning \  
--bucket amzn-s3-demo-source-bucket \  
--versioning-configuration Status=Enabled \  
--profile acctA
```

3. Crea un bucket di destinazione e abilita il controllo delle versioni su di esso utilizzando i seguenti comandi. AWS CLI Per utilizzare questi comandi, sostituire *user input placeholders* con le proprie informazioni.

Note

Per impostare una configurazione di replica quando i bucket di origine e di destinazione sono nello stesso Account AWS, si utilizza lo stesso profilo per i bucket di origine e di destinazione. Questo esempio usa *acctA*.

Per testare una configurazione di replica quando i bucket sono di proprietà di diversi Account AWS, specifica profili diversi per ogni account. Ad esempio, è possibile utilizzare un profilo *acctB* per il bucket di destinazione.

Il seguente comando `create-bucket` crea un bucket di destinazione denominato *amzn-s3-demo-destination-bucket* nella Regione Stati Uniti occidentali (Oregon) (*us-west-2*):

```
aws s3api create-bucket \  
--bucket amzn-s3-demo-destination-bucket \  
--region us-west-2 \  
--create-bucket-configuration LocationConstraint=us-west-2 \  
--profile acctA
```

Il seguente comando `put-bucket-versioning` abilita il controllo delle versioni S3 sul bucket *amzn-s3-demo-destination-bucket*:

```
aws s3api put-bucket-versioning \  
--bucket amzn-s3-demo-destination-bucket \  
--versioning-configuration Status=Enabled \  

```



```
--profile acctA
```

4. Creare un ruolo IAM. Specifica questo ruolo nella configurazione di replica che aggiungi al bucket *source* in un secondo momento. Amazon S3 assume questo ruolo per replicare gli oggetti per tuo conto. Il ruolo IAM si crea in due fasi:

- Creare un ruolo.
- Collegare una policy di autorizzazione al ruolo.

- a. Crea il ruolo IAM.

- i. Copiare la seguente policy di attendibilità e salvarla in un file denominato `s3-role-trust-policy.json` nella directory corrente sul computer locale. Questa policy concede al principale del servizio Amazon S3 le autorizzazioni per assumere il ruolo.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- ii. Per creare un ruolo, eseguire il comando seguente.

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json \
--profile acctA
```

- b. Collegare una policy di autorizzazione al ruolo.

- i. Copiare la seguente policy di autorizzazioni e salvarla in un file denominato `s3-role-permissions-policy.json` nella directory corrente sul computer locale. Questa policy di accesso concede le autorizzazioni per varie operazioni su oggetti e bucket Amazon S3.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetReplicationConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

}

 Note

- Se si desidera replicare oggetti crittografati, è opportuno anche concedere le autorizzazioni chiave AWS Key Management Service (AWS KMS) necessarie. Per ulteriori informazioni, consulta [the section called “Replica di oggetti crittografati”](#).
- Per utilizzare Object Lock con la replica, devi concedere due autorizzazioni aggiuntive sul bucket S3 di origine nel ruolo AWS Identity and Access Management (IAM) utilizzato per configurare la replica. Le due nuove autorizzazioni aggiuntive sono `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se il ruolo dispone di un'istruzione di autorizzazione `s3:Get*`, tale istruzione soddisfa il requisito. Per ulteriori informazioni, consulta [the section called “Utilizzo di Object Lock con la replica S3”](#).
- Per replicare le annotazioni degli oggetti, devi anche concedere le autorizzazioni al bucket S3 di origine nella `s3:GetObjectVersionAnnotationForReplication` policy delle autorizzazioni del ruolo IAM. Per ulteriori informazioni, consulta [the section called “Replica delle modifiche ai metadati”](#).

- ii. Eseguire il comando seguente per creare una policy e collegarla al ruolo. Sostituisci *user input placeholders* con le informazioni appropriate.

```
$ aws iam put-role-policy \  
--role-name replicationRole \  
--policy-document file://s3-role-permissions-policy.json \  
--policy-name replicationRolePolicy \  
--profile acctA
```

5. Aggiungi una configurazione di replica al bucket di origine.
 - a. Sebbene l'API Amazon S3 richieda di specificare la configurazione di replica come XML, AWS CLI richiede di specificare la configurazione di replica come JSON. Salvare il seguente JSON in un file denominato `replication.json` nella directory locale sul computer in uso.

```
{
  "Role": "IAM-role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": { "Status": "Disabled" },
      "Filter" : { "Prefix": "Tax"},
      "Destination": {
        "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      }
    }
  ]
}
```

- b. Aggiornare il JSON sostituendo i valori di *amzn-s3-demo-destination-bucket* e *IAM-role-ARN* con le proprie informazioni. Salvare le modifiche.
- c. Eseguire il seguente comando `put-bucket-replication` per aggiungere la configurazione della replica al bucket di origine. Assicurarsi di fornire il nome del bucket di origine:

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

Per recuperare la configurazione della replica, utilizzare il comando `get-bucket-replication`:

```
$ aws s3api get-bucket-replication \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. Verificare la configurazione nella console Amazon S3 eseguendo i seguenti passaggi:
 - a. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
 - b. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket). Scegli il bucket di origine nell'elenco Bucket per uso generico.

- c. Nel bucket di origine creare una cartella denominata *Tax*.
- d. Aggiungere oggetti di esempio alla cartella *Tax* nel bucket di origine.

 Note

Il tempo richiesto da Amazon S3 per la replica di un oggetto dipende dalle dimensioni dell'oggetto. Per informazioni su come visualizzare lo stato della replica, consulta la sezione [Ottenimento delle informazioni sullo stato della replica](#).

Nel bucket di *destinazione*, verificare quanto segue:

- Amazon S3 ha replicato gli oggetti.
- Gli oggetti sono repliche. Nella scheda Proprietà degli oggetti, scorrere verso il basso fino alla sezione Panoramica della gestione degli oggetti. In Configurazioni di gestione, controllare il valore in Stato della replica. Assicurarsi che questo valore sia impostato su REPLICA.
- Le repliche sono di proprietà dell'account del bucket di origine. È possibile verificare la proprietà dell'oggetto nella scheda Autorizzazioni degli oggetti.

Se i bucket di origine e di destinazione sono di proprietà di account diversi, è possibile aggiungere una configurazione ottimale per indicare ad Amazon S3 di modificare la proprietà di una replica nell'account di destinazione. Per un esempio, consulta [Come modificare il proprietario della replica](#).

Utilizzo di AWS SDK

Usa i seguenti esempi di codice per aggiungere una configurazione di replica a un bucket con AWS SDK per Java e AWS SDK per .NET, rispettivamente.

 Note

- Se si desidera replicare oggetti crittografati, è opportuno anche concedere le autorizzazioni chiave AWS Key Management Service (AWS KMS) necessarie. Per ulteriori informazioni, consulta [the section called “Replica di oggetti crittografati”](#).
- Per utilizzare Object Lock con la replica, devi concedere due autorizzazioni aggiuntive sul bucket S3 di origine nel ruolo AWS Identity and Access Management (IAM)

utilizzato per configurare la replica. Le due nuove autorizzazioni aggiuntive sono `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se il ruolo dispone di un'istruzione di autorizzazione `s3:Get*`, tale istruzione soddisfa il requisito. Per ulteriori informazioni, consulta [the section called "Utilizzo di Object Lock con la replica S3"](#).

Java

Per aggiungere una configurazione di replica a un bucket e quindi recuperare e verificare la configurazione utilizzando l' AWS SDK per Java, è possibile utilizzare `S3Client` per gestire le impostazioni di replica a livello di codice.

Per esempi di come configurare la replica con l' AWS SDK per Java, consulta [Impostare la configurazione della replica su un bucket nell'API Reference di Amazon S3](#).

C#

Il seguente esempio di AWS SDK per .NET codice aggiunge una configurazione di replica a un bucket e quindi la recupera. Per utilizzare questo codice, fornisci i nomi dei bucket e l'Amazon Resource Name (ARN) per il ruolo IAM. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Nozioni di base su AWS SDK per .NET](#) nella Guida per gli sviluppatori di AWS SDK per .NET .

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CrossRegionReplicationTest
    {
        private const string sourceBucket = "**** source bucket ****";
        // Bucket ARN example - arn:aws:s3:::destinationbucket
        private const string destinationBucketArn = "**** destination bucket ARN
****";
        private const string roleArn = "**** IAM Role ARN ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint sourceBucketRegion =
            RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
```

```
public static void Main()
{
    s3Client = new AmazonS3Client(sourceBucketRegion);
    EnableReplicationAsync().Wait();
}
static async Task EnableReplicationAsync()
{
    try
    {
        ReplicationConfiguration replConfig = new ReplicationConfiguration
        {
            Role = roleArn,
            Rules =
            {
                new ReplicationRule
                {
                    Prefix = "Tax",
                    Status = ReplicationRuleStatus.Enabled,
                    Destination = new ReplicationDestination
                    {
                        BucketArn = destinationBucketArn
                    }
                }
            }
        };

        PutBucketReplicationRequest putRequest = new
PutBucketReplicationRequest
        {
            BucketName = sourceBucket,
            Configuration = replConfig
        };

        PutBucketReplicationResponse putResponse = await
s3Client.PutBucketReplicationAsync(putRequest);

        // Verify configuration by retrieving it.
        await RetrieveReplicationConfigurationAsync(s3Client);
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
}
```

```

        catch (Exception e)
        {
            Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
        }
    }
    private static async Task RetrieveReplicationConfigurationAsync(IAmazonS3
client)
    {
        // Retrieve the configuration.
        GetBucketReplicationRequest getRequest = new GetBucketReplicationRequest
        {
            BucketName = sourceBucket
        };
        GetBucketReplicationResponse getResponse = await
client.GetBucketReplicationAsync(getRequest);
        // Print.
        Console.WriteLine("Printing replication configuration information...");
        Console.WriteLine("Role ARN: {0}", getResponse.Configuration.Role);
        foreach (var rule in getResponse.Configuration.Rules)
        {
            Console.WriteLine("ID: {0}", rule.Id);
            Console.WriteLine("Prefix: {0}", rule.Prefix);
            Console.WriteLine("Status: {0}", rule.Status);
        }
    }
}
}

```

Configurazione della replica per i bucket in account diversi

La replica in tempo reale è la copia automatica e asincrona di oggetti tra bucket uguali o diversi. Regioni AWS La replica in tempo reale copia gli oggetti appena creati e gli aggiornamenti degli oggetti da un bucket di origine in uno o più bucket di destinazione. Per ulteriori informazioni, consulta [Replica di oggetti all'interno e tra le Regioni](#).

Quando si configura la replica, vengono aggiunte le regole di replica al bucket di origine. Le regole di replica definiscono gli oggetti del bucket di origine da replicare e i bucket di destinazione in cui vengono archiviati gli oggetti replicati. È possibile creare una regola per replicare tutti gli oggetti in un bucket o un sottoinsieme di oggetti con un prefisso di nome di chiave specifico, uno o più tag di

oggetto o entrambi gli elementi. Un bucket di destinazione può trovarsi nello stesso bucket Account AWS di origine oppure in un account diverso.

Se specifichi l'ID della versione dell'oggetto da eliminare, Amazon S3 elimina la versione dell'oggetto nel bucket di origine. Ma non replica l'eliminazione nel bucket di destinazione. In altre parole, non elimina la stessa versione dell'oggetto dal bucket di destinazione. Ciò permette di proteggere i dati da eliminazioni da parte di utenti malintenzionati.

Quando si aggiunge una regola di replica a un bucket, la regola viene abilitata per impostazione predefinita e pertanto inizia a funzionare non appena viene salvata.

La configurazione della replica in tempo reale quando i bucket di origine e di destinazione sono di proprietà di Account AWS diversi prevede una procedura simile a quella della configurazione della replica quando entrambi i bucket sono di proprietà dello stesso account. Tuttavia, esistono varie differenze quando si configura la replica in uno scenario comprendente più account:

- Il proprietario del bucket di destinazione deve concedere al proprietario del bucket di origine l'autorizzazione necessaria per replicare gli oggetti nella policy del bucket di destinazione.
- Se stai replicando oggetti crittografati con crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS) in uno scenario con più account, il proprietario della chiave KMS deve concedere al proprietario del bucket di origine l'autorizzazione a utilizzare la chiave KMS. Per ulteriori informazioni, consulta [Concessione di autorizzazioni aggiuntive per scenari multi-account](#).
- Per impostazione predefinita, gli oggetti replicati appartengono al proprietario del bucket di origine. In uno scenario multi-account, è possibile configurare la replica per trasferire la proprietà degli oggetti replicati al proprietario del bucket di destinazione. Per ulteriori informazioni, consulta [Modifica del proprietario della replica](#).

Per configurare la replica quando i bucket di origine e di destinazione sono di proprietà diversa Account AWS

1. In questo esempio i bucket di origine e di destinazione vengono creati in due Account AWS diversi. È necessario disporre di due profili di credenziali impostati per AWS CLI. Questo esempio utilizza `acctA` e `acctB` per i nomi di tali profili. Per informazioni sull'impostazione di profili con credenziali e sull'uso di profili denominati, consulta [Impostazioni del file di configurazione e delle credenziali](#) nella Guida per l'utente di AWS Command Line Interface .
2. Segui le istruzioni dettagliate in [Configurazione della replica per i bucket nello stesso account](#) apportando le seguenti modifiche:

- Per tutti AWS CLI i comandi relativi alle attività del bucket di origine (come la creazione del bucket di origine, l'abilitazione del controllo delle versioni e la creazione del ruolo IAM), usa il profilo. `acctA` Utilizzare il profilo `acctB` per creare il bucket di destinazione.
 - Assicurarsi che la policy di autorizzazione per il ruolo IAM specifichi i bucket di origine e di destinazione creati per questo esempio.
3. Nella console, aggiungere la seguente policy di bucket al bucket *di destinazione* per consentire al proprietario del bucket *di origine* di replicare gli oggetti. Per istruzioni, consulta l'argomento [Aggiunta di una policy di bucket utilizzando la console di Amazon S3](#). Assicurati di modificare la policy fornendo l' Account AWS ID del proprietario del bucket di origine, il nome del ruolo IAM e il nome del bucket di destinazione.

Note

Per utilizzare l'esempio seguente, sostituisci *user input placeholders* con le informazioni appropriate. Sostituire `amzn-s3-demo-destination-bucket` con il nome del bucket di destinazione. Sostituire `source-bucket-account-ID:role/source-account-IAM-role` nel nome della risorsa Amazon (ARN) IAM con il ruolo IAM utilizzato per questa configurazione della replica.

Il percorso del ruolo nell'ARN IAM dipende da come hai creato il ruolo. Se hai creato il ruolo con AWS CLI (come mostrato in [Configurazione della replica per i bucket nello stesso account](#)), il percorso è `role/role-name`. Se hai creato il ruolo con la console IAM come ruolo di servizio, il percorso include `service-role/` (ovvero, `role/service-role/role-name`). Per ulteriori informazioni, consulta [ARN IAM](#) nella Guida per l'utente di IAM.

```
{
  "Version": "2012-10-17",
  "Id": "",
  "Statement": [
    {
      "Sid": "Set-permissions-for-objects",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source-bucket-account-ID:role/source-account-IAM-role"
      },
    },
  ],
}
```

```

        "Action": [
            "s3:ReplicateObject",
            "s3:ReplicateDelete"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
        "Sid": "Set-permissions-on-bucket",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::source-bucket-account-ID:role/source-account-  
IAM-role"
        },
        "Action": [
            "s3:GetBucketVersioning",
            "s3:PutBucketVersioning"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    }
]
}

```

4. (Facoltativo) Se stai replicando oggetti crittografati con SSE-KMS, il proprietario della chiave KMS deve concedere al proprietario del bucket di origine l'autorizzazione a utilizzare la chiave KMS. Per ulteriori informazioni, consulta [Concessione di autorizzazioni aggiuntive per scenari multi-account](#).
5. (Facoltativo) Nella replica il proprietario dell'oggetto di origine possiede la replica stessa per impostazione predefinita. Quando i bucket di origine e di destinazione sono di proprietà diversa Account AWS, puoi aggiungere impostazioni di configurazione opzionali per passare la proprietà della replica a Account AWS quella proprietaria dei bucket di destinazione. Ciò include la concessione dell'autorizzazione `ObjectOwnerOverrideToBucketOwner`. Per ulteriori informazioni, consulta [Modifica del proprietario della replica](#).

Modifica del proprietario della replica

Nella replica, il proprietario dell'oggetto di origine possiede anche la replica per impostazione predefinita. Tuttavia, quando i bucket di origine e di destinazione sono di proprietà diversa Account AWS, è possibile modificare la proprietà della replica. Ad esempio, è preferibile modificare la proprietà per limitare l'accesso alle repliche degli oggetti. Nella configurazione di replica, è possibile

aggiungere impostazioni di configurazione opzionali per modificare la proprietà della replica a Account AWS quella proprietaria dei bucket di destinazione.

Per modificare il proprietario della replica, procedere come segue:

- Aggiungere l'opzione di sostituzione del proprietario alla configurazione della replica per indicare ad Amazon S3 di modificare la proprietà della replica.
- Concedere ad Amazon S3 l'autorizzazione `s3:ObjectOwnerOverrideToBucketOwner` per modificare la proprietà della replica.
- Aggiungere l'autorizzazione `s3:ObjectOwnerOverrideToBucketOwner` alla policy del bucket di destinazione per consentire la modifica della proprietà della replica. L'autorizzazione `s3:ObjectOwnerOverrideToBucketOwner` consente al proprietario dei bucket di destinazione di accettare la proprietà delle repliche degli oggetti.

Per ulteriori informazioni, consulta [the section called “Considerazioni sull'opzione di sostituzione della proprietà”](#) e [Aggiunta dell'opzione di sostituzione del proprietario alla configurazione della replica](#). Per un esempio di utilizzo con istruzioni dettagliate, consulta la sezione [Come modificare il proprietario della replica](#).

Important

Anziché utilizzare l'opzione di sostituzione del proprietario, è possibile utilizzare l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto. Quando si utilizza la replica e i bucket di origine e di destinazione sono di proprietà diversa Account AWS, il proprietario del bucket di destinazione può utilizzare l'impostazione applicata dal proprietario del bucket per Object Ownership per modificare la proprietà della replica con quella proprietaria del bucket di destinazione. Account AWS Questa impostazione disabilita le liste di controllo degli accessi (ACL) degli oggetti.

L'impostazione Proprietario del bucket applicato imita il comportamento di sovrascrittura del proprietario esistente senza la necessità dell'autorizzazione `s3:ObjectOwnerOverrideToBucketOwner`. Tutti gli oggetti replicati nel bucket di destinazione con l'impostazione proprietario del bucket applicato sono di proprietà del proprietario del bucket di destinazione. Per ulteriori informazioni su Object Ownership, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Considerazioni sull'opzione di sostituzione della proprietà

Quando configuri l'opzione di sostituzione del proprietario, si applicano le seguenti considerazioni:

- Per impostazione predefinita, il proprietario dell'oggetto di origine possiede anche la replica. Amazon S3 replica la versione dell'oggetto e l'ACL associata.

Se si aggiunge l'opzione di sostituzione del proprietario alla configurazione della replica, Amazon S3 replica solo la versione dell'oggetto, non l'ACL. Inoltre, Amazon S3 non replica le modifiche successive all'ACL dell'oggetto di origine. Amazon S3 imposta l'ACL sulla replica che concede il controllo completo al proprietario del bucket di destinazione.

- Quando si aggiorna una configurazione della replica per abilitare o disabilitare la sostituzione del proprietario, si verifica quanto segue:
 - Se aggiungi l'opzione di sostituzione del proprietario alla configurazione della replica:

Quando replica una versione dell'oggetto, Amazon S3 elimina l'ACL associata all'oggetto di origine e imposta l'ACL sulla replica concedendo il controllo completo al proprietario del bucket di destinazione. Amazon S3 non replica le modifiche successive all'ACL dell'oggetto di origine. Tuttavia, questa modifica dell'ACL non si applica alle versioni dell'oggetto che sono state replicate prima di impostare l'opzione di sostituzione proprietario. Gli aggiornamenti all'ACL negli oggetti di origine che sono stati replicati prima che fosse impostata la sostituzione del proprietario continuano a essere replicati in quanto l'oggetto e le relative repliche continuano ad avere lo stesso proprietario.

- Se rimuovi l'opzione di sostituzione del proprietario dalla configurazione della replica:

Amazon S3 replica i nuovi oggetti presenti nel bucket di origine e le ACL associate ai bucket di destinazione. Per gli oggetti che sono stati replicati prima della rimozione della sostituzione del proprietario, Amazon S3 non replica le ACL perché rimane valida la modifica della proprietà dell'oggetto apportata da Amazon S3. In altre parole, le ACL associate alla versione dell'oggetto replicata quando la sostituzione del proprietario era impostata continuano a non essere replicate.

Aggiunta dell'opzione di sostituzione del proprietario alla configurazione della replica

Warning

Aggiungi l'opzione di override del proprietario solo quando i bucket di origine e di destinazione sono di proprietà diversa. Account AWS Amazon S3 non controlla se i bucket sono di proprietà dello stesso account o di account diversi. Se aggiungi l'override del

proprietario quando entrambi i bucket sono di proprietà dello stesso Account AWS, Amazon S3 applica l'override del proprietario. Questa opzione concede le autorizzazioni complete al proprietario del bucket di destinazione e non replica gli aggiornamenti successivi delle liste di controllo degli accessi (ACL) degli oggetti di origine. Il proprietario della replica può modificare direttamente l'ACL associata a una replica con una richiesta `PutObjectAcl`, ma non tramite replica.

Per specificare l'opzione di sostituzione del proprietario, aggiungi quanto segue all'elemento `Destination`:

- L'elemento `AccessControlTranslation`, che indica ad Amazon S3 di modificare la proprietà della replica
- L'Accountelemento, che specifica il proprietario del bucket di destinazione Account AWS

```
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  ...
  <Destination>
    ...
    <AccessControlTranslation>
      <Owner>Destination</Owner>
    </AccessControlTranslation>
    <Account>destination-bucket-owner-account-id</Account>
  </Destination>
</Rule>
</ReplicationConfiguration>
```

La seguente configurazione della replica di esempio indica ad Amazon S3 di replicare gli oggetti con il prefisso della chiave *Tax* nel bucket di destinazione *amzn-s3-demo-destination-bucket* e di modificare la proprietà delle repliche. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <ID>Rule-1</ID>
    <Priority>1</Priority>
    <Status>Enabled</Status>
```

```

    <DeleteMarkerReplication>
      <Status>Disabled</Status>
    </DeleteMarkerReplication>
    <Filter>
      <Prefix>Tax</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
      <Account>destination-bucket-owner-account-id</Account>
      <AccessControlTranslation>
        <Owner>Destination</Owner>
      </AccessControlTranslation>
    </Destination>
  </Rule>
</ReplicationConfiguration>

```

Concessione ad Amazon S3 dell'autorizzazione per modificare la proprietà della replica

Concedi ad Amazon S3 le autorizzazioni per modificare la proprietà della replica aggiungendo l'autorizzazione per `s3:ObjectOwnerOverrideToBucketOwner` nella politica delle autorizzazioni associata al ruolo (IAM). AWS Identity and Access Management Questo è il ruolo IAM specificato nella configurazione della replica che consente ad Amazon S3 di acquisire e replicare gli oggetti per conto dell'utente. Per utilizzare il seguente esempio, sostituire *amzn-s3-demo-destination-bucket* con il nome del bucket di destinazione.

```

...
{
  "Effect": "Allow",
  "Action": [
    "s3:ObjectOwnerOverrideToBucketOwner"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
...

```

Aggiunta dell'autorizzazione alla policy del bucket di destinazione per consentire la modifica della proprietà della replica

Il proprietario del bucket di destinazione deve concedere al proprietario del bucket di origine l'autorizzazione necessaria per modificare la proprietà della replica. Il proprietario del bucket di destinazione concede al proprietario del bucket di origine l'autorizzazione per l'operazione

s3:ObjectOwnerOverrideToBucketOwner. Questa autorizzazione consente al proprietario del bucket di destinazione di accettare la proprietà delle repliche degli oggetti. La seguente istruzione della policy del bucket di esempio mostra come fare: Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
...
{
  "Sid": "1",
  "Effect": "Allow",
  "Principal": { "AWS": "source-bucket-account-id" },
  "Action": [ "s3:ObjectOwnerOverrideToBucketOwner" ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
...
```

Come modificare il proprietario della replica

Quando i bucket di origine e di destinazione in una configurazione di replica sono di proprietà diversa Account AWS, puoi dire ad Amazon S3 di cambiare la proprietà della replica con quella proprietaria del Account AWS bucket di destinazione. Gli esempi seguenti mostrano come utilizzare la console Amazon S3, AWS Command Line Interface (AWS CLI) e gli AWS SDK per modificare la proprietà della replica.

Utilizzo della console S3

Per istruzioni dettagliate, consulta [Configurazione della replica per i bucket nello stesso account](#).

Questo argomento fornisce istruzioni per impostare una configurazione di replica quando i bucket di origine e di destinazione sono di proprietà identica e diversa. Account AWS

Utilizzo di AWS CLI

Nella seguente procedura viene mostrato come modificare la proprietà della replica utilizzando AWS CLI. In questa procedura, esegui le seguenti operazioni:

- Creazione dei bucket di origine e di destinazione.
- Abilitare il controllo delle versioni sui bucket.
- Crea un ruolo AWS Identity and Access Management (IAM) che conceda ad Amazon S3 il permesso di replicare oggetti.
- Aggiungere la configurazione della replica al bucket di origine.
- Nella configurazione della replica si indica ad Amazon S3 di modificare la proprietà della replica.

- Verificare la configurazione della replica.

Per modificare la proprietà della replica quando i bucket di origine e di destinazione sono di proprietà diversa Account AWS (AWS CLI)

Per utilizzare i AWS CLI comandi di esempio in questa procedura, sostituiscili *user input placeholders* con le tue informazioni.

1. In questo esempio, crei i bucket di origine e di destinazione in due diversi Account AWS. Per utilizzare questi due account, occorre configurare AWS CLI con due profili denominati. Questo esempio utilizza i profili denominati rispettivamente *acctA* e *acctB*. Per informazioni sull'impostazione di profili con credenziali e sull'uso di profili denominati, consulta [Impostazioni del file di configurazione e delle credenziali](#) nella Guida per l'utente di AWS Command Line Interface .

⚠ Important

I profili utilizzati per questa procedura devono disporre delle autorizzazioni necessarie. Ad esempio, nella configurazione di replica dovrai specificare il ruolo IAM che Amazon S3 può assumere. È possibile effettuare questa operazione solo se il profilo utilizzato dispone dell'autorizzazione `iam:PassRole`. Se si utilizzano le credenziali dell'utente amministratore per creare un profilo denominato, è possibile eseguire tutte le attività in questa procedura. Per ulteriori informazioni, consulta [Concessione di autorizzazioni utente per il passaggio di un ruolo a un Servizio AWS](#) nella Guida per l'utente di IAM.

2. Creare il bucket di origine e abilitare la funzione Controllo delle versioni. Questo esempio crea un bucket denominato *amzn-s3-demo-source-bucket* nella Regione Stati Uniti orientali (Virginia settentrionale) (*us-east-1*).

```
aws s3api create-bucket \  
--bucket amzn-s3-demo-source-bucket \  
--region us-east-1 \  
--profile acctA
```

```
aws s3api put-bucket-versioning \  
--bucket amzn-s3-demo-source-bucket \  
--versioning-configuration Status=Enabled \  
--profile acctA
```

3. Creare un bucket di destinazione e abilitare la funzione Controllo delle versioni. Questo esempio crea un bucket di destinazione denominato *amzn-s3-demo-destination-bucket* nella Regione Stati Uniti occidentali (Oregon) (us-west-2). Utilizzare un profilo Account AWS diverso da quello utilizzato per il bucket di origine.

```
aws s3api create-bucket \  
--bucket amzn-s3-demo-destination-bucket \  
--region us-west-2 \  
--create-bucket-configuration LocationConstraint=us-west-2 \  
--profile acctB
```

```
aws s3api put-bucket-versioning \  
--bucket amzn-s3-demo-destination-bucket \  
--versioning-configuration Status=Enabled \  
--profile acctB
```

4. Devi aggiungere l'autorizzazione alla policy del bucket di *destinazione* per consentire la modifica della proprietà della replica.
 - a. Salvare la seguente policy in un file denominato *destination-bucket-policy.json*. Assicurarsi di sostituire *user input placeholders* con le proprie informazioni.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "destination_bucket_policy_sid",  
      "Principal": {  
        "AWS": "source-bucket-owner-123456789012"  
      },  
      "Action": [  
        "s3:ReplicateObject",  
        "s3:ReplicateDelete",  
        "s3:ObjectOwnerOverrideToBucketOwner",  
        "s3:ReplicateTags",  
        "s3:GetObjectVersionTagging"  
      ],  
      "Effect": "Allow",  
      "Resource": [  

```

```

    "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
  ]
}
}

```

- b. Aggiungere la policy precedente al bucket di destinazione utilizzando il seguente comando `put-bucket-policy`:

```
aws s3api put-bucket-policy --region $ {destination-region} --bucket $ {amzn-s3-demo-destination-bucket} --policy file://destination_bucket_policy.json
```

5. Creare un ruolo IAM. Specifica questo ruolo nella configurazione di replica che aggiungi al bucket *source* in un secondo momento. Amazon S3 assume questo ruolo per replicare gli oggetti per tuo conto. Il ruolo IAM si crea in due fasi:

- Crea il ruolo.
- Collegare una policy di autorizzazione al ruolo.

- a. Crea il ruolo IAM.

- i. Copiare la seguente policy di attendibilità e salvarla in un file denominato *s3-role-trust-policy.json* nella directory corrente sul computer locale. Questa policy concede ad Amazon S3 le autorizzazioni per assumere il ruolo.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

- ii. Esegui il AWS CLI `create-role` comando seguente per creare il ruolo IAM:

```
$ aws iam create-role \  
--role-name replicationRole \  
--assume-role-policy-document file://s3-role-trust-policy.json \  
--profile acctA
```

Prendere nota del nome della risorsa Amazon (ARN) del ruolo IAM creato. Tale nome sarà necessario in un passaggio successivo.

- b. Collegare una policy di autorizzazione al ruolo.
 - i. Copiare la seguente policy di autorizzazioni e salvarla in un file denominato *s3-role-perm-pol-changeowner.json* nella directory corrente sul computer locale. Questa policy di accesso concede le autorizzazioni per varie operazioni su oggetti e bucket Amazon S3. Nelle fasi che seguono si associa questa policy al ruolo IAM creato in precedenza.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:GetObjectVersionForReplication",  
        "s3:GetObjectVersionAcl"  
      ],  
      "Resource": [  
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*"  
      ]  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:ListBucket",  
        "s3:GetReplicationConfiguration"  
      ],  
      "Resource": [  
        "arn:aws:s3:::amzn-s3-demo-source-bucket"  
      ]  
    }  
  ]  
}
```

```

    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:ReplicateObject",
      "s3:ReplicateDelete",
      "s3:ObjectOwnerOverrideToBucketOwner",
      "s3:ReplicateTags",
      "s3:GetObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
  }
]
}

```

- ii. Per associare la policy delle autorizzazioni precedente al ruolo, eseguire il seguente comando `put-role-policy`:

```

$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-perm-pol-changeowner.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA

```

6. Aggiungere una configurazione di replica al bucket di origine.

- a. AWS CLI Richiede di specificare la configurazione di replica come JSON. Salvare il seguente JSON in un file denominato *replication.json* nella directory corrente sul computer locale. Nella configurazione, `AccessControlTranslation` specifica la modifica della proprietà della replica dal proprietario del bucket di origine al proprietario del bucket di destinazione.

```

{
  "Role": "IAM-role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": {
        "Status": "Disabled"
      }
    },

```

```

    "Filter":{
    },
    "Status":"Enabled",
    "Destination":{
      "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
      "Account":"destination-bucket-owner-account-id",
      "AccessControlTranslation":{
        "Owner":"Destination"
      }
    }
  }
]
}

```

- b. Modificare il JSON fornendo i valori per il nome del bucket di destinazione, l'ID account del proprietario del bucket di destinazione e *IAM-role-ARN*. Sostituisci *IAM-role-ARN* con l'ARN del ruolo IAM creato in precedenza. Salvare le modifiche.
- c. Per aggiungere la configurazione della replica al bucket di origine, eseguire il seguente comando:

```

$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA

```

7. Verificare la configurazione della replica controllando la proprietà della replica nella console Amazon S3.
 - a. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
 - b. Aggiungere oggetti al bucket *di origine*. Verifica che il bucket di destinazione contenga le repliche degli oggetti e che la proprietà delle repliche sia passata a Account AWS quella proprietaria del bucket di destinazione.

Utilizzo di AWS SDK

Per un esempio di codice per l'aggiunta di una configurazione della replica, consulta [Utilizzo di AWS SDK](#). La configurazione della replica deve essere modificata di conseguenza. Per informazioni concettuali, consulta [Modifica del proprietario della replica](#).

Soddisfazione dei requisiti di conformità con il controllo del tempo di replica di Amazon S3

Amazon S3 Replication Time Control (S3 RTC) permette di soddisfare i requisiti aziendali o di conformità per la replica dei dati fornendo visibilità sui tempi di replica di Amazon S3. S3 RTC replica la maggior parte degli oggetti caricati in Amazon S3 in pochi secondi e il 99,9% di tali oggetti entro 15 minuti.

Per impostazione predefinita, S3 RTC include due modi per monitorare l'avanzamento della replica:

- **Parametri di Replica Amazon S3:** con i parametri di replica S3, è possibile monitorare il numero totale di operazioni API S3 in attesa di replica, la dimensione totale degli oggetti in attesa di replica, il tempo massimo di replica nella Regione di destinazione e il numero totale delle operazioni che non sono state replicate. Quindi puoi monitorare separatamente ogni set di dati replicato. È inoltre possibile abilitare i parametri di Replica Amazon S3 indipendentemente da S3 RTC. Per ulteriori informazioni, consulta [the section called “Utilizzo dei parametri di Replica S3”](#).

Le regole di replica per le quali è abilitato il controllo del tempo di replica di S3 (S3 RTC) pubblicano i parametri di Replica Amazon S3. I parametri di replica sono disponibili entro 15 minuti dall'attivazione di S3 RTC. Le metriche di replica sono disponibili tramite la console Amazon S3, l'API Amazon S3, gli AWS SDK, () e Amazon. AWS Command Line Interface AWS CLI CloudWatch Per ulteriori informazioni sulle metriche, consulta [CloudWatch Metriche di monitoraggio con Amazon CloudWatch](#) Per ulteriori informazioni sulla visualizzazione dei parametri di replica tramite la console Amazon S3, consulta [Visualizzazione dei parametri di replica](#).

Le metriche di replica S3 vengono fatturate alla stessa tariffa delle metriche personalizzate di Amazon. CloudWatch Per informazioni, consulta i prezzi di Amazon. [CloudWatch](#)

- **Notifiche di eventi Amazon S3:** S3 RTC fornisce gli eventi `OperationMissedThreshold` e `OperationReplicatedAfterThreshold` che notificano al proprietario del bucket se la replica dell'oggetto supera la soglia dei 15 minuti o si verifica dopo tale intervallo di tempo. Con S3 RTC, è possibile che Notifiche di eventi Amazon S3 invii una notifica nel caso raro in cui gli oggetti non vengano replicati entro 15 minuti e quando tali oggetti vengono replicati una volta superata la soglia di 15 minuti.

Gli eventi di replica sono disponibili entro 15 minuti dall'abilitazione di S3 RTC. Le notifiche di eventi Amazon S3 sono disponibili tramite Amazon SQS, Amazon SNS o AWS Lambda Per ulteriori informazioni, consulta [the section called “Ricezione eventi di errore di replica”](#).

Best practice e linee guida per S3 RTC

Per la replica dei dati in Amazon S3 con controllo del tempo di replica di S3 (S3 RTC) abilitato, attenersi alle seguenti linee guida di best practice per ottimizzare le prestazioni di replica dei carichi di lavoro.

Argomenti

- [Linee guida sulle prestazioni per la frequenza di richieste e la replica di Amazon S3](#)
- [Stima delle frequenze di richieste di replica](#)
- [Superamento delle quote di velocità di trasferimento dati di S3 RTC](#)
- [AWS KMS tassi di richiesta di replica di oggetti crittografati](#)

Linee guida sulle prestazioni per la frequenza di richieste e la replica di Amazon S3

Le applicazioni possono raggiungere migliaia di transazioni al secondo nelle prestazioni di richiesta durante il caricamento e il recupero di storage da Amazon S3. Ad esempio, un'applicazione può raggiungere almeno 3.500 richieste PUT/COPY/POST/DELETE o 5.500 richieste GET/HEAD al secondo per prefisso in un bucket S3, incluse le richieste che Replica Amazon S3 effettua per conto dell'utente. Non esistono limiti al numero di prefissi in un bucket. È possibile aumentare le proprie performance in lettura o scrittura parallelizzando le scritture. Ad esempio, se si creano 10 prefissi in un bucket S3 per parallelizzare le letture, è possibile scalare le prestazioni di lettura a 55.000 richieste di lettura al secondo.

Amazon S3 riduce orizzontalmente le risorse in modo automatico in risposta a frequenze di richieste sostenute oltre queste linee guida o a frequenze di richieste sostenute in contemporanea a richieste LIST. Mentre Amazon S3 si ottimizza internamente per la nuova frequenza di richieste, potresti ricevere temporaneamente risposte HTTP 503 fino al completamento dell'ottimizzazione. Questo comportamento potrebbe verificarsi con gli aumenti delle frequenze di richiesta al secondo o quando si abilita per la prima volta S3 RTC. Durante questi periodi, la latenza di replica potrebbe aumentare. L'accordo sul livello di servizio (SLA) RTC S3 non si applica ai periodi di tempo in cui vengono superate le linee guida prestazionali di Amazon S3 sulle richieste al secondo.

Lo SLA di S3 RTC non si applica neanche ai periodi di tempo in cui la velocità di trasferimento dati di replica supera il limite predefinito di 1 Gbps. Se si prevede che la velocità di trasferimento della replica superi 1 Gbps, è possibile contattare il [Centro Supporto AWS](#) o utilizzare [Service Quotas](#) per richiedere un aumento della quota della velocità di trasferimento della replica.

Stima delle frequenze di richieste di replica

La frequenza di richieste totale, incluse le richieste effettuate da Replica Amazon S3 per conto dell'utente, deve rientrare nelle linee guida sulla frequenza di richieste di Amazon S3 per i bucket di origine e di destinazione della replica. Per ogni oggetto replicato, Replica Amazon S3 esegue fino a cinque richieste GET/HEAD e una richiesta PUT al bucket di origine e una richiesta PUT a ciascun bucket di destinazione.

Ad esempio, se si prevede di replicare 100 oggetti al secondo, Replica Amazon S3 può eseguire 100 richieste PUT aggiuntive per conto dell'utente per un totale di 200 richieste PUT al secondo nel bucket S3 di origine. Replica Amazon S3 può anche eseguire fino a 500 richieste GET/HEAD (5 richieste GET/HEAD per ogni oggetto replicato).

Note

Vengono addebitati i costi per una sola richiesta PUT per oggetto replicato. Per ulteriori informazioni, consulta i prezzi nelle [domande frequenti di Amazon S3 sulla replica](#).

Superamento delle quote di velocità di trasferimento dati di S3 RTC

Se si prevede che la velocità di trasferimento dati di S3 RTC superi la quota predefinita di 1 Gbps, contattare il [Centro Supporto AWS](#) o utilizzare [Service Quotas](#) per richiedere un aumento della quota. Nel calcolo della velocità di trasferimento, includi i dati di annotazione perché i byte di annotazione vengono conteggiati ai fini della quota di velocità di trasferimento dati RTC S3.

AWS KMS tassi di richiesta di replica di oggetti crittografati

Quando si replicano oggetti crittografati con crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS), si applicano le quote per AWS KMS le richieste al secondo. AWS KMS potrebbe rifiutare una richiesta altrimenti valida perché la frequenza delle richieste supera la quota per il numero di richieste al secondo. Quando una richiesta viene limitata, AWS KMS restituisce un errore. `ThrottlingException` La quota del tasso di AWS KMS richiesta si applica alle richieste effettuate direttamente e alle richieste effettuate da Amazon S3 Replication per tuo conto.

Ad esempio, se prevedi di replicare 1.000 oggetti al secondo, puoi sottrarre 2.000 richieste dalla tua AWS KMS quota di richieste. La frequenza di richieste al secondo risultante è disponibile per i AWS KMS carichi di lavoro, esclusa la replica. Puoi utilizzare le metriche delle [AWS KMS richieste in Amazon CloudWatch](#) per monitorare il tasso totale di AWS KMS richieste sul tuo Account AWS

Per richiedere un aumento della quota di AWS KMS richieste al secondo, contatta il [Supporto AWS Centro assistenza](#) o utilizza [Service Quotas](#).

Abilitazione di S3 Replication Time Control

Puoi iniziare a utilizzare S3 Replication Time Control (S3 RTC) con una regola di replica nuova o esistente. È possibile scegliere di applicare la regola di replica a un intero bucket o a oggetti con un prefisso o un tag specifico. Quando si attiva S3 RTC, i parametri di Replica S3 vengono abilitati anche nella regola di replica.

Puoi configurare S3 RTC utilizzando la console Amazon S3, l'API Amazon S3, gli AWS SDK e (). AWS Command Line Interface AWS CLI

Utilizzo della console S3

Per istruzioni dettagliate, consulta [Configurazione della replica per i bucket nello stesso account](#). Questo argomento fornisce istruzioni per abilitare S3 RTC nella configurazione di replica quando i bucket di origine e destinazione sono di proprietà identica e diversa. Account AWS

Utilizzo di AWS CLI

Per AWS CLI replicare oggetti con S3 RTC abilitato, è necessario creare bucket, abilitare il controllo delle versioni sui bucket, creare un ruolo IAM che autorizza Amazon S3 a replicare gli oggetti e aggiungere la configurazione di replica al bucket di origine. La configurazione della replica deve avere S3 RTC abilitato, come mostrato nel seguente esempio.

Per istruzioni dettagliate sull'impostazione della configurazione di replica utilizzando il, consulta. AWS CLI [Configurazione della replica per i bucket nello stesso account](#)

Il seguente esempio di configurazione della replica abilita e imposta i valori `ReplicationTime` e `EventThreshold` per una regola di replica. L'attivazione e l'impostazione di questi valori abilita S3 RTC sulla regola.

```
{
  "Rules": [
    {
      "Status": "Enabled",
      "Filter": {
        "Prefix": "Tax"
      },
      "DeleteMarkerReplication": {
        "Status": "Disabled"
      }
    }
  ]
}
```

```
    },
    "Destination": {
      "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
      "Metrics": {
        "Status": "Enabled",
        "EventThreshold": {
          "Minutes": 15
        }
      },
      "ReplicationTime": {
        "Status": "Enabled",
        "Time": {
          "Minutes": 15
        }
      }
    },
    "Priority": 1
  },
  "Role": "IAM-Role-ARN"
}
```

Important

`Metrics:EventThreshold:Minutes` e `ReplicationTime:Time:Minutes` possono avere solo 15 come valore valido.

Utilizzo di AWS SDK per Java

Di seguito è riportato un esempio Java per aggiungere la configurazione della replica con controllo del tempo di replica di S3 (S3 RTC).

```
import software.amazon.awssdk.auth.credentials.AwsBasicCredentials;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.model.DeleteMarkerReplication;
import software.amazon.awssdk.services.s3.model.Destination;
import software.amazon.awssdk.services.s3.model.Metrics;
import software.amazon.awssdk.services.s3.model.MetricsStatus;
import software.amazon.awssdk.services.s3.model.PutBucketReplicationRequest;
import software.amazon.awssdk.services.s3.model.ReplicationConfiguration;
import software.amazon.awssdk.services.s3.model.ReplicationRule;
```

```
import software.amazon.awssdk.services.s3.model.ReplicationRuleFilter;
import software.amazon.awssdk.services.s3.model.ReplicationTime;
import software.amazon.awssdk.services.s3.model.ReplicationTimeStatus;
import software.amazon.awssdk.services.s3.model.ReplicationTimeValue;

public class Main {

    public static void main(String[] args) {
        S3Client s3 = S3Client.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(() -> AwsBasicCredentials.create(
                "AWS_ACCESS_KEY_ID",
                "AWS_SECRET_ACCESS_KEY"))
            .build();

        ReplicationConfiguration replicationConfig = ReplicationConfiguration
            .builder()
            .rules(
                ReplicationRule
                    .builder()
                    .status("Enabled")
                    .priority(1)
                    .deleteMarkerReplication(
                        DeleteMarkerReplication
                            .builder()
                            .status("Disabled")
                            .build()
                    )
                )
            .destination(
                Destination
                    .builder()
                    .bucket("destination_bucket_arn")
                    .replicationTime(
                        ReplicationTime.builder().time(
                            ReplicationTimeValue.builder().minutes(15).build()
                        ).status(
                            ReplicationTimeStatus.ENABLED
                        ).build()
                    )
                )
            .metrics(
                Metrics.builder().eventThreshold(
                    ReplicationTimeValue.builder().minutes(15).build()
                ).status(
```

```

        MetricsStatus.ENABLED
    ).build()
)
    .build()
)
    .filter(
        ReplicationRuleFilter
        .builder()
        .prefix("testtest")
        .build()
    )
    .build())
    .role("role_arn")
    .build();

// Put replication configuration
PutBucketReplicationRequest putBucketReplicationRequest =
PutBucketReplicationRequest
    .builder()
    .bucket("source_bucket")
    .replicationConfiguration(replicationConfig)
    .build();

s3.putBucketReplication(putBucketReplicationRequest);
}
}

```

Replica di oggetti crittografati (,,,) SSE-S3 SSE-KMS DSSE-KMS SSE-C

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS. Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

Quando si replicano oggetti che sono stati crittografati utilizzando la crittografia lato server, è necessario prestare particolare attenzione. Amazon S3 supporta i seguenti tipi di crittografia lato server:

- Server-side crittografia con SSE-S3 chiavi gestite da Amazon S3 ()
- Server-side crittografia con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS)
- Dual-layer crittografia lato server con AWS KMS chiavi () DSSE-KMS
- Server-side crittografia con chiavi fornite dal cliente () SSE-C

Per ulteriori informazioni sulla crittografia lato server, consulta [the section called “Server-side crittografia”](#).

Questo argomento spiega le autorizzazioni necessarie per indirizzare Amazon S3 a replicare oggetti che sono stati crittografati utilizzando la crittografia lato server. Questo argomento fornisce anche elementi di configurazione aggiuntivi che è possibile aggiungere ed esempi di policy AWS Identity and Access Management (IAM) che concedono le autorizzazioni necessarie per replicare oggetti crittografati.

Per un esempio con istruzioni dettagliate, consulta [Abilitazione della replica per oggetti crittografati](#). Per informazioni sulla creazione di una configurazione di replica, consulta [Replica di oggetti all'interno e tra le Regioni](#).

Note

Puoi usare Multi-region AWS KMS keys in Amazon S3. Tuttavia, Amazon S3 attualmente tratta le chiavi multiregionali come se fossero chiavi monoregionali e non utilizza le caratteristiche multiregionali della chiave. Per ulteriori informazioni, consulta [Utilizzo delle chiavi multiregione](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Argomenti

- [In che modo la crittografia predefinita del bucket influisce sulla replica](#)
- [Replica di oggetti crittografati con SSE-C](#)
- [Replica di oggetti crittografati con SSE-S3,, o SSE-KMS DSSE-KMS](#)
- [Abilitazione della replica per oggetti crittografati](#)

In che modo la crittografia predefinita del bucket influisce sulla replica

Una volta abilitata la crittografia predefinita per un bucket di destinazione della replica, si applica il seguente comportamento di crittografia:

- Se gli oggetti nel bucket di origine non sono crittografati, gli oggetti replicati nel bucket di destinazione vengono crittografati in base alle impostazioni di crittografia predefinita del bucket di destinazione. Di conseguenza, i tag di entità (ETag) degli oggetti di origine differiscono dagli ETag degli oggetti di replica. Se disponi di applicazioni che utilizzano ETag, devi aggiornarle per tenere conto di questa differenza.
- Se gli oggetti nel bucket di origine sono crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3), la crittografia lato server con chiavi () AWS Key Management Service (AWS KMS) o la crittografia lato server a doppio livello con AWS KMS chiavi (SSE-KMS), gli oggetti di replica nel bucket di destinazione utilizzano lo stesso tipo di crittografia degli oggetti di origine. DSSE-KMS Le impostazioni della crittografia predefinita del bucket di destinazione non vengono utilizzate.

Replica di oggetti crittografati con SSE-C

Utilizzando la crittografia lato server con chiavi fornite dal cliente (SSE-C), è possibile gestire le proprie chiavi di crittografia proprietarie. Con SSE-C, gestisci le chiavi mentre Amazon S3 gestisce il processo di crittografia e decrittografia. È necessario fornire una chiave di crittografia come parte della richiesta, ma non è necessario scrivere codice per eseguire la crittografia o la decrittografia degli oggetti. Quando carichi un oggetto, Amazon S3 ne esegue la crittografia utilizzando la chiave che hai specificato. Quindi Amazon S3 elimina la chiave dalla memoria. Quando viene recuperato un oggetto, è necessario fornire la stessa chiave di crittografia come parte della richiesta. Per ulteriori informazioni, consulta [the section called “Customer-provided chiavi di crittografia \(\) SSE-C”](#).

S3 Replication supporta oggetti crittografati con SSE-C. Puoi configurare la replica SSE-C degli oggetti nella console Amazon S3 o con gli AWS SDK nello stesso modo in cui configuri la replica per oggetti non crittografati. Non sono disponibili SSE-C autorizzazioni aggiuntive oltre a quelle attualmente richieste per la replica.

S3 Replication replica automaticamente gli oggetti SSE-C crittografati appena caricati se sono idonei, come specificato nella configurazione di S3 Replication. Per la replica di oggetti esistenti nei bucket, utilizza la replica in batch in S3. Per ulteriori informazioni sulla replica di oggetti, consulta [the section called “Configurazione della replica in tempo reale”](#) e [the section called “Replica di oggetti esistenti”](#).

Non sono previsti costi aggiuntivi per la replica degli oggetti. SSE-C Per informazioni dettagliate sui prezzi della replica, consulta [Prezzi di Amazon S3](#).

Replica di oggetti crittografati con SSE-S3,, o SSE-KMS DSSE-KMS

Per impostazione predefinita, Amazon S3 non replica oggetti crittografati con o. SSE-KMS DSSE-KMS Questa sezione illustra un'ulteriore configurazione che puoi aggiungere per fare in modo che Amazon S3 replichi questi oggetti.

Per un esempio con istruzioni dettagliate, consulta [Abilitazione della replica per oggetti crittografati](#). Per informazioni sulla creazione di una configurazione di replica, consulta [Replica di oggetti all'interno e tra le Regioni](#).

Specifica di informazioni aggiuntive nella configurazione di replica

Nella configurazione di replica, è necessario eseguire queste operazioni:

- Nell'*Destination* elemento della configurazione di replica, aggiungi l'ID della chiave simmetrica gestita dal AWS KMS cliente che desideri che Amazon S3 utilizzi per crittografare le repliche degli oggetti, come mostrato nel seguente esempio di configurazione di replica.
- Attiva esplicitamente abilitando la replica degli oggetti crittografati utilizzando le chiavi KMS (o). SSE-KMS DSSE-KMS Per attivare, aggiungi l'elemento *SourceSelectionCriteria*, come mostrato nel seguente esempio di configurazione della replica.

```
<ReplicationConfiguration>
  <Rule>
    ...
    <SourceSelectionCriteria>
      <SseKmsEncryptedObjects>
        <Status>Enabled</Status>
      </SseKmsEncryptedObjects>
    </SourceSelectionCriteria>

    <Destination>
      ...
      <EncryptionConfiguration>
        <ReplicaKmsKeyID>AWS KMS key ARN or Key Alias ARN that's in the same
        Regione AWS as the destination bucket.</ReplicaKmsKeyID>
      </EncryptionConfiguration>
    </Destination>
    ...
  </Rule>
</ReplicationConfiguration>
```



```
</Rule>
</ReplicationConfiguration>
```

Important

- La chiave KMS deve essere stata creata nello stesso bucket di Regione AWS destinazione.
- Chiave KMS deve essere valida. L'operazione PutBucketReplication dell'API non controlla la validità delle chiavi KMS. Se utilizzi una chiave KMS non valida, viene restituito il codice di stato HTTP 200 OK in risposta, ma la replica non riesce.

Nell'esempio seguente viene illustrata una configurazione di replica che include gli elementi di configurazione opzionali. Questa configurazione di replica ha una regola. La regola si applica agli oggetti con il prefisso della chiave *Tax*. Amazon S3 utilizza l' AWS KMS key ID specificato per crittografare queste repliche di oggetti.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration>
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <ID>Rule-1</ID>
    <Priority>1</Priority>
    <Status>Enabled</Status>
    <DeleteMarkerReplication>
      <Status>Disabled</Status>
    </DeleteMarkerReplication>
    <Filter>
      <Prefix>Tax</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
      <EncryptionConfiguration>
        <ReplicaKmsKeyID>AWS KMS key ARN or Key Alias ARN that's in the same
        Regione AWS as the destination bucket.</ReplicaKmsKeyID>
      </EncryptionConfiguration>
    </Destination>
    <SourceSelectionCriteria>
      <SseKmsEncryptedObjects>
        <Status>Enabled</Status>
      </SseKmsEncryptedObjects>
    </SourceSelectionCriteria>
```

```
</Rule>  
</ReplicationConfiguration>
```

Concessione di autorizzazioni aggiuntive per il ruolo IAM

Per replicare oggetti crittografati a riposo utilizzando SSE-S3, o SSE-KMS DSSE-KMS, concedi le seguenti autorizzazioni aggiuntive al ruolo AWS Identity and Access Management (IAM) specificato nella configurazione di replica. Queste autorizzazioni vengono concesse aggiornando la policy di autorizzazione associata al ruolo IAM.

- **s3:GetObjectVersionForReplication** azione per gli oggetti sorgente: questa azione consente ad Amazon S3 di replicare sia oggetti non crittografati sia oggetti creati con crittografia lato server utilizzando, o. SSE-S3 SSE-KMS DSSE-KMS

Note

Ti consigliamo di utilizzare l'operazione `s3:GetObjectVersionForReplication` anziché l'operazione `s3:GetObjectVersion` in quanto `s3:GetObjectVersionForReplication` concede ad Amazon S3 solo le autorizzazioni minime necessarie per la replica. Inoltre, l'`s3:GetObjectVersion` azione consente la replica di oggetti non crittografati, ma non di SSE-S3-encrypted oggetti crittografati utilizzando chiavi KMS (o). SSE-KMS DSSE-KMS

- **kms:Decrypte kms:Encrypt** AWS KMS azioni per le chiavi KMS
 - È necessario concedere `kms:Decrypt` le autorizzazioni per AWS KMS key ciò che protegge l'oggetto sorgente.
 - È necessario concedere `kms:Encrypt` le autorizzazioni per proteggere AWS KMS key la replica dell'oggetto.
- **kms:GenerateDataKey** azione per replicare oggetti in testo normale: se stai replicando oggetti in testo normale in un bucket con SSE-KMS o la DSSE-KMS crittografia abilitata per impostazione predefinita, devi includere l'`kms:GenerateDataKey` autorizzazione per il contesto di crittografia di destinazione e la chiave KMS nella policy IAM.

Important

Se utilizzi S3 Batch Replication per replicare set di dati in più regioni e in precedenza il tipo di crittografia lato server era aggiornato dal al, potresti aver bisogno di autorizzazioni

aggiuntive. SSE-S3 SSE-KMS Nel bucket della regione di origine, è necessario disporre delle autorizzazioni. `kms:decrypt` Quindi, avrai bisogno delle `kms:encrypt` autorizzazioni `kms:decrypt` e per il bucket nella regione di destinazione.

Ti consigliamo di limitare queste autorizzazioni solo ai bucket e agli oggetti di destinazione utilizzando le chiavi di condizione. AWS KMS Il Account AWS proprietario del ruolo IAM deve disporre delle autorizzazioni `kms:Encrypt` e delle `kms:Decrypt` azioni per le chiavi KMS elencate nella policy. Se le chiavi KMS sono di proprietà di un altro Account AWS, il proprietario delle chiavi KMS deve concedere tali autorizzazioni al proprietario del Account AWS ruolo IAM. Per ulteriori informazioni sulla gestione dell'accesso a queste chiavi KMS, consulta [Using IAM policies with AWS KMS](#) nella Developer Guide. AWS Key Management Service

Chiavi bucket S3 e replica

Per utilizzare la replica con una chiave S3 Bucket, la AWS KMS key policy per la chiave KMS utilizzata per crittografare la replica dell'oggetto deve includere l'autorizzazione per il `kms:Decrypt` principale chiamante. La chiamata a `kms:Decrypt` verifica l'integrità della chiave bucket S3 prima del suo utilizzo. Per ulteriori informazioni, consulta [Utilizzo di una chiave bucket S3 con la replica](#).

Quando una chiave del bucket S3 è abilitata per il bucket di origine o di destinazione, il contesto di crittografia sarà il nome della risorsa Amazon (ARN) del bucket e non l'ARN dell'oggetto, ad esempio `arn:aws:s3:::bucket_ARN`. Dovrai aggiornare le policy IAM per utilizzare l'ARN del bucket per il contesto di crittografia:

```
"kms:EncryptionContext:aws:s3:arn": [  
  "arn:aws:s3:::bucket_ARN"  
]
```

Per ulteriori informazioni, consulta [Contesto di crittografia \(x-amz-server-side-encryption-context\)](#) (nella sezione relativa a REST API) e [Modifiche alla nota prima dell'abilitazione di una chiave bucket S3](#).

Politiche di esempio: utilizzo e con la replica SSE-S3 SSE-KMS

Il seguente esempio di policy IAM mostra le istruzioni per l'utilizzo SSE-S3 e SSE-KMS con la replica.

Example— Utilizzo SSE-KMS con bucket di destinazione separati

La seguente politica di esempio mostra le istruzioni per l'utilizzo SSE-KMS con bucket di destinazione separati.

Example— Replica di oggetti creati con e SSE-S3 SSE-KMS

Quella che segue è una policy IAM completa che concede le autorizzazioni necessarie per replicare oggetti non crittografati, oggetti creati con e oggetti creati con SSE-S3. SSE-KMS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetReplicationConfiguration",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
    }
  ],
}
```

```

{
  "Action":[
    "kms:Decrypt"
  ],
  "Effect":"Allow",
  "Condition":{"
    "StringLike":{"
      "kms:ViaService":"s3.us-east-1.amazonaws.com",
      "kms:EncryptionContext:aws:s3:arn":["
        "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
      ]
    }
  },
  "Resource":["
    "arn:aws:kms:us-east-1:111122223333:key/key-id"
  ]
},
{
  "Action":[
    "kms:Encrypt"
  ],
  "Effect":"Allow",
  "Condition":{"
    "StringLike":{"
      "kms:ViaService":"s3.us-east-1.amazonaws.com",
      "kms:EncryptionContext:aws:s3:arn":["
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/prefix1*"
      ]
    }
  },
  "Resource":["
    "arn:aws:kms:us-east-1:111122223333:key/key-id"
  ]
}
]
}

```

Example- Replica oggetti con chiavi bucket S3

Di seguito è riportata una policy IAM completa che concede le autorizzazioni necessarie per la replica degli oggetti con chiavi bucket S3.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetReplicationConfiguration",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
    },
    {
      "Action": [
        "kms:Decrypt"
      ],
      "Effect": "Allow",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "s3.us-east-1.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn": [
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
          ]
        }
      }
    }
  ]
}
```

```

    ]
  },
  "Resource": [
    "arn:aws:kms:us-east-1:111122223333:key/key-id"
  ]
},
{
  "Action": [
    "kms:Encrypt"
  ],
  "Effect": "Allow",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "s3.us-east-1.amazonaws.com",
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      ]
    }
  },
  "Resource": [
    "arn:aws:kms:us-east-1:111122223333:key/key-id"
  ]
}
]
}

```

Concessione di autorizzazioni aggiuntive per scenari multi-account

In uno scenario con più account, in cui i bucket di origine e di destinazione sono di proprietà diversa Account AWS, è possibile utilizzare una chiave KMS per crittografare le repliche degli oggetti. Tuttavia, il proprietario della chiave KMS deve concedere al proprietario del bucket di origine l'autorizzazione per utilizzare la chiave KMS.

Note

Se devi replicare SSE-KMS i dati su più account, la regola di replica deve specificare una chiave gestita dal [cliente per l'account di destinazione](#). AWS KMS [Chiavi gestite da AWS](#) non consentono l'uso tra account e pertanto non possono essere utilizzati per eseguire la replica tra account.

Per concedere al proprietario del bucket di origine l'autorizzazione a utilizzare la chiave KMS (AWS KMS console)

1. Accedi Console di gestione AWS e apri la AWS KMS console all'indirizzo <https://console.aws.amazon.com/kms>.
2. Per modificare il Regione AWS, usa il selettore di regione nell'angolo in alto a destra della pagina.
3. Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente.
4. Scegli la chiave KMS.
5. In Configurazione generale, seleziona la scheda Policy delle chiavi.
6. Scorri verso il basso fino a Altro. Account AWS
7. Scegli Aggiungi altro Account AWS.

Viene visualizzata la finestra di dialogo Altri Account AWS.

8. Nella finestra di dialogo, scegli Aggiungi un altro Account AWS. Per `arn:aws:iam::`, inserisci l'ID account del bucket di origine.
9. Scegli Save changes (Salva modifiche).

Per concedere al proprietario del bucket di origine il permesso di utilizzare la chiave KMS (AWS CLI)

- Per informazioni sul comando `put-key-policy` AWS Command Line Interface (AWS CLI), vedi [put-key-policy](#) nel AWS CLI Command Reference. Per ulteriori informazioni sull'operazione API `PutKeyPolicy` sottostante, consulta [PutKeyPolicy](#) nella [Guida di riferimento delle API di AWS Key Management Service](#).

AWS KMS considerazioni sulla quota delle transazioni

Quando aggiungi molti nuovi oggetti con AWS KMS crittografia dopo aver abilitato Cross-Region Replication (CRR), potresti riscontrare limitazioni (errori HTTP). `503 Service Unavailable` La limitazione (della larghezza di banda della rete) si verifica quando il numero di transazioni AWS KMS al secondo supera la quota corrente. Per ulteriori informazioni, consulta [Quote](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per richiedere un aumento della quota, è possibile utilizzare Service Quotas. Per ulteriori informazioni, consulta la sezione [Richiesta di un aumento di quota](#). Se Service Quotas non è supportato nella tua regione, apri un caso. [Supporto AWS](#)

Abilitazione della replica per oggetti crittografati

Per impostazione predefinita, Amazon S3 non replica gli oggetti crittografati utilizzando la crittografia lato server con AWS Key Management Service (AWS KMS) chiavi () o la crittografia lato server a doppio livello con chiavi (SSE-KMS). AWS KMS DSSE-KMS Per replicare oggetti crittografati con SSE-KMS o DSS-KMS, devi modificare la configurazione di replica del bucket per dire ad Amazon S3 di replicare questi oggetti. Questo esempio spiega come utilizzare la console Amazon S3 e la AWS Command Line Interface (AWS CLI) per modificare la configurazione di replica del bucket per abilitare la replica di oggetti crittografati.

Note

Quando una chiave del bucket S3 è abilitata per il bucket di origine o di destinazione, il contesto di crittografia sarà il nome della risorsa Amazon (ARN) del bucket e non l'ARN dell'oggetto. Dovrai aggiornare le policy IAM per utilizzare l'ARN del bucket per il contesto di crittografia. Per ulteriori informazioni, consulta [Chiavi bucket S3 e replica](#).

Note

Puoi usare AWS KMS keys Multi-region in Amazon S3. Tuttavia, Amazon S3 attualmente tratta le chiavi multiregionali come se fossero chiavi monoregionali e non utilizza le caratteristiche multiregionali della chiave. Per ulteriori informazioni, consulta [Utilizzo delle chiavi multiregione](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Utilizzo della console S3

Per istruzioni dettagliate, consulta [Configurazione della replica per i bucket nello stesso account](#). Questo argomento fornisce istruzioni per impostare una configurazione di replica quando i bucket di origine e di destinazione sono di proprietà identica e diversa. Account AWS

Utilizzo di AWS CLI

Per replicare oggetti crittografati con AWS CLI, procedi come segue:

- Crea i bucket di origine e di destinazione e abilita il controllo delle versioni per questi bucket.
- Crea un ruolo di servizio AWS Identity and Access Management (IAM) che conceda ad Amazon S3 il permesso di replicare oggetti. Le autorizzazioni del ruolo IAM includono le autorizzazioni necessarie per replicare gli oggetti crittografati.
- Aggiungi una configurazione di replica al bucket di origine. La configurazione di replica fornisce informazioni relative alla replica di oggetti crittografati con le chiavi KMS.
- Aggiungi gli oggetti crittografati al bucket di origine.
- Esegui il test della configurazione per verificare che gli oggetti crittografati vengano replicati nel bucket di destinazione.

Le procedure seguenti ti guidano attraverso questo processo.

Per replicare oggetti crittografati sul lato server (AWS CLI)

Per utilizzare gli esempi in questa procedura, sostituire *user input placeholders* con le proprie informazioni.

1. In questo esempio vengono creati entrambi i bucket di origine (*amzn-s3-demo-source-bucket*) e di destinazione (*amzn-s3-demo-destination-bucket*) nello stesso Account AWS. Imposti anche un profilo di credenziali per la AWS CLI. In questo esempio si utilizza il nome del profilo *acctA*.

Per informazioni sull'impostazione di profili con credenziali e sull'uso di profili denominati, consulta [Impostazioni del file di configurazione e delle credenziali](#) nella Guida per l'utente di AWS Command Line Interface .

2. Usa i seguenti comandi per creare il bucket *amzn-s3-demo-source-bucket* e abilitare il controllo delle versioni. Il seguente comando di esempio crea il bucket *amzn-s3-demo-source-bucket* nella Regione Stati Uniti orientali (Virginia settentrionale) (us-east-1).

```
aws s3api create-bucket \  
--bucket amzn-s3-demo-source-bucket \  
--region us-east-1 \  
--profile acctA
```

```
aws s3api put-bucket-versioning \  
--bucket amzn-s3-demo-source-bucket \  
--versioning-configuration Status=Enabled \  

```

```
--profile acctA
```

3. Usa i seguenti comandi per creare il bucket *amzn-s3-demo-destination-bucket* e abilitare il controllo delle versioni. Il seguente comando di esempio crea il bucket *amzn-s3-demo-destination-bucket* nella Regione Stati Uniti occidentali (Oregon) (us-west-2).

Note

Per impostare la configurazione di replica quando entrambi i bucket *amzn-s3-demo-source-bucket* e *amzn-s3-demo-destination-bucket* si trovano nello stesso Account AWS, utilizza lo stesso profilo. Questo esempio usa *acctA*. Per configurare la replica quando i bucket sono di proprietà di diversi Account AWS, è necessario specificare profili diversi per ciascuno.

```
aws s3api create-bucket \  
--bucket amzn-s3-demo-destination-bucket \  
--region us-west-2 \  
--create-bucket-configuration LocationConstraint=us-west-2 \  
--profile acctA
```

```
aws s3api put-bucket-versioning \  
--bucket amzn-s3-demo-destination-bucket \  
--versioning-configuration Status=Enabled \  
--profile acctA
```

4. Quindi, crea un ruolo di servizio IAM. Questo ruolo verrà specificato nella configurazione della replica che verrà aggiunta al bucket *amzn-s3-demo-source-bucket* in un secondo momento. Amazon S3 assume questo ruolo per replicare gli oggetti per tuo conto. Il ruolo IAM si crea in due fasi:

- Creazione di un ruolo del servizio
- Collegare una policy di autorizzazione al ruolo.

a. Per creare un ruolo di servizio IAM, procedi come segue:

- i. Copiare la seguente policy di attendibilità e salvarla in un file denominato *s3-role-trust-policy-kmsobj*.json nella directory corrente sul computer locale. Questa

policy fornisce le autorizzazioni ai principali del servizio Amazon S3 per assumere il ruolo in modo che Amazon S3 possa eseguire attività per conto dell'utente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- ii. Usa il comando seguente per creare il ruolo:

```
$ aws iam create-role \
--role-name replicationRolekmsobj \
--assume-role-policy-document file://s3-role-trust-policy-kmsobj.json \
--profile acctA
```

- b. Quindi, collega una policy di autorizzazione al ruolo. Questa policy di accesso concede le autorizzazioni per varie operazioni su oggetti e bucket Amazon S3.
- i. Copiare la seguente policy di autorizzazioni e salvarla in un file denominato *s3-role-permissions-policykmsobj.json* nella directory corrente sul computer locale. Crea un ruolo IAM e successivamente collegalo alla policy.

 Important

Nella politica delle autorizzazioni, si specificano gli ID AWS KMS chiave che verranno utilizzati per la crittografia dei *amzn-s3-demo-source-bucket* bucket e *amzn-s3-demo-destination-bucket*. È necessario creare due chiavi KMS separate per i bucket e *amzn-s3-demo-source-bucket* *amzn-*

s3-demo-destination-bucket AWS KMS keys non sono condivisi al di fuori di quella Regione AWS in cui sono stati creati.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Action":[
        "s3:ListBucket",
        "s3:GetReplicationConfiguration",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Effect":"Allow",
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-source-bucket",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
      ]
    },
    {
      "Action":[
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags"
      ],
      "Effect":"Allow",
      "Condition":{"
        "StringLikeIfExists":{"
          "s3:x-amz-server-side-encryption":["
            "aws:kms",
            "AES256",
            "aws:kms:dsse"
          ],
          "s3:x-amz-server-side-encryption-aws-kms-key-id":["
            "AWS KMS key IDs(in ARN format) to use for
            encrypting object replicas"
          ]
        }
      }
    }
  ]
}
```

```

    },
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
  },
  {
    "Action": [
      "kms:Decrypt"
    ],
    "Effect": "Allow",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "s3.us-east-1.amazonaws.com",
        "kms:EncryptionContext:aws:s3:arn": [
          "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
        ]
      }
    },
    "Resource": [
      "arn:aws:kms:us-east-1:111122223333:key/key-id"
    ]
  },
  {
    "Action": [
      "kms:Encrypt"
    ],
    "Effect": "Allow",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "s3.us-west-2.amazonaws.com",
        "kms:EncryptionContext:aws:s3:arn": [
          "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        ]
      }
    },
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/key-id"
    ]
  }
]
}

```

- ii. Creare una policy e collegarla al ruolo.

```

$ aws iam put-role-policy \
--role-name replicationRolekmsobj \

```

```
--policy-document file://s3-role-permissions-policykmsobj.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

5. Quindi, aggiungi la seguente configurazione di replica al bucket *amzn-s3-demo-source-bucket* che indica ad Amazon S3 di replicare gli oggetti con prefisso *Tax/* nel bucket *amzn-s3-demo-destination-bucket*.

Important

Nella configurazione di replica dovrai specificare il ruolo IAM che Amazon S3 può assumere. Puoi effettuare questa operazione solo se disponi dell'autorizzazione `iam:PassRole`. Il profilo specificato nel comando della CLI deve disporre di questa autorizzazione. Per ulteriori informazioni, consulta [Concessione di autorizzazioni utente per il passaggio di un ruolo a un Servizio AWS](#) nella Guida per l'utente di IAM.

```
<ReplicationConfiguration>
  <Role>IAM-Role-ARN</Role>
  <Rule>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
      <Status>Disabled</Status>
    </DeleteMarkerReplication>
    <Filter>
      <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <SourceSelectionCriteria>
      <SseKmsEncryptedObjects>
        <Status>Enabled</Status>
      </SseKmsEncryptedObjects>
    </SourceSelectionCriteria>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
      <EncryptionConfiguration>
        <ReplicaKmsKeyID>AWS KMS key IDs to use for encrypting object replicas</
ReplicaKmsKeyID>
      </EncryptionConfiguration>
    </Destination>
  </Rule>
```

```
</ReplicationConfiguration>
```

Per aggiungere una configurazione di replica al bucket *amzn-s3-demo-source-bucket*, procedi come segue:

- a. AWS CLI Richiede di specificare la configurazione di replica come JSON. Salvare il seguente JSON in un file (*replication.json*) nella directory corrente sul computer locale.

```
{
  "Role": "IAM-Role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": {
        "Status": "Disabled"
      },
      "Filter": {
        "Prefix": "Tax"
      },
      "Destination": {
        "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "EncryptionConfiguration": {
          "ReplicaKmsKeyID": "AWS KMS key IDs (in ARN format) to use for encrypting object replicas"
        }
      },
      "SourceSelectionCriteria": {
        "SseKmsEncryptedObjects": {
          "Status": "Enabled"
        }
      }
    }
  ]
}
```

- b. Modifica il JSON per fornire valori per il bucket *amzn-s3-demo-destination-bucket*, *AWS KMS key IDs (in ARN format)* e *IAM-role-ARN*. Salvare le modifiche.

- c. Esegui il comando seguente per aggiungere la configurazione di replica al bucket *amzn-s3-demo-source-bucket*. Assicurati di fornire il nome del bucket di *amzn-s3-demo-source-bucket*.

```
$ aws s3api put-bucket-replication \  
--replication-configuration file://replication.json \  
--bucket amzn-s3-demo-source-bucket \  
--profile acctA
```

6. Esegui il test della configurazione per verificare che gli oggetti crittografati vengano replicati. Nella console di Amazon S3 effettuare quanto segue:
 - a. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
 - b. Nel bucket di *amzn-s3-demo-source-bucket*, crea una cartella denominata *Tax*.
 - c. Aggiungere oggetti campione alla cartella. Assicurati di scegliere l'opzione di crittografia e specifica la chiave KMS per crittografare gli oggetti.
 - d. Verifica che il bucket *amzn-s3-demo-destination-bucket* contenga le repliche dell'oggetto e che queste vengano crittografate utilizzando la chiave KMS specificata nella configurazione. Per ulteriori informazioni, consulta [the section called “Ottenimento dello stato della replica”](#).

Utilizzo di AWS SDK

Per un esempio di codice che illustra come aggiungere una configurazione di replica, consulta [Utilizzo di AWS SDK](#). La configurazione della replica deve essere modificata di conseguenza.

Replica delle modifiche ai metadati con la sincronizzazione delle modifiche alla replica

La sincronizzazione delle modifiche delle repliche di Amazon S3 può aiutarti a mantenere i metadati degli oggetti come tag, elenchi di controllo degli accessi (ACL), annotazioni e impostazioni di Object Lock replicati tra repliche e oggetti di origine. Per impostazione predefinita, Amazon S3 replica i metadati dagli oggetti di origine solo alle repliche. Quando la sincronizzazione delle modifiche alla replica è abilitata, Amazon S3 replica le modifiche dei metadati apportate alle copie di replica nell'oggetto di origine, rendendo la replica bidirezionale.

Abilitazione della sincronizzazione delle modifiche alla replica

Puoi utilizzare la sincronizzazione delle modifiche alla replica Amazon S3 con regole di replica nuove o esistenti. È possibile applicarla a un intero bucket o agli oggetti che hanno un prefisso specifico.

Per abilitare la sincronizzazione delle modifiche alla replica mediante la console Amazon S3, consulta [Esempi di configurazione della replica in tempo reale](#). Questo argomento fornisce istruzioni per abilitare la sincronizzazione delle modifiche delle repliche nella configurazione di replica quando i bucket di origine e destinazione sono di proprietà uguali o diversi. Account AWS

Per abilitare la sincronizzazione delle modifiche delle repliche utilizzando AWS Command Line Interface (AWS CLI), è necessario aggiungere una configurazione di replica al bucket contenente le repliche con abilitazione. ReplicaModifications Per impostare la replica bidirezionale, creare una regola di replica dal bucket di origine (*amzn-s3-demo-source-bucket*) al bucket contenente le repliche (*amzn-s3-demo-destination-bucket*). Quindi, creare una seconda regola di replica dal bucket contenente le repliche (*amzn-s3-demo-destination-bucket*) al bucket di origine (*amzn-s3-demo-source-bucket*). I bucket di origine e di destinazione possono essere uguali o diversi. Regioni AWS

Note

È necessario abilitare la sincronizzazione delle modifiche delle repliche sia sul bucket di origine che su quello di destinazione per replicare le modifiche ai metadati della replica come gli elenchi di controllo di accesso agli oggetti (ACL), i tag degli oggetti, le annotazioni degli oggetti o le impostazioni di blocco degli oggetti replicati. Analogamente a tutte le regole di replica, è possibile applicare queste regole all'intero bucket o a un sottoinsieme di oggetti filtrati per prefisso o tag di oggetto.

Nella seguente configurazione di esempio, Amazon S3 replica le modifiche dei metadati sotto il prefisso *Tax* al bucket *amzn-s3-demo-source-bucket*, che contiene gli oggetti di origine.

```
{
  "Rules": [
    {
      "Status": "Enabled",
      "Filter": {
        "Prefix": "Tax"
      },
      "SourceSelectionCriteria": {
```

```
        "ReplicaModifications":{
            "Status": "Enabled"
        },
        "Destination": {
            "Bucket": "arn:aws:s3:::amzn-s3-demo-source-bucket"
        },
        "Priority": 1
    },
    "Role": "IAM-Role-ARN"
}
```

Per istruzioni complete sulla creazione di regole di replica utilizzando il, vedere. AWS CLI [Configurazione della replica per i bucket nello stesso account](#)

Replica dei contrassegni di eliminazione tra i bucket

Per impostazione predefinita, quando la replica S3 è abilitata e un oggetto viene eliminato nel bucket di origine, Amazon S3 aggiunge un contrassegno di eliminazione solo nel bucket di origine. Questa operazione consente di proteggere i dati nei bucket di destinazione da eliminazioni accidentali o dolose. Se è stata abilitata la replica dei contrassegni di eliminazione, questi contrassegni vengono copiati nei bucket di destinazione e Amazon S3 si comporterà come se l'oggetto fosse stato eliminato nei bucket di origine e di destinazione. Per ulteriori informazioni sul funzionamento dei contrassegni di eliminazione, consulta [Utilizzo dei contrassegni di eliminazione](#).

Note

- La replica dei contrassegni di eliminazione non è supportata per le regole di replica basate su tag. La replica dei contrassegni di eliminazione non rispetta l'Accordo sul livello di servizio (SLA) di 15 minuti concesso quando si utilizza il controllo del tempo di replica di S3 (S3 RTC).
- Se non si utilizza la versione XML più recente della configurazione della replica, le operazioni di eliminazione influiscono sulla replica in modo diverso. Per ulteriori informazioni, consulta [Effetto delle operazioni di eliminazione sulla replica](#).
- Se si abilita la replica dei contrassegni di eliminazione e il bucket di origine ha una regola di scadenza del ciclo di vita S3, i contrassegni di eliminazione aggiunti dalla regola di scadenza del ciclo di vita S3 non verranno replicati nel bucket di destinazione.

Abilitazione della replica dei contrassegni di eliminazione

Puoi iniziare a utilizzare la replica dei contrassegni di eliminazione con una regola di replica nuova o esistente. È possibile applicare la replica dei contrassegni di eliminazione a un intero bucket o agli oggetti che hanno un prefisso specifico.

Per abilitare la replica dei contrassegni di eliminazione utilizzando la console Amazon S3, consulta [Utilizzo della console S3](#). Questo argomento fornisce istruzioni per abilitare la replica degli indicatori di eliminazione nella configurazione di replica quando i bucket di origine e destinazione sono di proprietà uguale o diversa. Account AWS

Per abilitare la replica dei marker di eliminazione utilizzando AWS Command Line Interface (AWS CLI), è necessario aggiungere una configurazione di replica al bucket di origine con `DeleteMarkerReplication` abilitato, come mostrato nella seguente configurazione di esempio.

Nella seguente configurazione della replica di esempio, i contrassegni di eliminazione vengono replicati nel bucket di destinazione *amzn-s3-demo-destination-bucket* per gli oggetti sotto il prefisso *Tax*.

```
{
  "Rules": [
    {
      "Status": "Enabled",
      "Filter": {
        "Prefix": "Tax"
      },
      "DeleteMarkerReplication": {
        "Status": "Enabled"
      },
      "Destination": {
        "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      },
      "Priority": 1
    }
  ],
  "Role": "IAM-RoLe-ARN"
}
```

Per istruzioni complete sulla creazione di regole di replica tramite, vedere. AWS CLI [Configurazione della replica per i bucket nello stesso account](#)

Replica delle annotazioni

Quando configuri la replica su un bucket, Amazon S3 replica automaticamente le annotazioni come parte della replica live. Ogni annotazione viene replicata indipendentemente man mano che si verificano modifiche. Per replicare le annotazioni, il ruolo IAM di replica deve includere l'`s3:GetObjectVersionAnnotationForReplication` autorizzazione nel bucket di origine.

L'esempio seguente mostra l'istruzione del bucket di origine nella policy delle autorizzazioni del ruolo IAM con l'autorizzazione di replica delle annotazioni inclusa:

```
{
  "Effect": "Allow",
  "Action": [
    "s3:GetObjectVersionForReplication",
    "s3:GetObjectVersionAcl",
    "s3:GetObjectVersionTagging",
    "s3:GetObjectVersionAnnotationForReplication"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
  ]
}
```

Non sono richieste autorizzazioni aggiuntive per il bucket di destinazione per la replica delle annotazioni. L'`s3:ReplicateObject` autorizzazione sul bucket di destinazione copre la replica delle annotazioni.

Nota i seguenti comportamenti per la replica delle annotazioni:

- Le aggiunte e gli aggiornamenti delle annotazioni sull'origine vengono replicati nella destinazione. Ogni annotazione viene replicata indipendentemente man mano che si verificano modifiche.
- Le cancellazioni delle annotazioni sull'origine non vengono replicate nella destinazione. Se si elimina un'annotazione sull'origine, l'annotazione persiste nella destinazione.
- Se si eliminano e si ricreano ripetutamente annotazioni sull'origine con nomi diversi, le annotazioni si accumulano nella destinazione nel tempo perché le eliminazioni non vengono replicate.

Se non desideri che le annotazioni vengano replicate in un bucket di destinazione, il proprietario del bucket di destinazione può aggiungere un'istruzione Deny per l'azione alla policy del bucket di destinazione. `s3:ReplicateObjectAnnotation` La replica degli oggetti continua ad avere

successo; viene bloccata solo la replica delle annotazioni. L'esempio seguente mostra l'istruzione Deny:

```
...
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::source-bucket-account-id:role/service-role/source-account-IAM-role"
      },
      "Action": "s3:ReplicateObjectAnnotation",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
...
```

Per ulteriori informazioni sul comportamento di replica delle annotazioni, vedere [the section called “Cosa viene replicato?”](#) Per istruzioni sulla configurazione delle autorizzazioni, vedere [Configurazione delle autorizzazioni per la replica in tempo reale](#)

Gestione o sospensione della replica in tempo reale

La replica in tempo reale è la copia automatica e asincrona di oggetti tra bucket uguali o diversi. Regioni AWS Dopo aver impostato la configurazione della replica, Amazon S3 replica gli oggetti nuovi e gli aggiornamenti degli oggetti da un bucket di origine a uno o più bucket di destinazione specifici.

Per aggiungere regole di replica al bucket di origine, viene utilizzata la console di Amazon S3. Le regole di replica definiscono gli oggetti del bucket di origine da replicare e i bucket o i bucket di destinazione in cui vengono archiviati gli oggetti replicati. Per ulteriori informazioni sulla replica, consulta [Replica di oggetti all'interno e tra le Regioni](#).

È possibile gestire le regole di replica nella pagina Replica nella console Amazon S3. È possibile aggiungere, visualizzare, modificare, abilitare, disabilitare o eliminare le regole di replica. Inoltre, è possibile modificare la priorità delle regole di replica. Per informazioni sull'aggiunta di regole di replica a un bucket, consulta [Utilizzo della console S3](#).

Per gestire le regole di replica per un bucket utilizzando la console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nella scheda Bucket per uso generico scegli il nome del bucket desiderato.
4. Seleziona la scheda Gestione, quindi scorri verso il basso fino a Regole di replica.
5. È possibile modificare le regole di replica come indicato di seguito:
 - Per abilitare o disabilitare una regola di replica, scegli il pulsante di opzione a sinistra della regola. Dal menu Azioni scegli Abilita regola o Disabilita regola. È anche possibile disabilitare, abilitare o eliminare tutte le regole nel bucket dal menu Operazioni.

 Note

Se si disabilita, e successivamente si riabilita, una regola di replica, tutti gli oggetti nuovi o modificati che non sono stati replicati mentre la regola era disabilitata non vengono replicati automaticamente quando la regola viene riabilitata. Per replicare questi oggetti, è necessario utilizzare Replica in batch S3. Per ulteriori informazioni, consulta [the section called “Replica di oggetti esistenti”](#).

- Per modificare la priorità di una regola, scegli il pulsante di opzione a sinistra della regola, quindi scegli Modifica regola.

È necessario impostare le priorità delle regole per evitare i conflitti causati dagli oggetti inclusi nell'ambito di più regole. In caso di regole sovrapposte, Amazon S3 utilizza la priorità delle regole per determinare quale regola applicare. Più elevato è il numero, maggiore è la priorità. Per ulteriori informazioni sulla priorità delle regole, consulta [Elementi del file di configurazione della replica](#).

Sospensione o interruzione della replica

Per sospendere temporaneamente la replica e farla riprendere automaticamente in un secondo momento, è possibile utilizzare l'operazione `aws:s3:bucket-pause-replication` in AWS Fault Injection Service. Per ulteriori informazioni, consulta [aws:s3:bucket-pause-replication](#) e [Sospensione della replica S3](#) nella Guida per l'utente di AWS Fault Injection Service .

Per interrompere la replica in Amazon S3, è consigliabile disabilitare le regole di replica. Se si disabilita, e successivamente si riabilita, una regola di replica, tutti gli oggetti nuovi o modificati che non sono stati replicati mentre la regola era disabilitata non vengono replicati automaticamente quando la regola viene riabilitata. Per replicare questi oggetti, è necessario utilizzare Replica in batch S3. Per ulteriori informazioni, consulta [the section called “Replica di oggetti esistenti”](#).

La replica si interromperà anche se rimuovi il ruolo AWS Identity and Access Management (IAM), le autorizzazioni AWS Key Management Service (AWS KMS) o le autorizzazioni della policy del bucket che concedono ad Amazon S3 le autorizzazioni richieste. Tuttavia, è consigliabile non utilizzare questi approcci perché impediscono la replica. Amazon S3 segnala lo stato di replica per gli oggetti interessati come FAILED. Se le autorizzazioni vengono successivamente ripristinate, gli oggetti contrassegnati come FAILED non vengono replicati automaticamente. Per replicare questi oggetti, è necessario utilizzare Replica in batch S3.

Replica di oggetti esistenti con Replica in batch

Replica in batch S3 differisce dalla replica in tempo reale, che replica in modo continuo e automatico nuovi oggetti tra bucket Amazon S3. Invece, Replica in batch S3 viene utilizzato on demand su oggetti esistenti. È possibile utilizzare Replica in batch S3 per replicare i tipi di oggetti seguenti:

- Oggetti esistenti prima dell'applicazione di una configurazione della replica
- Oggetti che sono stati replicati in precedenza
- Oggetti la cui replica non è riuscita

È possibile replicare questi oggetti on demand utilizzando un processo Operazioni in batch.

Per iniziare a utilizzare Replica in batch occorre:

- Avviare Replica in batch per una nuova regola o destinazione di replica: è possibile creare un processo Replica in batch una tantum al momento della creazione della prima regola in una nuova configurazione della replica o dell'aggiunta di un nuovo bucket di destinazione a una configurazione esistente tramite la console Amazon S3.
- Avvia la replica in batch per una configurazione di replica esistente: puoi creare un nuovo processo di replica in batch utilizzando S3 Batch Operations tramite la console Amazon S3, AWS Command Line Interface (AWS CLI), gli SDK o l'API REST di Amazon S3. AWS

Al termine del processo Batch Replication, viene visualizzato un report di completamento. Per ulteriori informazioni su come utilizzare questo report per esaminare il processo, consulta [Monitoraggio dei rapporti sullo stato e sul completamento dei processi](#).

Considerazioni su S3 Batch Replication

Prima di utilizzare Replica in batch S3, esaminare il seguente elenco di considerazioni:

- Il bucket di origine deve avere una configurazione di replica esistente. Per abilitare la replica, consulta le sezioni [Panoramica della configurazione della replica in tempo reale](#) e [Esempi di configurazione della replica in tempo reale](#).
- Se si è configurato Ciclo di vita S3 per il bucket, è consigliabile disabilitare le regole del ciclo di vita mentre il processo Replica in batch è attivo. Ciò garantisce la parità tra il bucket di origine e quello di destinazione. Altrimenti, questi bucket potrebbero divergere e il bucket di destinazione non sarà una replica esatta del bucket di origine. Si consideri ad esempio lo scenario riportato di seguito:
 - Il bucket di origine ha più versioni di un oggetto e un contrassegno di eliminazione su tale oggetto.
 - I bucket di origine e destinazione dispongono di una configurazione del ciclo di vita per rimuovere i contrassegni di eliminazione scaduti.

In questo scenario, Replica in batch può replicare il contrassegno di eliminazione nel bucket di destinazione prima di replicare le versioni dell'oggetto. Questo comportamento può far sì che la configurazione del ciclo di vita indichi il contrassegno di eliminazione come scaduto e che il contrassegno di eliminazione venga rimosso dal bucket di destinazione prima della replica delle versioni dell'oggetto.

- Il ruolo AWS Identity and Access Management (IAM) specificato per eseguire il job Batch Operations deve disporre delle autorizzazioni necessarie per eseguire l'operazione di replica batch sottostante. Per ulteriori informazioni sulla creazione dei ruoli IAM, consulta la sezione [Configurazione di un ruolo IAM per Replica in batch S3](#).
- Replica in batch richiede un manifesto che può essere generato da Amazon S3. Il manifest generato deve essere archiviato nello stesso bucket Regione AWS di origine. Se si sceglie di non generare il manifesto, è possibile fornire un report di inventario Amazon S3 o un file CSV contenente gli oggetti che si desidera replicare. Per ulteriori informazioni, consulta [the section called "Specifica di un manifesto per un processo Batch Replication"](#).
- Se hai aggiunto o aggiornato di recente la configurazione di replica nel bucket di origine, aspettati un ritardo di alcuni minuti prima che la modifica sia completamente propagata. È consigliabile attendere prima di creare un processo di replica in batch con un manifesto. S3-generated

- Replica in batch non supporta la ripetizione della replica di oggetti eliminati con l'ID versione dell'oggetto dal bucket di destinazione. Per replicare nuovamente questi oggetti è possibile copiare gli oggetti di origine presenti con un processo di copia in batch. La copia di tali oggetti crea nuove versioni degli oggetti nel bucket di origine e avvia automaticamente la replica nel bucket di destinazione. L'eliminazione e la nuova creazione del bucket di destinazione non avviano la replica.

Per ulteriori informazioni su Copia in batch, consulta [Esempi che utilizzano operazioni in batch per copiare oggetti](#).

- Se si sta utilizzando una regola di replica sul bucket di origine, assicurarsi di [aggiornare la configurazione della replica](#), concedendo al ruolo IAM associato alla regola di replica le autorizzazioni adeguate per replicare gli oggetti. Il ruolo IAM deve disporre delle autorizzazioni necessarie per eseguire la replica sia sul bucket di origine che su quello di destinazione.
- Se si inviano più processi Replica in batch per lo stesso bucket in un breve intervallo di tempo, Amazon S3 eseguirà tali processi contemporaneamente.
- Se si inviano più processi Replica in batch per due bucket diversi, tenere presente che Amazon S3 potrebbe non eseguire tutti i processi contemporaneamente. Se si supera il numero di processi Replica in batch che possono essere eseguiti contemporaneamente sul proprio account, Amazon S3 metterà in pausa i processi con priorità più bassa per gestire quelli con priorità più alta. Una volta completati i processi con priorità più alta, tutti i processi in pausa tornano attivi.
- Replica in batch non è supportato per gli oggetti archiviati nelle classi di storage Recupero flessibile Amazon S3 Glacier e S3 Glacier Deep Archive.
- Per replicare in batch Intelligent-Tiering gli oggetti S3 archiviati nei livelli di storage Archive Access o Deep Archive Access, è necessario innanzitutto avviare una [richiesta di](#) ripristino e attendere che gli oggetti vengano spostati nel livello Frequent Access.
- Un singolo processo di replica in batch può supportare un manifesto con un massimo di 20 miliardi di oggetti.
- Se utilizzi S3 Batch Replication per replicare set di dati su più regioni e in precedenza il tipo di crittografia sul lato server degli oggetti era aggiornato da a, potresti aver bisogno di autorizzazioni aggiuntive. SSE-S3 SSE-KMS Nel bucket della regione di origine, è necessario disporre delle autorizzazioni. kms:decrypt Quindi, avrai bisogno delle kms:encrypt autorizzazioni kms:decrypt e per il bucket nella regione di destinazione. Per ulteriori informazioni, consulta [Replica di oggetti crittografati](#).
- Se gli oggetti nel bucket di origine dispongono di annotazioni, queste vengono replicate indipendentemente insieme all'oggetto durante la replica in batch. Non sono previste attività

lavorative separate per le singole annotazioni. Lo stato del job task dipende sia dallo stato di replica dell'oggetto principale che dallo stato di replica dell'annotazione.

Specifica di un manifesto per un processo Batch Replication

Un manifesto è un oggetto Amazon S3 che contiene le chiavi dell'oggetto su cui si desidera che Amazon S3 agisca. Se si desidera creare un processo Replica in batch, occorre fornire un manifesto generato dall'utente o fare in modo che Amazon S3 generi un manifesto basato sulla configurazione della replica.

Se si fornisce un manifesto generato dall'utente, deve essere sotto forma di report di inventario Amazon S3 o di file CSV. Se gli oggetti nel manifesto sono in un bucket con versione, è necessario specificare gli ID versione per gli oggetti. Verrà replicato solo l'oggetto con l'ID versione specificato nel manifesto. Per ulteriori informazioni sulla specifica di un manifesto, consulta la sezione [Specifica di un manifest](#).

Se Amazon S3 deve generare automaticamente un file manifesto per conto dell'utente, gli oggetti elencati utilizzano lo stesso bucket, prefisso e tag di origine di tutte le configurazioni di replica del bucket di origine. Con un manifesto generato, Amazon S3 replica tutte le versioni idonee degli oggetti.

Note

Se scegli di fare in modo che Amazon S3 generi il manifest, il manifest deve essere archiviato nello stesso Regione AWS bucket di origine.

Filtri per i processi Batch Replication

Quando si crea un processo Replica in batch, è possibile specificare dei filtri aggiuntivi, ad esempio la data di creazione dell'oggetto e lo stato della replica, al fine di ridurre l'ambito del processo.

Puoi filtrare gli oggetti da replicare in base al valore `ObjectReplicationStatuses` fornendo uno o più dei seguenti valori:

- "NONE": indica che Amazon S3 non ha mai tentato di replicare l'oggetto in precedenza.
- "FAILED": indica che Amazon S3 ha tentato di replicare l'oggetto in precedenza ma la replica non è andata a buon fine.

- "COMPLETED": indica che Amazon S3 ha replicato correttamente l'oggetto in precedenza.
- "REPLICA": indica che questo oggetto è una replica eseguita da Amazon S3 da un altro bucket di origine.

Per ulteriori informazioni sugli stati di replica, consulta la sezione [Ottenimento delle informazioni sullo stato della replica](#).

Se non si filtra il processo Replica in batch, Operazioni in batch tenta di replicare tutti gli oggetti (indipendentemente dal relativo valore `ObjectReplicationStatus`) nel file manifesto che corrispondono alle regole di configurazione della replica, ad eccezione di alcuni oggetti che non vengono replicati per impostazione predefinita. Per ulteriori informazioni, consulta [the section called "Che cosa non viene replicato con le configurazioni di replica?"](#)

A seconda del proprio obiettivo, è possibile impostare `ObjectReplicationStatuses` su uno dei seguenti valori:

- Per replicare solo gli oggetti esistenti che non sono mai stati replicati, includere solo "NONE".
- Per ritentare la replica dei soli oggetti la cui replica precedente non è andata a buon fine, includere solo "FAILED".
- Per replicare gli oggetti esistenti e ritentare la replica degli oggetti la cui replica precedente non è andata a buon fine, includere sia "NONE" sia "FAILED".
- Per riempire un bucket di destinazione con gli oggetti replicati in un'altra destinazione, includere "COMPLETED".
- Per replicare gli oggetti replicati in precedenza, includere "REPLICA".

Report di completamento della replica in batch

Quando crei un processo di Batch Replication, puoi richiedere un report di completamento in formato CVS. Questo report mostra gli oggetti, i codici di esito positivo o negativo della replica, gli output e le descrizioni. Per ulteriori informazioni sul monitoraggio dei processi e sui report di completamento, consulta [Rapporti di completamento](#).

Per l'elenco dei codici di esito negativo della replica con le descrizioni, consulta [Motivi degli errori di replica Amazon S3](#).

Per informazioni sulla risoluzione dei problemi di Replica in batch, consulta [Errori di replica in batch](#).

Guida introduttiva alla replica in batch

Per ulteriori informazioni su come utilizzare Batch Replication, consulta e. [Creazione di un processo Replica in batch per nuove destinazioni o regole di replica](#) [Creazione di un processo Batch Replication per le regole di replica esistenti](#)

Configurazione di un ruolo IAM per Replica in batch S3

Poiché Replica in batch Amazon S3 è un tipo di processo Operazioni in batch, è necessario creare un ruolo AWS Identity and Access Management (IAM) per concedere le autorizzazioni Operazioni in batch per eseguire operazioni per conto dell'utente. Inoltre, devi collegare una policy IAM di Batch Replication al ruolo IAM di Batch Operations.

Utilizzare le procedure seguenti per creare una policy e un ruolo IAM che fornisce a Operazioni in batch l'autorizzazione per avviare un processo Replica in batch.

Per creare una policy per Replica in batch

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>
2. In Gestione accessi scegli Policy.
3. Seleziona Create Policy (Crea policy).
4. Nella pagina Specifica autorizzazioni, seleziona JSON.
5. Inserire una delle seguenti policy, a seconda che il manifesto sia stato generato da Amazon S3 o fornito dall'utente. Per ulteriori informazioni sui manifest, consulta [Specifica di un manifesto per un processo Batch Replication](#).

Prima di utilizzare queste policy, sostituire *user input placeholders* nelle policy seguenti con i nomi del bucket di origine della replica, del bucket del manifesto e del bucket dei report di completamento.

Note

Il ruolo IAM dell'utente per Replica in batch richiede autorizzazioni diverse, a seconda che l'utente generi o fornisca un manifesto, pertanto è necessario assicurarsi di scegliere la policy appropriata tra i seguenti esempi.

Policy da impiegare se si utilizza e si archivia un manifesto generato da Amazon S3

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:InitiateReplication"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
      ]
    },
    {
      "Action": [
        "s3:GetReplicationConfiguration",
        "s3:PutInventoryConfiguration"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket"
      ]
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
```

```

    ]
  }
]
}

```

Policy da impiegare se si utilizza un manifesto fornito dall'utente

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:InitiateReplication"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
      ]
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}

```

```
}
```

6. Scegli Avanti.
7. Specifica un nome per la policy e scegli Crea policy.

Per creare un ruolo IAM per Replica in batch

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. In Access management (Gestione accessi), scegli Roles (Ruoli).
3. Scegliere Crea ruolo.
4. Scegli Servizio AWS come tipo di entità attendibile. Nella sezione Casi d'uso scegli S3 come servizio e Operazioni in batch S3 come caso d'uso.
5. Scegli Avanti. Viene visualizzata la pagina Aggiungi autorizzazioni. Nella casella di ricerca, immettere la policy creata nella procedura precedente. Seleziona la casella di controllo accanto al nome della policy, quindi scegli Successivo.
6. Nella pagina Nomina, verifica e crea specificare un nome per il ruolo IAM.
7. Nella sezione Passaggio 1: Attribuire attendibilità alle identità, verificare che il proprio ruolo IAM utilizzi la seguente policy di fiducia:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "batchoperations.s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

8. Nella sezione Passaggio 2: Aggiungere autorizzazioni, verificare che il proprio ruolo IAM utilizzi la policy creata in precedenza.

9. Scegliere Crea ruolo.

Creazione di un processo Replica in batch per nuove destinazioni o regole di replica

In Amazon S3, la replica in tempo reale non replica alcun oggetto già esistente nel bucket di origine prima della creazione di una configurazione della replica. La replica in tempo reale replica automaticamente solo gli oggetti nuovi e aggiornati che vengono scritti nel bucket dopo la creazione della configurazione della replica. Per replicare oggetti già esistenti, è possibile utilizzare Replica in batch S3 per replicare questi oggetti on demand.

Quando si crea la prima regola in una nuova configurazione della replica in tempo reale o quando si aggiunge un nuovo bucket di destinazione a una configurazione della replica esistente tramite la console Amazon S3, è possibile creare un processo Replica in batch. Questo processo Replica in batch può essere utilizzato per replicare nel bucket di destinazione gli oggetti esistenti nel bucket di origine.

Per utilizzare Replica in batch per una configurazione esistente senza aggiungere un nuovo bucket di destinazione, consulta [Creazione di un processo Batch Replication per le regole di replica esistenti](#).

Prerequisiti

Prima di creare un processo Replica in batch, è necessario creare un ruolo AWS Identity and Access Management (IAM) per Operazioni in batch al fine di concedere ad Amazon S3 le autorizzazioni per eseguire operazioni per conto dell'utente. Per ulteriori informazioni, consulta [Configurazione di un ruolo IAM per Replica in batch S3](#).

Utilizzo di Replica in batch per una nuova regola di replica o una nuova destinazione tramite la console Amazon S3

Quando si crea la prima regola in una nuova configurazione della replica o quando si aggiunge un nuovo bucket di destinazione a una configurazione esistente tramite la console Amazon S3, si ha la possibilità di creare un processo Replica in batch per replicare oggetti esistenti nel bucket di origine.

Per creare un processo Replica in batch durante la creazione o l'aggiornamento di una configurazione della replica

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).

3. Scegli dall'elenco Bucket per uso generico il nome del bucket che contiene gli oggetti da replicare.
4. Per creare una nuova regola di replica o modificare una regola esistente, scegli la scheda Gestione e scorri verso il basso fino a Regole di replica:
 - Per creare una nuova regola di replica, scegliere Create replication rule (Crea regola di replica). Per esempi su come configurare una regola di replica di base, consulta [Esempi di configurazione della replica in tempo reale](#).
 - Per modificare una regola di replica esistente, seleziona il pulsante di opzione vicino alla regola, quindi scegli Modifica regola.
5. Creare la nuova regola di replica o modificare la destinazione per la regola di replica esistente e scegliere Save (Salva).

Dopo aver creato la prima regola in una nuova configurazione di replica o dopo aver modificato una configurazione esistente per aggiungere una nuova destinazione, viene visualizzata una finestra di dialogo Replicate existing objects? (Replicare gli oggetti esistenti?) che offre la possibilità di creare un processo Batch Replication.

6. Se desideri creare ed eseguire questo processo ora, scegli Sì, replica gli oggetti esistenti.

Se desideri creare un processo Replica in batch in un secondo momento, scegli No, non replicare oggetti esistenti.

7. Se si sceglie Sì, replica oggetti esistenti, viene visualizzata la pagina Crea processo di operazioni in batch. Il processo Replica in batch S3 ha le impostazioni seguenti:

Opzioni di esecuzione del processo

Se desideri che il processo Replica in batch S3 venga eseguito immediatamente, scegli Esegui automaticamente il processo quando è pronto. Se desideri eseguire il processo in un secondo momento, seleziona Attendi l'esecuzione del processo quando è pronto.

Note

Se si sceglie Esegui automaticamente il processo quando è pronto, non sarà possibile creare e salvare un manifesto Operazioni in batch. Per salvare il manifesto Operazioni in batch, scegli Attendi l'esecuzione del processo quando è pronto.

Manifesto Batch Operations

Se si sceglie Attendi l'esecuzione del processo quando è pronto, viene visualizzata la sezione Manifesto Operazioni in batch. Il manifesto è un elenco di tutti gli oggetti sui quali desideri eseguire l'operazione specificata. È possibile scegliere di salvare il manifesto. Analogamente ai file di inventario S3, il manifesto viene salvato come file CSV e archiviato in un bucket.

Per ulteriori informazioni sui manifesti Batch Operations, consulta la sezione [Specifica di un manifest](#).

Report di completamento

Operazioni in batch S3 esegue un'unica attività per ciascun oggetto specificato nel manifesto. I report di completamento offrono un modo semplice per visualizzare i risultati delle attività in un formato consolidato, senza ulteriori operazioni di configurazione. Puoi richiedere un report di completamento per tutte le attività o solo per le attività fallite. Per ulteriori informazioni sui report di completamento, consulta la sezione [Rapporti di completamento](#).

Permissions

Una delle cause più comuni di errori di replica sono le autorizzazioni insufficienti nel ruolo fornito AWS Identity and Access Management (IAM). Per ulteriori informazioni sulla creazione di questo ruolo, consulta [Configurazione di un ruolo IAM per Replica in batch S3](#). Assicurati di creare o scegliere un ruolo IAM con le autorizzazioni richieste per Replica in batch.

8. Selezionare Salva.

Creazione di un processo Batch Replication per le regole di replica esistenti

In Amazon S3, la replica in tempo reale non replica alcun oggetto già esistente nel bucket di origine prima della creazione di una configurazione della replica. La replica in tempo reale replica automaticamente solo gli oggetti nuovi e aggiornati che vengono scritti nel bucket dopo la creazione della configurazione della replica. Per replicare oggetti già esistenti, è possibile utilizzare Replica in batch S3 per replicare questi oggetti on demand.

Puoi configurare S3 Batch Replication per una configurazione di replica esistente utilizzando gli AWS SDK, AWS Command Line Interface (AWS CLI) o la console Amazon S3. Per una panoramica di Replica in batch, consulta [Replica di oggetti esistenti con Replica in batch](#).

Al termine del processo Batch Replication, viene visualizzato un report di completamento. Per ulteriori informazioni su come utilizzare il report per esaminare il processo, consulta la sezione [Monitoraggio dei rapporti sullo stato e sul completamento dei processi](#).

Prerequisiti

Prima di creare un processo Replica in batch, è necessario creare un ruolo AWS Identity and Access Management (IAM) per Operazioni in batch al fine di concedere ad Amazon S3 le autorizzazioni per eseguire operazioni per conto dell'utente. Per ulteriori informazioni, consulta [Configurazione di un ruolo IAM per Replica in batch S3](#).

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Operazioni in batch.
3. Scegli Crea processo.
4. Verificare che la sezione Regione AWS mostri la Regione in cui si desidera creare il processo.
5. Nella sezione Manifesto specificare il formato del manifesto che si desidera utilizzare. Il manifesto è un elenco di tutti gli oggetti sui quali desideri eseguire l'operazione specificata. Per ulteriori informazioni sui manifesti Batch Operations, consulta la sezione [Specifica di un manifest](#).
 - Se hai preparato un manifesto, scegli S3 inventory report (manifest.json) (Report di inventario S3 (manifest.json)) o CSV. Se il manifesto è in un bucket con versione, è possibile specificare l'ID versione per il manifesto. Se non si specifica un ID versione, Operazioni in batch utilizza la versione corrente del manifesto. Per ulteriori informazioni sulla creazione di un manifesto, consulta [Specifica di un manifest](#).

Note

Se gli oggetti nel manifesto sono in un bucket con versione, è necessario specificare gli ID versione per gli oggetti. Per ulteriori informazioni, consulta [Specifica di un manifest](#).

- Per creare un manifesto basato sulla configurazione di replica, scegli Create manifest using S3 Replication configuration (Crea manifesto utilizzando la configurazione di replica S3). Quindi, scegli il bucket di origine della configurazione della replica.

6. (Facoltativo) Se si sceglie Crea manifesto utilizzando la configurazione di Replica S3, è possibile includere filtri aggiuntivi, come la data di creazione dell'oggetto e lo stato della replica. Per esempi su come filtrare in base allo stato della replica, consulta [Specifica di un manifesto per un processo Batch Replication](#).
7. (Facoltativo) Se si è scelto Crea manifesto utilizzando la configurazione di Replica S3, è possibile salvare il manifesto generato. Per salvare questo manifesto, seleziona Manifesto delle operazioni in batch di salvataggio. Specifica quindi il bucket di destinazione per il manifesto e scegli se crittografare il manifesto.

 Note

Il manifest generato deve essere archiviato nello Regione AWS stesso bucket di origine.

8. Scegli Avanti.
9. Nella pagina Operazioni scegli Replica, quindi scegli Successivo.
10. (Facoltativo) Fornisci un valore per Description (Descrizione).
11. Modifica il valore Priority (Priorità) del processo, se necessario. Numeri maggiori indicano una priorità superiore. Amazon S3 tenta di eseguire i processi con priorità più elevata prima dei processi con priorità inferiore. Per ulteriori informazioni sulla priorità dei processi, consulta [Assegnazione della priorità dei processi](#).
12. (Facoltativo) Genera un report di completamento. Per generarlo, seleziona Genera report di completamento.

Se scegli di generare un report di completamento, devi scegliere se riferire Failed tasks only (Solo attività fallite) o All tasks (Tutte le attività) e fornire un bucket di destinazione per il report.
13. Nella sezione Autorizzazioni, assicurati di scegliere un ruolo IAM con le autorizzazioni richieste per Replica in batch. Una delle cause più comuni degli errori di replica è rappresentata dalla mancanza di autorizzazioni sufficienti nel ruolo IAM fornito. Per ulteriori informazioni sulla creazione di questo ruolo, consulta [Configurazione di un ruolo IAM per Replica in batch S3](#).
14. (Facoltativo) Aggiungi tag di processo al processo Batch Replication.
15. Scegli Avanti.
16. Rivedi la configurazione del processo e scegli Crea processo.

Utilizzo di AWS CLI con un manifesto S3

Il seguente comando di esempio `create-job` crea un processo Replica in batch S3 tramite un manifesto generato da S3 per l' Account AWS **111122223333**. Questo esempio replica oggetti esistenti e oggetti la cui replica in precedenza non è andata a buon fine. Per informazioni sul filtro in base allo stato della replica, consulta [Specifica di un manifesto per un processo Batch Replication](#).

Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate. Sostituire il ruolo IAM `role/batch-Replication-IAM-policy` con il ruolo IAM creato in precedenza. Per ulteriori informazioni, consulta [Configurazione di un ruolo IAM per Replica in batch S3](#).

```
aws s3control create-job --account-id 111122223333 \
--operation '{"S3ReplicateObject:{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest-generator '{"S3JobManifestGenerator": {"ExpectedBucketOwner":\
"111122223333", \
"SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket", \
"EnableManifestOutput": false, "Filter": {"EligibleForReplication": true, \
"ObjectReplicationStatuses": ["NONE","FAILED"]}}}' \
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
--no-confirmation-required \
--region source-bucket-region
```

Note

È necessario avviare il processo dallo stesso bucket Regione AWS di origine della replica.

Dopo aver avviato correttamente un processo Batch Replication, viene visualizzato l'ID del processo come risposta. Il processo può essere monitorato utilizzando il seguente comando `describe-job`. Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

Utilizzo di AWS CLI con un manifesto fornito dall'utente

Nell'esempio seguente viene creato un processo Replica in batch S3 tramite un manifesto definito dall'utente per l' Account AWS **111122223333**. Se gli oggetti nel manifesto sono in un bucket con versione, è necessario specificare gli ID versione per gli oggetti. Verrà replicato solo l'oggetto con l'ID versione specificato nel manifesto. Per ulteriori informazioni sulla creazione di un manifesto, consulta [Specifica di un manifest](#).

Per utilizzare questo comando, sostituisci *user input placeholders* con le informazioni appropriate. Sostituire il ruolo IAM `role/batch-Replication-IAM-policy` con il ruolo IAM creato in precedenza. Per ulteriori informazioni, consulta [Configurazione di un ruolo IAM per Replica in batch S3](#).

```
aws s3control create-job --account-id 111122223333 \  
--operation '{"S3ReplicateObject":{}}' \  
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\  
"Prefix":"batch-replication-report",\  
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \  
--manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820",\  
"Fields":["Bucket","Key","VersionId"]},\  
"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest.csv",\  
"ETag":"Manifest Etag"}}' \  
--priority 1 \  
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \  
--no-confirmation-required \  
--region source-bucket-region
```

Note

È necessario avviare il processo dallo stesso bucket Regione AWS di origine della replica.

Dopo aver avviato correttamente un processo Batch Replication, viene visualizzato l'ID del processo come risposta. Il processo può essere monitorato utilizzando il seguente comando `describe-job`.

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

Risoluzione dei problemi nella replica

Questa sezione riporta i suggerimenti per la risoluzione dei problemi di Replica Amazon S3 e informazioni sugli errori di replica in batch di Amazon S3.

Argomenti

- [Suggerimenti per la risoluzione dei problemi di Replica Amazon S3](#)
- [Errori di replica in batch](#)

Suggerimenti per la risoluzione dei problemi di Replica Amazon S3

Se le repliche degli oggetti non vengono visualizzate nel bucket di destinazione dopo aver configurato la replica, usa questi suggerimenti per identificare e correggere i problemi.

- La replica della maggior parte degli oggetti viene eseguita entro 15 minuti. Il tempo impiegato da Amazon S3 per replicare un oggetto dipende da diversi fattori, tra cui la combinazione di regione di origine/regione di destinazione e le dimensioni dell'oggetto. La replica di oggetti di grandi dimensioni può richiedere anche diverse ore. Per una migliore visibilità dei tempi di replica, puoi [utilizzare la funzionalità di controllo del tempo di replica di S3 \(S3 RTC\)](#).

Se l'oggetto replicato è di grandi dimensioni, attendi qualche minuto prima di controllare se è diventato disponibile nella destinazione. È inoltre possibile controllare lo stato della replica dell'oggetto di origine. Se lo stato della replica dell'oggetto è PENDING, Amazon S3 non ha completato la replica. Se lo stato della replica dell'oggetto è FAILED, controlla la configurazione della replica impostata nel bucket di origine.

Inoltre, per ricevere informazioni sugli errori di Amazon S3 durante la replica, è possibile configurare la funzionalità Notifiche eventi Amazon S3 in modo da ricevere gli eventi di errore di replica. Per ulteriori informazioni, consulta [Ricezione di eventi di errore di replica con notifiche di eventi Amazon S3](#).

- È possibile chiamare l'operazione API `HeadObject` per verificare lo stato della replica di un oggetto. L'operazione API `HeadObject` restituisce lo stato della replica PENDING, COMPLETED o FAILED di un oggetto. In risposta a una chiamata API `HeadObject`, lo stato della replica viene restituito nell'intestazione `x-amz-replication-status`.

 Note

Per eseguire `HeadObject`, è necessario disporre dell'accesso in lettura all'oggetto che si sta richiedendo. Una richiesta `HEAD` ha le stesse opzioni di una richiesta `GET`, senza eseguire alcuna operazione `GET`. Ad esempio, per eseguire una `HeadObject` richiesta utilizzando AWS Command Line Interface (AWS CLI), è possibile eseguire il comando seguente. Sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api head-object --bucket amzn-s3-demo-source-bucket --key index.html
```

- Se `HeadObject` restituisce oggetti con uno stato della replica `FAILED`, è possibile utilizzare Replica in batch S3 per eseguire la replica degli oggetti con replica non riuscita. Per ulteriori informazioni, consulta [the section called “Replica di oggetti esistenti”](#). In alternativa, puoi caricare nuovamente gli oggetti con replica non riuscita nel bucket di origine, che avvierà la replica dei nuovi oggetti.

 Note

Se la regola di replica utilizza l'opzione di modifica della proprietà dell'oggetto con il proprietario del bucket di destinazione e l'oggetto esiste nel bucket di destinazione ma mostra uno stato di `FAILED` replica, S3 Batch Replication potrebbe non risolvere questo stato. Se si verifica questa situazione, contatta l'AWS assistenza per verificare lo stato di replica degli oggetti interessati.

- Nella configurazione di replica nel bucket di origine verifica quanto segue:
 - La correttezza dell'Amazon Resource Name (ARN) relativo al bucket di destinazione.
 - La correttezza del prefisso del nome della chiave. Ad esempio, se si imposta la configurazione per replicare gli oggetti con il prefisso `Tax`, solo gli oggetti con i nomi della chiave quali `Tax/document1` o `Tax/document2` vengono replicati. Un oggetto con il nome della chiave `document3` non sia replicato.
 - Lo stato della regola di replica è `Enabled`.
- Verificare che il controllo delle versioni non sia stato sospeso per i bucket inclusi nella configurazione della replica. Sia per il bucket di origine che per quello di destinazione deve essere abilitata la funzione Controllo delle versioni.

- Se una regola di replica è impostata su Modifica la proprietà dell'oggetto in base al proprietario del bucket di destinazione, il ruolo AWS Identity and Access Management (IAM) utilizzato per la replica deve disporre dell'autorizzazione `s3:ObjectOwnerOverrideToBucketOwner`. Questa autorizzazione viene concessa sulla risorsa (in questo caso, il bucket di destinazione). Ad esempio, la seguente istruzione Resource mostra come concedere questa autorizzazione al bucket di destinazione:

```
{
  "Effect": "Allow",
  "Action": [
    "s3:ObjectOwnerOverrideToBucketOwner"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

- Se il bucket di destinazione è di proprietà di un altro account, il proprietario del bucket di origine deve concedere l'autorizzazione `s3:ObjectOwnerOverrideToBucketOwner` al proprietario del bucket di origine. Per utilizzare la seguente policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Policy1644945280205",
  "Statement": [
    {
      "Sid": "Stmt1644945277847",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
      },
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateTags",
        "s3:ObjectOwnerOverrideToBucketOwner"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

 Note

Se le impostazioni dell'opzione Proprietà dell'oggetto del bucket di destinazione includono Bucket owner enforced, non è necessario aggiornare l'impostazione su Assegna la proprietà degli oggetti al proprietario del bucket di destinazione nella regola di replica. La modifica della proprietà dell'oggetto avverrà per impostazione predefinita. Per ulteriori informazioni sulla modifica della proprietà della replica, consulta [Modifica del proprietario della replica](#).

- Se stai impostando la configurazione della replica in uno scenario con più account, in cui i bucket di origine e di destinazione sono di proprietà diversa Account AWS, i bucket di destinazione non possono essere configurati come bucket Requester Pays. Per ulteriori informazioni, consulta [Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati](#).
- Se gli oggetti di origine di un bucket sono crittografati utilizzando la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS), la regola di replica deve essere configurata per includere oggetti -encrypted. AWS KMS Assicurati di selezionare Replica oggetti crittografati con AWS KMS nelle impostazioni dell'opzione Crittografia nella console Amazon S3. Quindi, seleziona una AWS KMS chiave per crittografare gli oggetti di destinazione.

 Note

Se il bucket di destinazione si trova in un account diverso, specifica una chiave gestita dal AWS KMS cliente di proprietà dell'account di destinazione. Non utilizzare la chiave predefinita gestita da Amazon S3 (aws/s3). L'utilizzo della chiave predefinita crittografa gli oggetti con la chiave gestita da Amazon S3 di proprietà dell'account di origine, impedendo che l'oggetto venga condiviso con un altro account. Di conseguenza, l'account di destinazione non sarà in grado di accedere agli oggetti nel bucket di destinazione.

Per utilizzare una AWS KMS chiave appartenente all'account di destinazione per crittografare gli oggetti di destinazione, l'account di destinazione deve concedere le `kms:Encrypt` autorizzazioni `kms:GenerateDataKey` e al ruolo di replica nella politica delle chiavi KMS. Per utilizzare la seguente istruzione di esempio nella policy della chiave KMS, sostituisci *user input placeholders* con le tue informazioni:

```
{
  "Sid": "AllowS3ReplicationSourceRoleToUseTheKey",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
  },
  "Action": ["kms:GenerateDataKey", "kms:Encrypt"],
  "Resource": "*"
}
```

Se usi un asterisco (*) per l'istruzione Resource nella policy della chiave AWS KMS, la policy concede l'autorizzazione all'uso della chiave KMS solo per il ruolo di replica. La policy non consente al ruolo di replica di aumentare il livello delle proprie autorizzazioni.

Per impostazione predefinita, la policy della chiave KMS concede all'utente root le autorizzazioni complete per la chiave. Queste autorizzazioni possono essere delegate ad altri utenti nello stesso account. A meno che non siano presenti istruzioni Deny nella policy della chiave KMS di origine, è sufficiente utilizzare una policy IAM per concedere le autorizzazioni del ruolo di replica alla chiave KMS di origine.

Note

Le policy della chiave KMS che limitano l'accesso a intervalli CIDR, endpoint del cloud privato virtuale (VPC) o punti di accesso S3 specifici possono causare la mancata riuscita della replica.

Se le chiavi KMS di origine o destinazione concedono autorizzazioni in base al contesto di crittografia, verifica che le chiavi dei bucket Amazon S3 siano attivate per i bucket. Se le chiavi dei bucket Amazon S3 sono attive per i bucket, il contesto di crittografia deve essere la risorsa a livello di bucket, come segue:

```
"kms:EncryptionContext:arn:aws:arn": [
  "arn:aws:s3:::amzn-s3-demo-source-bucket"
]
"kms:EncryptionContext:arn:aws:arn": [
  "arn:aws:s3:::amzn-s3-demo-destination-bucket"
]
```

Oltre alle autorizzazioni concesse dalla policy della chiave KMS, l'account di origine deve aggiungere le seguenti autorizzazioni minime alla policy IAM del ruolo di replica:

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "Source-KMS-Key-ARN"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey",
    "kms:Encrypt"
  ],
  "Resource": [
    "Destination-KMS-Key-ARN"
  ]
}
```

Important

Se utilizzi S3 Batch Replication per replicare i set di dati in più regioni e in precedenza il tipo di crittografia lato server era aggiornato dal al, potresti aver bisogno di autorizzazioni aggiuntive. SSE-S3 SSE-KMS Nel bucket della regione di origine, è necessario disporre delle autorizzazioni. `kms:decrypt` Quindi, avrai bisogno delle `kms:encrypt` autorizzazioni `kms:decrypt` e per il bucket nella regione di destinazione.

Per ulteriori informazioni su come replicare oggetti crittografati con AWS KMS, vedere

[Replicazione di oggetti crittografati](#).

- Se il bucket di destinazione è di proprietà di un altro Account AWS, verifica che il proprietario del bucket abbia una policy sul bucket di destinazione che consenta al proprietario del bucket di origine di replicare gli oggetti. Per un esempio, consulta [Configurazione della replica per i bucket in account diversi](#).

- Per utilizzare Object Lock con la replica, devi concedere due autorizzazioni aggiuntive sul bucket S3 di origine nel ruolo AWS Identity and Access Management (IAM) che utilizzi per configurare la replica. Le due nuove autorizzazioni aggiuntive sono `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se il ruolo dispone di un'istruzione di autorizzazione `s3:Get*`, tale istruzione soddisfa il requisito. Per ulteriori informazioni, consulta [the section called “Utilizzo di Object Lock con la replica S3”](#).
- Se i tuoi oggetti non si replicano anche dopo aver convalidato le autorizzazioni, verifica la presenza di eventuali istruzioni Deny esplicite nelle seguenti posizioni:
 - Le istruzioni Deny nelle policy di bucket di origine o di destinazione. La replica non riesce se la policy del bucket nega l'accesso al ruolo di replica per una delle seguenti operazioni:

Bucket di origine:

```
"s3:GetReplicationConfiguration",  
"s3:ListBucket",  
"s3:GetObjectVersionForReplication",  
"s3:GetObjectVersionAcl",  
"s3:GetObjectVersionTagging"
```

Bucket di destinazione:

```
"s3:ReplicateObject",  
"s3:ReplicateDelete",  
"s3:ReplicateTags"
```

- Le istruzioni Deny o i limiti delle autorizzazione associati al ruolo IAM possono causare la mancata esecuzione della replica.
- Denyle dichiarazioni nelle policy di controllo del AWS Organizations servizio (SCP) associate agli account di origine o di destinazione possono causare il fallimento della replica.
- Denyle dichiarazioni nelle politiche di controllo AWS Organizations delle risorse (RCP) allegate ai bucket di origine o di destinazione possono causare il fallimento della replica.
- Se la replica di un oggetto non è presente nel bucket di destinazione, il problema a livello di replica potrebbe essere dovuto alle cause seguenti:
 - Amazon S3 non replica un oggetto in un bucket di origine che è una replica creata da un'altra configurazione di replica. Se, ad esempio, imposti una configurazione di replica dal bucket A al bucket B al bucket C, Amazon S3 non replica le repliche degli oggetti del bucket B nel bucket C.

- Il proprietario di un bucket di origine può concedere altre Account AWS autorizzazioni per caricare oggetti. Per impostazione predefinita, il proprietario del bucket di origine non dispone di autorizzazioni per gli oggetti creati da altri account. La configurazione di replica esegue la replica solo degli oggetti per i quali il proprietario del bucket di origine dispone delle autorizzazioni di accesso. Per evitare questo problema, il proprietario del bucket di origine può concedere altre Account AWS autorizzazioni per creare oggetti in modo condizionale, richiedendo autorizzazioni di accesso esplicite su tali oggetti. Per un esempio di policy, consulta [Concedere autorizzazioni multi-account per il caricamento di oggetti a garanzia del controllo completo da parte del proprietario del bucket](#).
- Supponiamo di aggiungere nella configurazione della replica una regola per replicare un sottoinsieme di oggetti con un tag specifico. In questo caso, è necessario assegnare il valore e la chiave del tag specifici al momento della creazione dell'oggetto per permettere ad Amazon S3 di replicare l'oggetto. Se prima crei un oggetto e quindi aggiungi il tag all'oggetto esistente, Amazon S3 non replica l'oggetto.
- Usare la funzionalità Notifiche di eventi Amazon S3 per inviare un avviso nei casi in cui gli oggetti non vengono replicati nella Regione AWS di destinazione. Le notifiche di eventi Amazon S3 sono disponibili tramite Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) o AWS Lambda Per ulteriori informazioni, consulta [Ricezione di eventi di errore di replica con notifiche di eventi Amazon S3](#).

Puoi anche visualizzare i motivi degli errori di replica usando la funzionalità Notifiche eventi Amazon S3. Per esaminare l'elenco dei motivi degli errori, consulta [Motivi degli errori di replica Amazon S3](#).

Errori di replica in batch

Per risolvere i problemi relativi agli oggetti che non vengono replicati nel bucket di destinazione, controllare i diversi tipi di autorizzazioni per i bucket, il ruolo di replica e il ruolo IAM utilizzati per creare il processo di replica in batch. Inoltre, occorre assicurarsi di controllare le impostazioni Blocco dell'accesso pubblico e le impostazioni Proprietà oggetti S3 dei bucket.

Per ulteriori suggerimenti per la risoluzione dei problemi relativi all'utilizzo di Operazioni in batch, consulta [the section called “Risoluzione dei problemi relativi a Operazioni in batch S3”](#).

Se hai impostato la replica e gli oggetti non si replicano, vedi [Perché i miei oggetti Amazon S3 non si replicano quando configuro la replica tra i miei bucket?](#) AWS re:Post nel Knowledge Center.

Durante l'utilizzo della replica in batch, è possibile che si verifichi uno dei seguenti errori:

- La generazione del manifesto non ha trovato chiavi corrispondenti ai criteri di filtro.

Questo errore può verificarsi per uno dei seguenti motivi:

- Quando gli oggetti nel bucket di origine vengono archiviati nelle classi di storage Recupero flessibile Amazon S3 Glacier o S3 Glacier Deep Archive.

Per utilizzare la replica in batch su questi oggetti, è innanzitutto necessario ripristinarli nella classe di storage S3 Standard utilizzando un'operazione Ripristino (`S3InitiateRestoreObjectOperation`) in un processo di operazioni in batch. Per ulteriori informazioni, consulta [Ripristino di un oggetto archiviato](#) e [Ripristino di oggetti \(operazioni in batch\)](#). Dopo aver ripristinato gli oggetti, è possibile replicarli utilizzando un processo di replica in batch.

- Quando i criteri di filtro forniti non corrispondono a nessun oggetto valido nel bucket di origine.

Verificare e correggere i criteri di filtro. Ad esempio, nella regola Replica in batch, i criteri di filtro cercano tutti gli oggetti nel bucket di origine con il prefisso `Tax/`. Se il nome del prefisso è stato inserito in modo errato, con una barra all'inizio e alla fine `/Tax/` anziché solo alla fine, non viene trovato alcun oggetto S3. Per risolvere l'errore, correggere il prefisso, in questo caso, da `/Tax/` in `Tax/` nella regola di replica.

- Lo stato dell'operazione in batch non è riuscito e il motivo è: non è stato possibile scrivere il report del processo nel bucket dei report.

Questo errore si verifica se il ruolo IAM utilizzato per il processo Operazioni in batch non è in grado di inserire il report di completamento nella posizione specificata al momento della creazione del processo. Per risolvere questo problema, verificare che il ruolo IAM disponga dell'autorizzazione `s3:PutObject` per il bucket in cui si desidera salvare il report di completamento di Operazioni in batch. È consigliabile inviare il report a un bucket diverso dal bucket di origine.

- L'operazione in batch è stata completata con errori e il totale degli errori non è 0.

Questo errore si verifica in presenza di problemi relativi ad autorizzazioni oggetti insufficienti per il processo di replica in batch in esecuzione. Se si utilizza una regola di replica per il processo di replica in batch, assicurarsi che il ruolo IAM utilizzato per la replica disponga delle autorizzazioni appropriate per accedere agli oggetti dal bucket di origine o di destinazione. Puoi anche controllare il [rapporto sul completamento della replica in batch](#) per esaminare il [motivo specifico dell'errore di Replica Amazon S3](#).

- Il processo batch è stato eseguito correttamente ma il numero di oggetti previsti nel bucket di destinazione non è lo stesso.

Questo errore si verifica quando c'è una mancata corrispondenza tra gli oggetti elencati nel manifesto fornito nel processo di replica in batch e i filtri selezionati al momento della creazione del processo. È possibile che questo messaggio venga visualizzato anche quando gli oggetti nel bucket di origine non corrispondono a nessuna regola di replica e non sono inclusi nel manifesto generato.

Gli errori relativi alle operazioni in batch si verificano dopo l'aggiunta di una nuova regola di replica a una configurazione della replica esistente

Il processo Operazioni in batch tenta di eseguire la replica degli oggetti esistenti per ogni regola nella configurazione della replica del bucket di origine. In caso di problemi con una delle regole di replica esistenti, è possibile che vengano restituiti errori.

Il report di completamento del processo Operazioni in batch spiega i motivi della mancata esecuzione del processo. Per visualizzare un elenco di errori comuni, consulta [Motivi degli errori di replica Amazon S3](#).

Monitoraggio della replica con parametri, notifiche di eventi e stati

È possibile monitorare le configurazioni di replica in tempo reale e i processi Replica in batch S3 tramite i seguenti meccanismi:

- **Metriche di replica S3:** quando abiliti le metriche di replica S3, Amazon CloudWatch emette metriche che puoi utilizzare per tenere traccia dei byte in sospeso, delle operazioni in sospeso e della latenza di replica a livello di regola di replica. Puoi visualizzare le metriche di S3 Replication tramite la console Amazon S3 e la console Amazon CloudWatch. Nella console Amazon S3 è possibile visualizzare questi parametri nella scheda Parametri del bucket di origine. Per ulteriori informazioni sui parametri di Replica S3, consulta [the section called “Utilizzo dei parametri di Replica S3”](#).
- **Parametri di S3 Storage Lens:** oltre ai parametri di Replica S3, è possibile utilizzare i parametri di Protezione dati relativi alla replica forniti dai pannelli di controllo di S3 Storage Lens. Ad esempio, se si utilizzano i parametri gratuiti di S3 Storage Lens, è possibile visualizzare parametri come il numero totale di byte replicati dal bucket di origine o il numero di oggetti replicati dal bucket di origine.

Per verificare la posizione complessiva di replica, è possibile abilitare parametri avanzati in S3 Storage Lens. Con i parametri avanzati di S3 Storage Lens, è possibile vedere di quante regole

di vario tipo si dispone, incluso il numero di regole di replica con una destinazione di replica non valida.

Per ulteriori informazioni sull'utilizzo dei parametri di replica in S3 Storage Lens, consulta [the section called “Visualizzazione dei parametri di replica nei pannelli di controllo di S3 Storage Lens”](#).

- Notifiche di eventi S3: le notifiche di eventi S3 possono inviarti notifiche a livello di oggetto nei casi in cui gli oggetti non si replicano verso la loro destinazione Regione AWS o quando gli oggetti non vengono replicati entro determinate soglie. Notifiche di eventi S3 fornisce i seguenti tipi di eventi di replica: `s3:Replication:OperationFailedReplication`, `s3:Replication:OperationMissedThreshold`, `s3:Replication:OperationReplicatedAfterThreshold` e `s3:Replication:OperationNotTracked`.

Gli eventi Amazon S3 sono disponibili tramite Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) o AWS Lambda. Per ulteriori informazioni, consulta [the section called “Ricezione eventi di errore di replica”](#).

- Valori dello stato della replica: è possibile recuperare anche lo stato della replica degli oggetti. Lo stato della replica consente di determinare lo stato corrente di un oggetto sottoposto a replica. Lo stato della replica di un oggetto di origine restituirà PENDING, COMPLETED o FAILED. Lo stato della replica di una replica restituirà REPLICATION.

È anche possibile utilizzare i valori dello stato della replica durante la creazione di processi di Replica in batch S3. Ad esempio questi valori di stato possono essere utilizzati per replicare gli oggetti che non sono mai stati replicati o la cui replica non è andata a buon fine.

Per ulteriori informazioni sul recupero dello stato della replica degli oggetti, consulta [the section called “Ottenimento dello stato della replica”](#). Per ulteriori informazioni sull'utilizzo di questi valori con Replica in batch, consulta [the section called “Filtri per i processi Batch Replication”](#).

Argomenti

- [Utilizzo dei parametri di Replica S3](#)
- [Visualizzazione dei parametri di replica nei pannelli di controllo di S3 Storage Lens](#)
- [Ricezione di eventi di errore di replica con notifiche di eventi Amazon S3](#)
- [Ottenimento delle informazioni sullo stato della replica](#)

Utilizzo dei parametri di Replica S3

Le metriche di replica S3 forniscono metriche dettagliate per le regole nella configurazione di replica. Con le metriche di replica, puoi monitorare l'avanzamento della replica minuto per minuto controllando i byte in attesa di replica, le operazioni in attesa di replica, le operazioni con replica non riuscita e la latenza di replica.

Note

- Le metriche di replica S3 vengono fatturate alla stessa tariffa delle metriche personalizzate di Amazon CloudWatch. Per ulteriori informazioni, consulta i prezzi di Amazon [CloudWatch](#).
- Se utilizzi S3 Replication Time Control, Amazon CloudWatch inizia a segnalare le metriche di replica 15 minuti dopo aver abilitato S3 RTC sulla rispettiva regola di replica.

I parametri di replica S3 vengono attivati automaticamente quando si abilita il controllo del tempo di replica di S3 (S3 RTC). È anche possibile abilitare i parametri di Replica S3 indipendentemente da S3 RTC durante [la creazione o la modifica di una regola](#). La funzionalità di controllo del tempo di replica di S3 (S3 RTC) include altre funzionalità, ad esempio un Accordo sul livello di servizio (SLA) e notifiche per soglie non raggiunte. Per ulteriori informazioni, consulta [Soddisfazione dei requisiti di conformità con il controllo del tempo di replica di Amazon S3](#).

Quando le metriche di replica S3 sono abilitate, Amazon S3 pubblica le seguenti metriche su Amazon CloudWatch. Le metriche vengono fornite con il massimo impegno possibile.

Nome parametro	Descrizione parametro	A quali oggetti si applica questo parametro?	In quale Regione viene pubblicato o questo parametro?	Questo parametro viene ancora pubblicato se il bucket di destinazione viene eliminato?	Questo parametro viene ancora pubblicato se la replica non avviene?
Byte in attesa di replica	Numero totale di byte	Questa metrica si	Questo parametro	No	Sì

Nome parametro	Descrizione parametro	A quali oggetti si applica questo parametro?	In quale Regione viene pubblicato o questo parametro?	Questo parametro viene ancora pubblicato se il bucket di destinazione viene eliminato?	Questo parametro viene ancora pubblicato se la replica non avviene?
	di oggetti in attesa di replica per una determinata regola di replica.	applica solo ai nuovi oggetti replicati con S3 Replicati on (S3 CRR) o S3 Cross-Region Replication (S3 SRR). Same-Region	viene pubblicato nella Regione del bucket di destinazione.		
Latenza di replica	Numero massimo di secondi in base ai quali il bucket di destinazione della replica è dietro al bucket di origine per una determinata regola di replica.	Questo parametro si applica solo ai nuovi oggetti replicati con S3 CRR o S3 SRR.	Questo parametro viene pubblicato nella Regione del bucket di destinazione.	No	Sì

Nome parametro	Descrizione parametro	A quali oggetti si applica questo parametro?	In quale Regione viene pubblicato o questo parametro?	Questo parametro viene ancora pubblicato se il bucket di destinazione viene eliminato?	Questo parametro viene ancora pubblicato se la replica non avviene?
Operazioni in attesa di replica	Numero di operazioni in attesa di replica per una determinata regola di replica. Questa metrica tiene traccia delle operazioni relative a oggetti, contrassegni di eliminazione, tag, liste di controllo degli accessi (ACL) e blocco degli oggetti S3.	Questo parametro si applica solo ai nuovi oggetti replicati con S3 CRR o S3 SRR.	Questo parametro viene pubblicato nella Regione del bucket di destinazione.	No	Sì

Nome parametro	Descrizione parametro	A quali oggetti si applica questo parametro?	In quale Regione viene pubblicato o questo parametro?	Questo parametro viene ancora pubblicato se il bucket di destinazione viene eliminato?	Questo parametro viene ancora pubblicato se la replica non avviene?
Operazioni di replica non riuscite	Numero di operazioni che non sono state replicate per una determinata regola di replica. Questo parametro tiene traccia delle operazioni relative a oggetti, contrassegni di eliminazione, tag, liste di controllo degli accessi (ACL) e Object Lock. Operazioni di replica non riuscite tiene traccia	Questo parametro si applica sia ai nuovi oggetti replicati con S3 CRR o S3 SRR sia agli oggetti esistenti replicati con S3 Batch Replication. <div>  Note Se un job S3 Batch Replication non viene eseguito affatto, le metriche non </div>	Questo parametro viene pubblicato nella Regione del bucket di origine.	Sì	No

Nome parametro	Descrizione parametro	A quali oggetti si applica questo parametro?	In quale Regione viene pubblicato o questo parametro?	Questo parametro viene ancora pubblicato se il bucket di destinazione viene eliminato?	Questo parametro viene ancora pubblicato se la replica non avviene?
	degli errori di Replica Amazon S3 aggregati a intervalli di un minuto. Per identificare gli oggetti specifici la cui replica non è riuscita e i relativi motivi, iscriviti all'evento Operation FailedReplication mediante la funzionalità Notifiche eventi Amazon S3. Per ulteriori informazioni, consulta Ricezione di eventi di errore di	vengono inviate ad Amazon CloudWatch. Ad esempio, il processo non verrà eseguito se non disponi delle autorizzazioni necessari e per eseguire un processo Replica Amazon S3 o se i tag			

Nome parametro	Descrizione parametro	A quali oggetti si applica questo parametro?	In quale Regione viene pubblicato o questo parametro?	Questo parametro viene ancora pubblicato se il bucket di destinazione viene eliminato?	Questo parametro viene ancora pubblicato se la replica non avviene?
	replica con notifiche di eventi Amazon S3.	o il prefisso nella configurazione della replica non corrispondono.			

Per informazioni su come utilizzare queste metriche in, consulta. CloudWatch [the section called “Metriche di replica S3 in CloudWatch”](#)

Abilitazione dei parametri di replica S3

Puoi iniziare a utilizzare i parametri di replica S3 con una regola di replica nuova o esistente. Per istruzioni complete sulla creazione delle regole di replica, consulta [Configurazione della replica per i bucket nello stesso account](#). Puoi decidere di applicare la regola di replica a un intero bucket S3 o a oggetti Amazon S3 con un prefisso o un tag specifico.

In questo argomento vengono fornite le istruzioni per abilitare le metriche di Replica S3 nella configurazione della replica quando i bucket di origine e destinazione sono di proprietà dello stesso o di diversi Account AWS.

Per abilitare le metriche di replica utilizzando AWS Command Line Interface (AWS CLI), è necessario aggiungere una configurazione di replica al bucket di origine con abilitato. Metrics In questa

configurazione di esempio, gli oggetti con il prefisso *Tax* vengono replicati nel bucket di destinazione *amzn-s3-demo-bucket* e vengono generate le metriche per tali oggetti.

```
{
  "Rules": [
    {
      "Status": "Enabled",
      "Filter": {
        "Prefix": "Tax"
      },
      "Destination": {
        "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
        "Metrics": {
          "Status": "Enabled"
        }
      },
      "Priority": 1
    }
  ],
  "Role": "IAM-Role-ARN"
}
```

Visualizzazione dei parametri di replica

I parametri di Replica S3 sono visualizzati nella scheda Parametri del bucket per uso generico di origine nella console Amazon S3. Queste CloudWatch metriche Amazon sono disponibili anche nella console Amazon CloudWatch. Quando abiliti le metriche di replica S3, Amazon CloudWatch emette metriche che puoi utilizzare per tenere traccia dei byte in sospeso, delle operazioni in sospeso e della latenza di replica a livello di regola di replica.

I parametri di Replica S3 vengono attivati automaticamente quando si abilita la replica con la funzionalità di controllo del tempo di replica di S3 (S3 RTC) utilizzando la console Amazon S3 o la REST API di Amazon S3. È anche possibile abilitare i parametri di Replica S3 indipendentemente da S3 RTC durante [la creazione o la modifica di una regola](#).

Se utilizzi S3 Replication Time Control, Amazon CloudWatch inizia a segnalare le metriche di replica 15 minuti dopo aver abilitato S3 RTC sulla rispettiva regola di replica. Per ulteriori informazioni, consulta [Utilizzo dei parametri di Replica S3](#).

I parametri di replica tengono traccia degli ID regola della configurazione di replica. Un ID regola di replica può essere specifico per un prefisso, un tag o una combinazione di entrambi.

Per ulteriori informazioni sulle metriche per Amazon S3, consulta [CloudWatch Metriche di monitoraggio con Amazon CloudWatch](#)

Prerequisiti

Creare una regola di replica che dispone di parametri di Replica S3 abilitati. Per ulteriori informazioni, consulta [the section called “Abilitazione dei parametri di replica”](#).

Per visualizzare le metriche di replica di S3 tramite il bucket di origine Metriche linguetta

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket seleziona il nome del bucket contenente gli oggetti per cui desideri ottenere le metriche di replica.
4. Seleziona la scheda Parametri.
5. In Parametri di replica, scegli le regole di replica per le quali desideri visualizzare i parametri.
6. Seleziona Visualizza grafici.

Amazon S3 visualizza i grafici relativi a Latenza di replica, Byte in attesa di replica, Operazioni in attesa di replica e Operazioni di replica non riuscite per le regole selezionate.

Visualizzazione dei parametri di replica nei pannelli di controllo di S3 Storage Lens

Oltre ai [parametri di Replica S3](#), è possibile utilizzare i parametri di Protezione dati relativi alla replica forniti da S3 Storage Lens. S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti. Per ulteriori informazioni, consulta [Utilizzo di S3 Storage Lens per proteggere i dati](#).

A un costo aggiuntivo, è possibile eseguire l'aggiornamento e ricevere due livelli di parametri di S3 Storage Lens: parametri gratuiti e parametri e suggerimenti avanzati. I parametri avanzati e i suggerimenti ti consentono di accedere a parametri e funzionalità aggiuntive per ottenere informazioni dettagliate sul tuo spazio di archiviazione. Per maggiori informazioni sui prezzi di S3 Storage Lens, consulta i [prezzi di Amazon S3](#).

Se si utilizzano i parametri gratuiti di S3 Storage Lens, è possibile visualizzare parametri come il numero totale di byte replicati dal bucket di origine o il numero di oggetti replicati dal bucket di origine.

Per verificare la posizione complessiva di replica, è possibile abilitare parametri avanzati in S3 Storage Lens. Con i parametri avanzati di S3 Storage Lens, è possibile vedere di quante regole di vario tipo si dispone, incluso il numero di regole di replica con una destinazione di replica non valida.

Per un elenco completo dei parametri di S3 Storage Lens, inclusi i parametri di replica presenti in ogni livello, consulta il [Glossario dei parametri di S3 Storage Lens](#).

Prerequisiti

Creare una [configurazione della replica in tempo reale](#) o un [processo di Replica in batch S3](#).

Per visualizzare i parametri di replica in Amazon S3 Storage Lens

1. Creare un pannello di controllo di S3 Storage Lens. Per istruzioni dettagliate, consulta [the section called “Utilizzo della console S3”](#).
2. (Facoltativo) Durante la configurazione del pannello di controllo, se desideri visualizzare tutti i parametri di replica di S3 Storage Lens, seleziona Parametri e raccomandazioni avanzati, quindi seleziona Parametri avanzati di protezione dei dati. Per un elenco completo dei parametri, consulta [Glossario dei parametri di S3 Storage Lens](#).

Se si abilitano i suggerimenti e i parametri avanzati, è possibile ottenere ulteriori informazioni sulle configurazioni di replica. I parametri relativi al conteggio delle regole di replica di S3 Storage Lens possono essere utilizzati per ottenere informazioni dettagliate sui bucket configurati per la replica. Queste informazioni includono le regole di replica all'interno di e tra bucket e regioni. Per ulteriori informazioni, consulta [the section called “Conteggiare il numero totale di regole di replica per ogni bucket”](#).

3. Dopo aver creato il pannello di controllo, aprilo e scegli la scheda Bucket.
4. Scorri fino alla sezione Buckets (Bucket). In Metrics categories (Categorie parametri), scegli Data protection (Protezione dati). Quindi deseleziona Summary (Riepilogo).
5. Per filtrare l'elenco dei bucket in modo da visualizzare solo le metriche di replica, scegli l'icona Preferenze ().



6. Deseleziona tutti i parametri di protezione dei dati finché non rimangono selezionati solo i parametri di replica.
7. (Facoltativo) In Page size (Dimensioni pagina), scegli il numero di bucket da visualizzare nell'elenco.
8. Scegli Continua.

Ricezione di eventi di errore di replica con notifiche di eventi Amazon S3

Se sulla propria configurazione della replica sono stati abilitati i parametri di Replica S3, è possibile configurare Notifiche di eventi Amazon S3 per inviare una notifica quando gli oggetti non vengono replicati nella loro Regione AWS di destinazione. Se si è abilitato il controllo del tempo di replica di S3 (S3 RTC) sulla propria configurazione della replica, è anche possibile ricevere una notifica quando gli oggetti non vengono replicati entro la soglia S3 RTC di 15 minuti per la replica.

Important

Per ricevere le notifiche degli eventi di errore di replica (`s3:Replication:OperationFailedReplication`), è necessario abilitare le metriche di replica S3 nella regola di replica. Non è necessario abilitare S3 Replication Time Control (S3 RTC) per ricevere notifiche di errore. S3 RTC è richiesto solo per le notifiche basate sulla soglia (`s3:Replication:OperationMissedThreshold` e `s3:Replication:OperationReplicatedAfterThreshold`). È possibile abilitare le metriche di replica S3 indipendentemente da S3 RTC. Per ulteriori informazioni, consulta [Abilitazione dei parametri di replica S3](#).

Attraverso l'uso dei seguenti tipi di evento `Replication`, è possibile monitorare l'avanzamento degli eventi di replica minuto per minuto controllando i byte in sospeso, le operazioni in sospeso e la latenza di replica. Per ulteriori informazioni sui parametri di Replica S3, consulta [Utilizzo dei parametri di Replica S3](#).

- Il tipo di evento `s3:Replication:OperationFailedReplication` notifica quando un oggetto idoneo per la replica non è stato replicato.
- Il tipo di evento `s3:Replication:OperationMissedThreshold` notifica quando un oggetto idoneo per la replica che utilizza S3 RTC supera la soglia di 15 minuti per la replica.
- Il tipo di evento `s3:Replication:OperationReplicatedAfterThreshold` notifica quando un oggetto idoneo per la replica che utilizza S3 RTC viene replicato dopo la soglia di 15 minuti.
- Il tipo di `s3:Replication:OperationNotTracked` evento ti avvisa quando un oggetto idoneo per la replica in tempo reale (Replication [SRR] o Same-Region Replication [CRR]) non viene più tracciato dalle metriche di Cross-Region replica.

Per una descrizione completa dei tipi di eventi di replica supportati, consulta [the section called “Tipi di eventi supportati per SQS, SNS e Lambda”](#).

Per l'elenco dei codici di errore acquisiti da Notifiche di eventi S3, consulta [Motivi degli errori di replica Amazon S3](#).

Puoi ricevere notifiche di eventi Amazon S3 utilizzando Amazon Simple Queue Service (Amazon SQS), Servizio di notifica semplice Amazon (Amazon SNS) o AWS Lambda. Per ulteriori informazioni, consulta [the section called “Notifiche di eventi Amazon S3”](#).

Per istruzioni su come configurare Notifiche di eventi Amazon S3, consulta [Abilitare le notifiche di eventi](#).

Quello che segue è un esempio di un messaggio inviato da Amazon S3 per pubblicare un evento `s3:Replication:OperationFailedReplication`. Per ulteriori informazioni, consulta [the section called “Struttura del messaggio di evento”](#).

```
{
  "Records": [
    {
      "eventVersion": "2.2",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "2024-09-05T21:04:32.527Z",
      "eventName": "Replication:OperationFailedReplication",
      "userIdentity": {
        "principalId": "s3.amazonaws.com"
      },
      "requestParameters": {
        "sourceIPAddress": "s3.amazonaws.com"
      },
      "responseElements": {
        "x-amz-request-id": "123bf045-2b4b-4ca8-a211-c34a63c59426",
        "x-amz-id-2":
"12VAWNDIHNwJsRhTccqQTeAPoXQmRt22KkewMV8G3XZihAuf9CLDdmkApgZzudaIe2K1LfDqGS0="
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "ReplicationEventName",
        "bucket": {
          "name": "amzn-s3-demo-bucket1",
          "ownerIdentity": {
            "principalId": "111122223333"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
        }
      }
    }
  ]
}
```

```
    "object": {
      "key": "replication-object-put-test.png",
      "size": 520080,
      "eTag": "e12345ca7e88a38428305d3ff7fcb99f",
      "versionId": "abcdeH0Xp66ep__QDjR76LK7Gc9X4wK0",
      "sequencer": "0066DA1CBF104C0D51"
    },
    "replicationEventData": {
      "replicationRuleId": "notification-test-replication-rule",
      "destinationBucket": "arn:aws:s3:::amzn-s3-demo-bucket2",
      "s3Operation": "OBJECT_PUT",
      "requestTime": "2024-09-05T21:03:59.168Z",
      "failureReason": "AssumeRoleNotPermitted"
    }
  ]
}
```

Motivi degli errori di replica Amazon S3

La seguente tabella elenca i motivi degli errori di replica in Amazon S3. È possibile visualizzare questi motivi ricevendo l'evento `s3:Replication:OperationFailedReplication` con Notifiche di eventi Amazon S3 e cercando il valore `failureReason`.

Puoi visualizzare questi motivi di errore anche nei report di completamento della replica in batch in S3. Per ulteriori informazioni, consulta [Report di completamento della replica in batch](#).

Motivo dell'errore di replica	Description
AssumeRoleNotPermitted	Amazon S3 non può assumere il ruolo AWS Identity and Access Management (IAM) specificato nella configurazione di replica o nel job Batch Operations.
DstBucketInvalidRegion	Il bucket di destinazione non è lo stesso specificato dal Regione AWS job Batch Operations. Questo errore è specifico per la replica in batch.

Motivo dell'errore di replica	Description
DstBucketNotFound	Amazon S3 non è in grado di trovare il bucket di destinazione specificato nella configurazione della replica.
DstBucketObjectLockConfigMissing	Per replicare gli oggetti da un bucket di origine con la funzionalità di blocco degli oggetti abilitata, anche la destinazione deve avere il blocco degli oggetti abilitato. Questo errore indica che il blocco degli oggetti potrebbe non essere abilitato nel bucket di destinazione. Per ulteriori informazioni, consulta Considerazioni su Object Lock .
DstBucketUnversioned	Il controllo delle versioni non è abilitato per il bucket di destinazione S3. Per replicare gli oggetti con la funzionalità Replica Amazon S3, abilita il controllo delle versioni per bucket di destinazione.
DstDelObjNotPermitted	Amazon S3 non è in grado di replicare i contrassegni di eliminazione nel bucket di destinazione. È possibile che manchi l'autorizzazione <code>s3:ReplicateDelete</code> per il bucket di destinazione.
DstKmsKeyInvalidState	La chiave AWS Key Management Service (AWS KMS) per il bucket di destinazione non è valida. Rivedi e abilita la AWS KMS chiave richiesta. Per ulteriori informazioni sulla gestione delle AWS KMS chiavi, consulta Key states of AWS KMS keys nella AWS Key Management Service Developer Guide.
DstKmsKeyNotFound	La AWS KMS chiave configurata per il bucket di destinazione nella configurazione di replica non esiste.

Motivo dell'errore di replica	Description
<code>DstMultipartCompleteNotPermitted</code>	Amazon S3 non è in grado di completare i caricamenti in più parti degli oggetti nel bucket di destinazione. È possibile che manchi l'autorizzazione <code>s3:ReplicateObject</code> per il bucket di destinazione.
<code>DstMultipartInitNotPermitted</code>	Amazon S3 non è in grado di avviare i caricamenti in più parti degli oggetti nel bucket di destinazione. È possibile che manchi l'autorizzazione <code>s3:ReplicateObject</code> per il bucket di destinazione.
<code>DstMultipartUploadNotPermitted</code>	Amazon S3 non è in grado di caricare oggetti in più parti nel bucket di destinazione. È possibile che manchi l'autorizzazione <code>s3:ReplicateObject</code> per il bucket di destinazione.
<code>DstObjectHardDeleted</code>	S3 Batch Replication non supporta la ripetizione della replica di oggetti eliminati con l'ID versione dell'oggetto del bucket di destinazione. Questo errore è specifico per la replica in batch.
<code>DstPutAclNotPermitted</code>	Amazon S3 non è in grado di replicare le liste di controllo degli accessi (ACL) dell'oggetto nel bucket di destinazione. È possibile che manchi l'autorizzazione <code>s3:ReplicateObject</code> per il bucket di destinazione.

Motivo dell'errore di replica	Description
DstPutLegalHoldNotPermitted	Amazon S3 non è in grado di impostare un blocco legale di Object Lock per l'oggetto di destinazione durante la replica di oggetti immutabili. È possibile che manchi l'autorizzazione <code>s3:PutObjectLegalHold</code> per il bucket di destinazione. Per ulteriori informazioni, consulta Blocchi a fini giudiziari .
DstPutObjectNotPermitted	Amazon S3 non è in grado di replicare oggetti nel bucket di destinazione. Ciò può verificarsi quando mancano le autorizzazioni (<code>s3:ReplicateObject</code> o le <code>s3:ObjectOwnerOverrideToBucketOwner</code> autorizzazioni) richieste per il bucket di destinazione o quando la policy AWS KMS chiave non consente al ruolo di replica del bucket di origine di utilizzare la AWS KMS chiave (<code>kms:Decrypt</code> e <code>kms:GenerateDataKey*</code> le azioni) nel bucket di destinazione.
DstPutRetentionNotPermitted	Amazon S3 non è in grado di impostare un periodo di conservazione degli oggetti di destinazione durante la replica di oggetti immutabili. È possibile che manchi l'autorizzazione <code>s3:PutObjectRetention</code> per il bucket di destinazione.
DstPutTaggingNotPermitted	Amazon S3 non è in grado di replicare tag di oggetti nel bucket di destinazione. È possibile che manchi l'autorizzazione <code>s3:ReplicateObject</code> per il bucket di destinazione.

Motivo dell'errore di replica	Description
<code>DstVersionNotFound</code>	Amazon S3 non è in grado di trovare la versione dell'oggetto richiesta nel bucket di destinazione per cui devono essere replicati i metadati.
<code>InitiateReplicationNotPermitted</code>	Amazon S3 non è in grado di avviare la replica sugli oggetti. È possibile che manchi l'autorizzazione <code>s3:InitiateReplication</code> per il processo Operazioni in batch. Questo errore è specifico per la replica in batch.
<code>SrcBucketInvalidRegion</code>	Il bucket di origine non è lo stesso specificato dal job Batch Operations Regione AWS . Questo errore è specifico per la replica in batch.
<code>SrcBucketNotFound</code>	Amazon S3 non è in grado di trovare il bucket di origine.
<code>SrcBucketReplicationConfigMissing</code>	Amazon S3 non è riuscito a trovare una configurazione della replica per il bucket di origine.

Motivo dell'errore di replica	Description
<code>SrcGetAclNotPermitted</code>	<p>Amazon S3 non è in grado di accedere all'oggetto nel bucket di origine per la replica. È possibile che manchi l'autorizzazione <code>s3:GetObjectVersionAcl</code> per l'oggetto del bucket di origine.</p> <p>Gli oggetti nel bucket di origine devono essere di proprietà del proprietario del bucket. Se gli ACL sono abilitati, verifica se Proprietà dell'oggetto è impostata su Proprietario del bucket preferito o Autore dell'oggetto. Se Proprietà dell'oggetto è impostata su Proprietario del bucket preferito, gli oggetti del bucket di origine devono avere l'ACL <code>bucket-owner-full-control</code> affinché il proprietario del bucket diventi il proprietario dell'oggetto. L'account di origine può acquisire la proprietà di tutti gli oggetti nel relativo bucket impostando Proprietà dell'oggetto su Proprietario del bucket preferito e disabilitando gli ACL.</p>
<code>SrcGetLegalHoldNotPermitted</code>	<p>Amazon S3 non è in grado di accedere alle informazioni di conservazione legale di S3 Object Lock.</p>
<code>SrcGetObjectNotPermitted</code>	<p>Amazon S3 non è in grado di accedere all'oggetto nel bucket di origine per la replica. È possibile che manchi l'autorizzazione <code>s3:GetObjectVersionForReplication</code> per il bucket di origine.</p>
<code>SrcGetRetentionNotPermitted</code>	<p>Amazon S3 non è in grado di accedere alle informazioni del periodo di conservazione di S3 Object Lock.</p>

Motivo dell'errore di replica	Description
<code>SrcGetTaggingNotPermitted</code>	Amazon S3 non è in grado di accedere alle informazioni sui tag di oggetto dal bucket di origine. È possibile che manchi l'autorizzazione <code>s3:GetObjectVersionTagging</code> per il bucket di origine.
<code>SrcHeadObjectNotPermitted</code>	Amazon S3 non è in grado di recuperare i metadati dell'oggetto dal bucket di origine. È possibile che manchi l'autorizzazione <code>s3:GetObjectVersionForReplication</code> per il bucket di origine.
<code>SrcKeyNotFound</code>	Amazon S3 non è in grado di trovare la chiave dell'oggetto di origine da replicare. L'oggetto di origine potrebbe essere stato eliminato prima del completamento della replica.
<code>SrcKmsKeyInvalidState</code>	La AWS KMS chiave per il bucket di origine non è valida. Rivedi e abilita la AWS KMS chiave richiesta. Per ulteriori informazioni sulla gestione delle AWS KMS chiavi, consulta Key states of AWS KMS keys nella AWS Key Management Service Developer Guide.
<code>SrcObjectNotEligible</code>	Alcuni oggetti non sono idonei per la replica. Ciò può essere dovuto alla classe di archiviazione dell'oggetto o ai tag dell'oggetto che non corrispondono alla configurazione di replica.
<code>SrcObjectNotFound</code>	L'oggetto di origine non esiste.
<code>SrcReplicationNotPending</code>	Amazon S3 ha già replicato questo oggetto. Questo oggetto non è più in attesa di replica.

Motivo dell'errore di replica	Description
<code>SrcVersionNotFound</code>	Amazon S3 non è in grado di trovare la versione dell'oggetto di origine da replicare. La versione dell'oggetto di origine potrebbe essere stato eliminato prima del completamento della replica.
<code>SrcAnnotationNotFound</code>	L'annotazione di origine non è stata trovata. L'annotazione è stata eliminata prima del completamento della replica.
<code>SrcGetObjectAnnotationNotPermitted</code>	Accesso negato durante il recupero dell'annotazione di origine per la replica. Manca il ruolo IAM. <code>s3:GetObjectVersionAnnotationForReplication</code>
<code>DstPutObjectAnnotationNotPermitted</code>	Accesso negato durante la replica dell'annotazione nel bucket di destinazione. Il ruolo IAM è mancante <code>s3:ReplicateObject</code> o non ha accesso alla chiave richiesta. AWS KMS
<code>SrcAnnotationEncryptionUnsupported</code>	Il tipo di crittografia delle annotazioni degli oggetti non è supportato.
<code>AnnotationLimitExceeded</code>	Il numero di annotazioni degli oggetti supera il limite (1000). La replica supererebbe il limite di annotazioni sulla destinazione.

Argomenti correlati

[Configurazione delle autorizzazioni per la replica in tempo reale](#)

[Risoluzione dei problemi nella replica](#)

Ottenimento delle informazioni sullo stato della replica

Lo stato della replica consente di determinare lo stato corrente di un oggetto da replicare. Lo stato della replica di un oggetto di origine restituirà PENDING, COMPLETED o FAILED. Lo stato della replica di una replica restituirà REPLICA.

È anche possibile utilizzare i valori dello stato della replica durante la creazione di processi di Replica in batch S3. Ad esempio questi valori di stato possono essere utilizzati per replicare gli oggetti che non sono mai stati replicati o la cui replica non è andata a buon fine. Per ulteriori informazioni sull'utilizzo di questi valori con Replica in batch, consulta [the section called “Utilizzo delle informazioni sullo stato della replica con i processi di Replica in batch”](#).

Argomenti

- [Panoramica dello stato della replica](#)
- [Stato della replica in caso di replica su più bucket di destinazione](#)
- [Stato della replica se è abilitata la sincronizzazione della modifica alla replica Amazon S3](#)
- [Utilizzo delle informazioni sullo stato della replica con i processi di Replica in batch](#)
- [Ricerca dello stato di replica](#)

Panoramica dello stato della replica

Nella replica esistono un bucket di origine in cui si configura la replica e uno o più bucket di destinazione in cui Amazon S3 replica gli oggetti. Quando si richiede un oggetto (utilizzando GetObject) o i metadati di un oggetto (utilizzando HeadObject) da questi bucket, Amazon S3 restituisce l'intestazione `x-amz-replication-status` nella risposta:

- Quando richiedi un oggetto dal bucket di origine, Amazon S3 restituisce l'intestazione `x-amz-replication-status` se l'oggetto nella richiesta è idoneo per la replica.

Supponi, ad esempio, che nella configurazione di replica venga specificato il prefisso di oggetto `TaxDocs` che indica ad Amazon S3 di replicare solo gli oggetti con il prefisso del nome della chiave `TaxDocs`. Tutti gli oggetti caricati che hanno questo prefisso del nome della chiave, ad esempio `TaxDocs/document1.pdf`, verranno replicati. Per le richieste di oggetti con questo prefisso del nome della chiave, Amazon S3 restituisce l'intestazione `x-amz-replication-status` con uno dei valori seguenti per lo stato della replica dell'oggetto: PENDING, COMPLETED o FAILED.

 Note

Se la replica dell'oggetto ha esito negativo dopo il caricamento di un oggetto, non è possibile provare a eseguirla di nuovo. È necessario caricare nuovamente l'oggetto oppure utilizzare Replica in batch S3 per replicare eventuali oggetti la cui replica non è riuscita. S3 Lifecycle blocca le azioni di scadenza e transizione sugli oggetti con o stato di replica. PENDING FAILED Per ulteriori informazioni su Replica in batch, consulta [the section called “Replica di oggetti esistenti”](#).

Gli oggetti passano a uno FAILED stato per problemi quali la mancanza delle autorizzazioni dei ruoli di replica, delle autorizzazioni AWS Key Management Service (AWS KMS) o delle autorizzazioni dei bucket. In caso di errori temporanei, ad esempio se un bucket o una Regione non è disponibile, lo stato della replica non passerà a FAILED, ma rimarrà PENDING. Dopo che la risorsa torna online, Amazon S3 riprende la replica di tali oggetti.

- Quando richiedi un oggetto dal bucket di destinazione, se l'oggetto nella richiesta è una replica creata da Amazon S3, Amazon S3 restituisce l'intestazione `x-amz-replication-status` con il valore REPLICATION.

 Note

Prima di eliminare un oggetto da un bucket di origine in cui è abilitata la replica, è consigliabile controllare lo stato della replica per assicurarsi che l'oggetto sia stato replicato. Se una configurazione del ciclo di vita S3 è abilitata nel bucket di origine, Amazon S3 sospende le azioni del ciclo di vita finché non contrassegna lo stato di replica dell'oggetto come COMPLETED. Se lo stato della replica è FAILED, S3 Lifecycle continua a bloccare le azioni di scadenza e transizione sull'oggetto finché non si risolve il problema di replica sottostante. Per ulteriori informazioni, consulta [S3 Lifecycle e S3 Replication](#).

Stato della replica in caso di replica su più bucket di destinazione

Quando si replicano oggetti in più bucket di destinazione, l'intestazione `x-amz-replication-status` funziona in modo diverso. L'intestazione dell'oggetto di origine restituisce un valore COMPLETED solo se la replica ha esito positivo su tutte le destinazioni. L'intestazione rimane al valore

PENDING fino al completamento della replica per tutte le destinazioni. Se la replica su una o più destinazioni non riesce, viene restituita l'intestazione FAILED.

Stato della replica se è abilitata la sincronizzazione della modifica alla replica Amazon S3

Quando le regole di replica abilitano la sincronizzazione delle modifiche alla replica Amazon S3, le repliche possono riportare stati diversi da REPLICATION. Se le modifiche dei metadati sono in corso di replica, l'intestazione `x-amz-replication-status` restituisce PENDING. Se la sincronizzazione delle modifiche della replica non riesce a replicare i metadati, l'intestazione restituisce FAILED. Se i metadati vengono replicati correttamente, le repliche restituiscono l'intestazione REPLICATION.

Utilizzo delle informazioni sullo stato della replica con i processi di Replica in batch

Quando si crea un processo di Replica in batch, è possibile specificare opzionalmente dei filtri aggiuntivi, ad esempio la data di creazione dell'oggetto e lo stato della replica, al fine di ridurre l'ambito del processo.

Puoi filtrare gli oggetti da replicare in base al valore `ObjectReplicationStatuses` fornendo uno o più dei seguenti valori:

- "NONE": indica che Amazon S3 non ha mai tentato di replicare l'oggetto in precedenza.
- "FAILED": indica che Amazon S3 ha tentato di replicare l'oggetto in precedenza ma la replica non è andata a buon fine.
- "COMPLETED": indica che Amazon S3 ha replicato correttamente l'oggetto in precedenza.
- "REPLICATION": indica che si tratta di un oggetto di replica replicato da Amazon S3 da un'altra origine.

Per ulteriori informazioni sull'utilizzo di questi valori dello stato della replica con Replica in batch, consulta [the section called “Filtri per i processi Batch Replication”](#).

Ricerca dello stato di replica

Per visualizzare lo stato della replica degli oggetti in un bucket, è possibile utilizzare lo strumento Inventario Amazon S3. Amazon S3 invia un file CSV al bucket di destinazione specificato nella configurazione dell'inventario. Puoi anche utilizzare Amazon Athena per eseguire una query sullo stato della replica nel report di inventario. Per ulteriori informazioni su Inventario Amazon S3, consulta [Catalogazione e analisi dei dati con Inventario S3](#).

Puoi anche trovare lo stato di replica dell'oggetto utilizzando la console Amazon S3, () o l' AWS Command Line Interface SDK.AWS CLI AWS

Utilizzo della console S3

Nella console Amazon S3 è possibile visualizzare lo stato della replica di un oggetto nella pagina dei dettagli dell'oggetto.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Scegli il nome del bucket di origine della replica nell'elenco Bucket per uso generico.
4. Nell'elenco Oggetti, seleziona il nome dell'oggetto. Viene visualizzata la pagina dei dettagli dell'oggetto.
5. Nella scheda Proprietà scorrere verso il basso fino alla sezione Panoramica della gestione degli oggetti. In Configurazioni di gestione, controllare il valore in Stato della replica.

Utilizzo di AWS CLI

Usa il `head-object` comando AWS Command Line Interface (AWS CLI) per recuperare i metadati degli oggetti, come mostrato nell'esempio seguente. Sostituire *amzn-s3-demo-source-bucket1* con il nome del bucket di origine della replica e sostituire l'altro *user input placeholders* con le proprie informazioni.

```
aws s3api head-object --bucket amzn-s3-demo-source-bucket1 --key object-key --version-id object-version-id
```

Il comando restituisce i metadati dell'oggetto, incluso l'elemento `ReplicationStatus` come illustrato nella risposta di esempio seguente.

```
{
  "AcceptRanges": "bytes",
  "ContentType": "image/jpeg",
  "LastModified": "Mon, 23 Mar 2015 21:02:29 GMT",
  "ContentLength": 3191,
  "ReplicationStatus": "COMPLETED",
  "VersionId": "jfnW.HIM0fYiD_9rGbSkmroXsFj3fqZ.",
  "ETag": "\"6805f2cfc46c0f04559748bb039d69ae\"",
  "Metadata": {

  }
}
```

Utilizzo di AWS SDK

I seguenti frammenti di codice consentono di ottenere lo stato della replica utilizzando rispettivamente il simbolo e. AWS SDK per Java AWS SDK per .NET

Java

```
GetObjectMetadataRequest metadataRequest = new GetObjectMetadataRequest(bucketName,
    key);
ObjectMetadata metadata = s3Client.getObjectMetadata(metadataRequest);

System.out.println("Replication Status : " +
    metadata.getRawMetadataValue(Headers.OBJECT_REPLICATION_STATUS));
```

.NET

```
GetObjectMetadataRequest getmetadataRequest = new GetObjectMetadataRequest
{
    BucketName = sourceBucket,
    Key        = objectKey
};

GetObjectMetadataResponse getmetadataResponse =
    client.GetObjectMetadata(getmetadataRequest);
Console.WriteLine("Object replication status: {0}",
    getmetadataResponse.ReplicationStatus);
```

Puoi trovare lo stato di replica delle annotazioni utilizzando l'API Amazon S3 o i metadati Amazon S3. Le operazioni `ListObjectAnnotations` e `GetObjectAnnotation` API restituiscono lo stato di replica per ogni annotazione nella risposta. Se disponi di una configurazione della tabella dei metadati di Amazon S3 che include annotazioni, puoi interrogare la `replication_status` colonna nella tabella delle annotazioni. Per ulteriori informazioni, consulta [the section called “Schema della tabella di annotazione”](#).

Gestione del traffico multiregionale con punti di Multi-Region accesso

Amazon S3 Multi-Region Access Points fornisce un endpoint globale che le applicazioni possono utilizzare per soddisfare le richieste provenienti da bucket S3 che si trovano in più unità. Regioni AWS

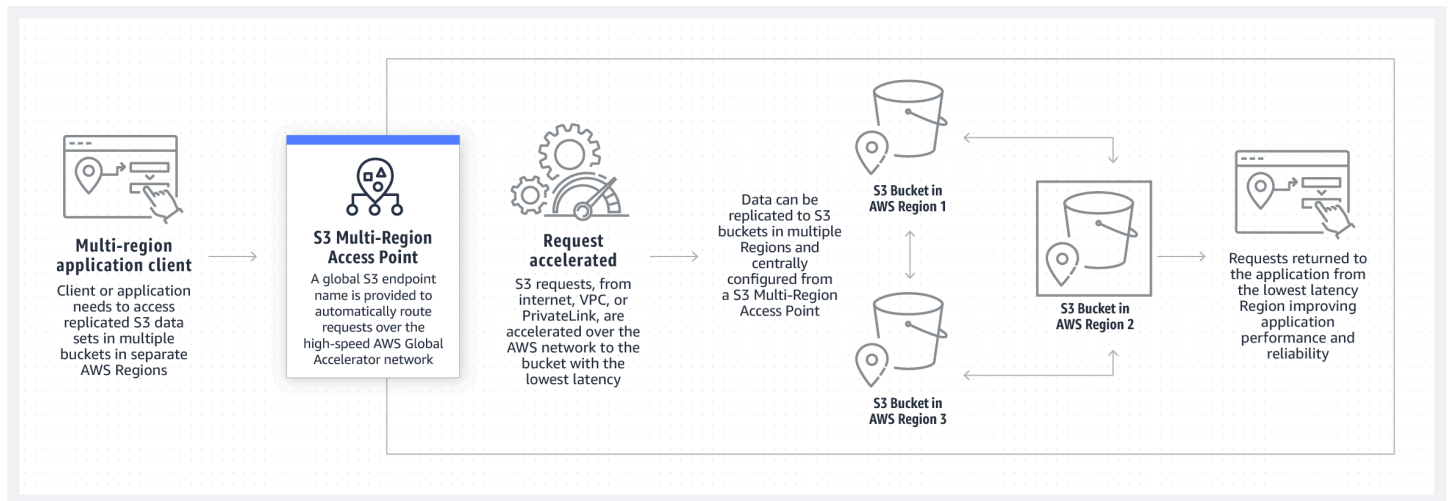
Puoi utilizzare gli Multi-Region Access Points per creare applicazioni multiregionali con la stessa architettura utilizzata in una singola regione e quindi eseguire tali applicazioni in qualsiasi parte del mondo. Invece di inviare richieste sulla rete Internet pubblica congestionata, Multi-Region Access Points offre una resilienza di rete integrata con accelerazione delle richieste basate su Internet ad Amazon S3. Le richieste applicative effettuate a un endpoint globale di Multi-Region Access Point vengono utilizzate [AWS Global Accelerator](#) automaticamente attraverso la rete AWS globale verso il bucket S3 più vicino con uno stato di routing attivo.

Se si verifica un'interruzione del traffico regionale, puoi utilizzare i controlli di failover degli Multi-Region Access Points per spostare il traffico delle richieste di dati S3 tra Regioni AWS e reindirizzare il traffico S3 lontano dalle interruzioni in pochi minuti. È possibile anche testare la resilienza dell'applicazione rispetto a un'interruzione per eseguire il failover delle applicazioni ed eseguire simulazioni di disaster recovery. Se hai bisogno di connettere e accelerare le richieste a S3 dall'esterno di un VPC, puoi semplificare le applicazioni e l'architettura di rete con gli Amazon Multi-Region S3 Access Point. Le tue richieste di Multi-Region Access Point verranno inoltrate sulla rete AWS globale e quindi nuovamente a S3 all'interno della rete Regione AWS, senza dover attraversare la rete Internet pubblica. Di conseguenza, è possibile creare applicazioni ad altissima disponibilità.

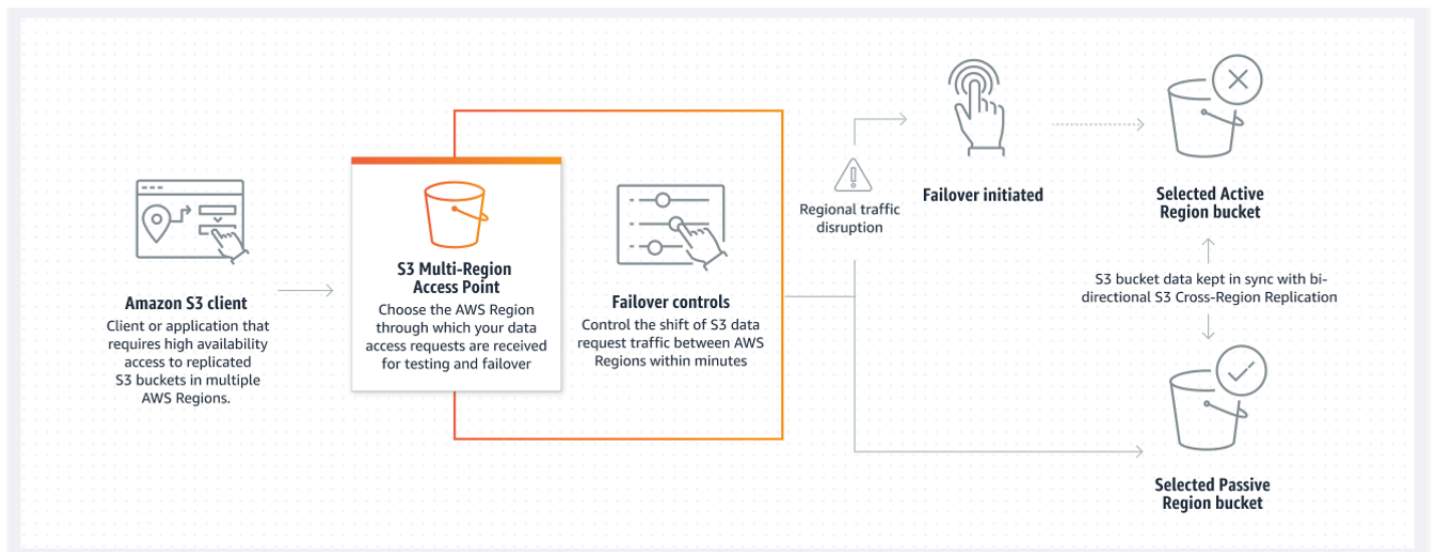
Durante la creazione e la configurazione degli Multi-Region Access Point, specificherai una serie di punti Regioni AWS in cui desideri archiviare i dati da fornire tramite quell'Access Point. Multi-Region Puoi utilizzare il nome dell'endpoint degli Multi-Region Access Points fornito per connettere i tuoi client. Dopo aver stabilito le connessioni con i client, puoi selezionare i bucket esistenti o nuovi tra i quali desideri instradare le richieste di Multi-Region Access Point. Quindi, utilizza le regole di [Cross-Region replica S3 \(CRR\)](#) per sincronizzare i dati tra i bucket in quelle regioni.

Dopo aver configurato l' Multi-Region Access Point, puoi quindi richiedere o scrivere dati tramite l'endpoint globale di Access Points. Multi-Region Amazon S3 gestisce automaticamente le richieste al set di dati replicato dalla Regione disponibile più vicina. All'interno di Console di gestione AWS, puoi anche visualizzare la topologia di replica sottostante e le metriche di replica relative alle tue richieste di Access Point. Multi-Region In questo modo è ancora più semplice creare, gestire e monitorare lo storage per le applicazioni multi-regione. In alternativa, puoi utilizzare Amazon CloudFront per automatizzare la creazione e la configurazione degli Multi-Region Access Point S3.

L'immagine seguente è una rappresentazione grafica di un punto di accesso Amazon Multi-Region S3 in una configurazione active-active. Il grafico mostra come le richieste Amazon S3 vengono indirizzate automaticamente ai bucket nella Regione AWS attiva più vicina.



L'immagine seguente è una rappresentazione grafica di un punto di accesso Amazon Multi-Region S3 in una configurazione attiva-passiva. Il grafico illustra come controllare il traffico di accesso ai dati di Amazon S3 per passare tra Regioni AWS attive e passive.



Argomenti

- [Creazione di punti di Multi-Region accesso](#)
- [Configurazione di un punto di accesso multiregionale da utilizzare con AWS PrivateLink](#)
- [Effettuare richieste tramite un punto di Multi-Region accesso](#)

Creazione di punti di Multi-Region accesso

Per creare un Multi-Region Access Point in Amazon S3, procedi come segue:

- Specifica il nome dell' Multi-Region Access Point.
- Scegli un bucket in ciascuno in Regione AWS cui desideri soddisfare le richieste per l' Multi-Region Access Point.
- Configura le impostazioni di Amazon S3 Block Public Access per l' Multi-Region Access Point.

Fornisci tutte queste informazioni in una richiesta di creazione, che Amazon S3 elabora in modo asincrono. Amazon S3 offre un token che consente di monitorare lo stato della richiesta di creazione asincrona.

Assicurati di risolvere avvisi di sicurezza, errori, avvisi generali e suggerimenti da AWS Identity and Access Management Access Analyzer prima di salvare la policy. IAM Access Analyzer esegue controlli della policy per convalidarla in rapporto alla [sintassi della policy](#) e alle [best practice](#) di IAM. Questi controlli generano risultati e forniscono suggerimenti utili per aiutarti a creare policy funzionali e conformi alle best practice per la sicurezza. Per ulteriori informazioni sulla convalida delle policy tramite IAM Access Analyzer, consulta [IAM Access Analyzer policy validation \(Convalida delle policy di IAM Access Analyzer\)](#) nella Guida per l'utente di IAM. Per visualizzare un elenco di avvisi, errori e suggerimenti di IAM Access Analyzer, consulta [Riferimento ai controlli delle policy IAM Access Analyzer](#).

Quando si utilizza l'API, la richiesta di creazione di un Multi-Region Access Point è asincrona. Quando invii una richiesta per creare un punto di Multi-Region accesso, Amazon S3 autorizza la richiesta in modo sincrono. Quindi restituisce immediatamente un token che consente di monitorare lo stato di avanzamento della richiesta di creazione. Per ulteriori informazioni sul monitoraggio delle richieste asincrone per creare e gestire punti di accesso, consulta. Multi-Region [Utilizzo Multi-Region degli access point con operazioni API supportate](#)

Dopo aver creato l' Multi-Region Access Point, è possibile creare una relativa policy di controllo degli accessi. Ogni Multi-Region Access Point può avere una policy associata. Una politica di Multi-Region Access Point è una politica basata sulle risorse che è possibile utilizzare per limitare l'uso dell' Multi-Region Access Point per risorsa, utente o altre condizioni.

Note

Affinché un'applicazione o un utente possa accedere a un oggetto tramite un Multi-Region Access Point, entrambe le seguenti politiche devono consentire la richiesta:

- La politica di accesso per l' Multi-Region Access Point
- La policy di accesso per il bucket sottostante contenente l'oggetto

Quando le due policy sono diverse, ha la precedenza quella più restrittiva. Per semplificare la gestione delle autorizzazioni per gli Multi-Region Access Point, puoi delegare il controllo degli accessi dal bucket all' Multi-Region Access Point. Per ulteriori informazioni, consulta [the section called “Multi-Region Esempi di politiche relative agli Access Point”](#).

L'utilizzo di un bucket con un Multi-Region Access Point non modifica il comportamento del bucket quando si accede al bucket tramite il nome del bucket esistente o un Amazon Resource Name (ARN). Tutte le operazioni esistenti inerenti il bucket continuano a funzionare come prima. Le restrizioni incluse in una policy di Multi-Region Access Point si applicano solo alle richieste effettuate tramite l'Access Point. Multi-Region

È possibile aggiornare la politica per un Multi-Region Access Point dopo averla creata, ma non è possibile eliminarla. Tuttavia, puoi aggiornare la politica dell' Multi-Region Access Point per negare tutte le autorizzazioni.

Argomenti

- [Regole per la denominazione degli Access Point di Amazon S3 Multi-Region](#)
- [Regole per la scelta dei bucket per i punti di accesso Amazon S3 Multi-Region](#)
- [Crea un punto di accesso Amazon S3 Multi-Region](#)
- [Blocco dell'accesso pubblico con i punti di accesso Amazon S3 Multi-Region](#)
- [Visualizzazione dei dettagli di configurazione degli Multi-Region Access Point di Amazon S3](#)
- [Eliminazione di un punto di Multi-Region accesso](#)

Regole per la denominazione degli Access Point di Amazon S3 Multi-Region

Quando crei un Multi-Region Access Point, gli dai un nome, che è una stringa che scegli. Non è possibile modificare il nome dell' Multi-Region Access Point dopo averlo creato. Il nome deve essere univoco nel tuo Account AWS e deve essere conforme ai requisiti di denominazione elencati in [Multi-Region Restrizioni e limitazioni dell'Access Point](#). Per aiutarti a identificare l' Multi-Region Access Point, utilizza un nome significativo per te, per la tua organizzazione o che rifletta lo scenario.

Si utilizza questo nome quando si richiamano operazioni di gestione degli Multi-Region Access Point, ad esempio `eGetMultiRegionAccessPoint`. `PutMultiRegionAccessPointPolicy` Il nome

non viene utilizzato per inviare richieste all' Multi-Region Access Point e non deve essere esposto ai client che effettuano richieste utilizzando l' Multi-Region Access Point.

Quando Amazon S3 crea un Multi-Region Access Point, gli assegna automaticamente un alias. Questo alias è una stringa alfanumerica univoca che termina in `.mr.ap`. L'alias viene utilizzato per creare il nome host e l'Amazon Resource Name (ARN) per un Access Point. Multi-Region Il nome completo si basa anche sull'alias dell'Access Point. Multi-Region

Non è possibile determinare il nome di un Multi-Region Access Point in base al relativo alias, quindi è possibile divulgare un alias senza rischiare di rivelare il nome, lo scopo o il proprietario dell'Access Point. Multi-Region Amazon S3 seleziona l'alias per ogni nuovo Multi-Region Access Point e l'alias non può essere modificato. Per ulteriori informazioni sull'indirizzamento a un Multi-Region Access Point, consulta. [Effettuare richieste tramite un punto di Multi-Region accesso](#)

Multi-Region Gli alias degli Access Point sono unici nel tempo e non si basano sul nome o sulla configurazione di un Multi-Region Access Point. Se si crea un Multi-Region Access Point, quindi lo si elimina e se ne crea un altro con lo stesso nome e configurazione, il secondo Multi-Region Access Point avrà un alias diverso dal primo. I nuovi Multi-Region Access Point non possono mai avere lo stesso alias di un Multi-Region Access Point precedente.

Regole per la scelta dei bucket per i punti di accesso Amazon S3 Multi-Region

Ogni Multi-Region Access Point è associato alle regioni in cui desideri soddisfare le richieste. L' Multi-Region Access Point deve essere associato esattamente a un bucket in ciascuna di queste regioni. Specificate il nome di ogni bucket nella richiesta per creare l' Multi-Region Access Point. I bucket che supportano l' Multi-Region Access Point possono trovarsi nello stesso Account AWS proprietario dell' Multi-Region Access Point oppure in un altro. Account AWS

Un singolo bucket può essere utilizzato da più Multi-Region Access Point.

Important

- È possibile specificare i bucket associati a un Multi-Region Access Point solo nel momento in cui lo si crea. Una volta creato, non è possibile aggiungere, modificare o rimuovere i bucket dalla configurazione dell' Multi-Region Access Point. Per modificare i bucket, è necessario eliminare l'intero Multi-Region Access Point e crearne uno nuovo.
- Non è possibile eliminare un bucket che fa parte di un Multi-Region Access Point. Se desideri eliminare un bucket collegato a un Multi-Region Access Point, elimina prima l' Multi-Region Access Point.

- Se aggiungi un bucket di proprietà di un altro account al tuo Multi-Region Access Point, il proprietario del bucket deve inoltre aggiornare la propria politica del bucket per concedere le autorizzazioni di accesso all'Access Point. Multi-Region Altrimenti, l' Multi-Region Access Point non sarà in grado di recuperare i dati da quel bucket. Ad esempio, le politiche che mostrano come concedere tale accesso, vedi Esempi di politiche per gli [Multi-Region Access Point](#).
- Non tutte le regioni supportano gli Multi-Region Access Point. Per vedere l'elenco delle regioni supportate, consulta [Multi-Region Restrizioni e limitazioni dell'Access Point](#).

Puoi creare regole di replica per sincronizzare i dati tra i bucket. Queste regole consentono di copiare automaticamente i dati dai bucket di origine ai bucket di destinazione. La connessione dei bucket a un Multi-Region Access Point non influisce sul funzionamento della replica. La configurazione della replica con gli Multi-Region Access Points è descritta in una sezione successiva.

Important

Quando si effettua una richiesta a un Multi-Region Access Point, quest' Multi-Region ultimo non è a conoscenza del contenuto di dati dei bucket nell' Multi-Region Access Point. Pertanto, il bucket che riceve la richiesta potrebbe non contenere i dati richiesti. Per creare set di dati coerenti nei bucket Amazon S3 associati a un Multi-Region Access Point, ti consigliamo di configurare S3 Cross-Region Replication (CRR). Per ulteriori informazioni, consulta [Configurazione della replica per l'utilizzo con punti di accesso multi-regione](#).

Crea un punto di accesso Amazon S3 Multi-Region

L'esempio seguente dimostra come creare un Multi-Region Access Point utilizzando la console Amazon S3.

Utilizzo della console S3

Per creare un Access Point Multi-Region

Note

Multi-Region Le regioni con attivazione degli Access Point non sono attualmente supportate nella console Amazon S3.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso).
3. Scegli Crea punti di Multi-Region accesso per iniziare a creare il tuo punto di Multi-Region accesso.
4. Nella pagina Multi-Region Access Point, inserisci un nome per l' Multi-Region Access Point nel campo Nome Multi-Region Access Point.
5. Seleziona i bucket che verranno associati a questo Multi-Region Access Point. Puoi scegliere i bucket che si trovano nel tuo account oppure puoi scegliere i bucket da altri account.

 Note

Devi aggiungere almeno un bucket dal tuo account o da altri account. Inoltre, tieni presente che gli Multi-Region Access Point supportano solo un bucket per. Regione AWS Pertanto, non puoi aggiungere due bucket dalla stessa regione. Non sono supportate le [Regioni AWS disattivate per impostazione predefinita](#).

- Per aggiungere un bucket presente nel tuo account, scegli Aggiungi bucket. Viene visualizzato un elenco dei bucket disponibili nel tuo account. Puoi cercare il tuo bucket per nome o ordinare i nomi dei bucket in ordine alfabetico.
- Per aggiungere un bucket da un altro account, scegli Aggiungi bucket da altri account. Assicurati di conoscere il nome e l' Account AWS ID esatti del bucket perché non puoi cercare o sfogliare i bucket in altri account.

 Note

Devi inserire un Account AWS ID e un nome del bucket validi. Il bucket deve inoltre trovarsi in una regione supportata, altrimenti si verificherà un errore quando proverai a creare il tuo Multi-Region Access Point. Per l'elenco delle regioni che supportano i punti di Multi-Region accesso, vedi Restrizioni e limitazioni dei [punti di](#) Multi-Region accesso.

6. (Facoltativo) Se devi rimuovere un bucket aggiunto, scegli Rimuovi.

 Note

Non puoi aggiungere o rimuovere bucket a questo Multi-Region Access Point dopo averlo creato.

7. In Blocca impostazioni di accesso pubblico per questo punto di Multi-Region accesso, seleziona le impostazioni di blocco dell'accesso pubblico che desideri applicare all' Multi-Region Access Point. Per impostazione predefinita, tutte le impostazioni di Blocca accesso pubblico sono abilitate per i nuovi punti di Multi-Region accesso. È consigliabile lasciare tutte le impostazioni abilitate, a meno che tu non debba necessariamente disabilitarne una specifica.

 Note

Non è possibile modificare le impostazioni di blocco dell'accesso pubblico per un punto di Multi-Region accesso dopo che il punto di Multi-Region accesso è stato creato. Pertanto, se intendi bloccare l'accesso pubblico, assicurati che le tue applicazioni funzionino correttamente senza accesso pubblico prima di creare un punto di Multi-Region accesso.

8. Scegli Crea punto di Multi-Region accesso.

 Important

Quando aggiungi un bucket di proprietà di un altro account al tuo Multi-Region Access Point, il proprietario del bucket deve anche aggiornare la propria politica del bucket per concedere le autorizzazioni di accesso all'Access Point. Multi-Region Altrimenti, l' Multi-Region Access Point non sarà in grado di recuperare i dati da quel bucket. Ad esempio, le politiche che mostrano come concedere tale accesso, vedi Esempi di politiche per gli [Multi-Region Access Point](#).

Utilizzo di AWS CLI

È possibile utilizzare il AWS CLI per creare un punto di Multi-Region accesso. Quando si crea l' Multi-Region Access Point, è necessario fornire tutti i bucket che supporterà. Non è possibile aggiungere bucket all' Multi-Region Access Point dopo averlo creato.

L'esempio seguente crea un Multi-Region Access Point con due bucket utilizzando il. AWS CLI. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Note

Per creare un Multi-Region Access Point utilizzando i bucket in una regione opt-in, assicurati di [abilitare prima tutte le regioni opt-in](#). Altrimenti, riceverai un 403 `InvalidRegion` messaggio di errore quando proverai a creare un Multi-Region Access Point utilizzando i bucket per una regione con opt-in a cui non hai effettivamente aderito.

```
aws s3control create-multi-region-access-point --account-id 111122223333 --details '{
  "Name": "simple-multiregionaccesspoint-with-two-regions",
  "PublicAccessBlock": {
    "BlockPublicAcls": true,
    "IgnorePublicAcls": true,
    "BlockPublicPolicy": true,
    "RestrictPublicBuckets": true
  },
  "Regions": [
    { "Bucket": "amzn-s3-demo-bucket1" },
    { "Bucket": "amzn-s3-demo-bucket2" }
  ]
}' --region us-west-2
```

Blocco dell'accesso pubblico con i punti di accesso Amazon S3 Multi-Region

Ogni Multi-Region Access Point ha impostazioni distinte per Amazon S3 Block Public Access. Queste impostazioni funzionano insieme alle impostazioni Block Public Access per il proprietario dell'Account AWS Multi-Region Access Point e dei bucket sottostanti.

Quando Amazon S3 autorizza una richiesta, applica la combinazione più restrittiva di queste impostazioni. Se le impostazioni Block Public Access per una di queste risorse (l'account del proprietario dell' Multi-Region Access Point, il bucket sottostante o l'account del proprietario del bucket) bloccano l'accesso all'azione o alla risorsa richiesta, Amazon S3 rifiuta la richiesta.

È consigliabile abilitare tutte le impostazioni di blocco dell'accesso pubblico a meno che non sia necessario disabilitarne alcune. Per impostazione predefinita, tutte le impostazioni di Block Public

Access sono abilitate per un Access Point. Multi-Region Se l'opzione Blocca accesso pubblico è abilitata, l' Multi-Region Access Point non può accettare richieste basate su Internet.

 Important

Non è possibile modificare le impostazioni di blocco dell'accesso pubblico per un punto di Multi-Region accesso dopo che è stato creato.

Per ulteriori informazioni sul blocco dell'accesso pubblico in Amazon S3, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Visualizzazione dei dettagli di configurazione degli Multi-Region Access Point di Amazon S3

L'esempio seguente dimostra come visualizzare i dettagli di configurazione dell' Multi-Region Access Point utilizzando la console Amazon S3.

Utilizzo della console S3

Per creare un Access Point Multi-Region

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso).
3. Scegli il nome dell' Multi-Region Access Point di cui desideri visualizzare i dettagli di configurazione.
 - La scheda Proprietà elenca tutti i bucket associati al tuo Multi-Region Access Point, la data di creazione, l'Amazon Resource Name (ARN) e l'alias. La colonna Account AWS ID elenca anche tutti i bucket di proprietà di account esterni associati al tuo Multi-Region Access Point.
 - La scheda Autorizzazioni elenca le impostazioni di blocco dell'accesso pubblico applicate ai bucket associati a questo Multi-Region Access Point. Puoi anche visualizzare la politica dell' Multi-Region Access Point per il tuo Multi-Region Access Point, se ne hai creata una. L'avviso Info nella pagina Autorizzazioni elenca anche tutti i bucket (nel tuo account e in altri account) per questo Multi-Region Access Point per cui è abilitata l'impostazione Accesso pubblico bloccato.

- La scheda Replica e failover fornisce una mappa dei bucket associati al punto di Multi-Region accesso e delle regioni in cui risiedono i bucket. Se sono presenti bucket di un altro account per i quali non disponi delle autorizzazioni per estrarre i dati, la regione verrà contrassegnata in rosso sulla mappa Riepilogo della replica, a indicare che si tratta di una Regione AWS che ha generato errori durante il recupero dello stato della replica.

Note

Per recuperare le informazioni sullo stato della replica da un bucket in un account esterno, il proprietario del bucket deve concederti l'autorizzazione `s3:GetBucketReplication` nella propria policy dei bucket.

Questa scheda fornisce anche le metriche di replica, le regole di replica e gli stati di failover per le regioni utilizzate con l'Access Point. Multi-Region

Utilizzo di AWS CLI

È possibile utilizzare il AWS CLI per visualizzare i dettagli di configurazione di un Access Point. Multi-Region

L' AWS CLI esempio seguente ottiene la configurazione corrente dell' Multi-Region Access Point. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control get-multi-region-access-point --account-id 111122223333 --name amzn-s3-demo-bucket
```

Eliminazione di un punto di Multi-Region accesso

La procedura seguente spiega come eliminare un Multi-Region Access Point utilizzando la console Amazon S3. Tieni presente che l'eliminazione di un Multi-Region Access Point non elimina i bucket associati all' Multi-Region Access Point. Invece, elimina solo l' Multi-Region Access Point stesso.

Note

Gli Multi-Region Access Point S3 che utilizzano bucket nelle regioni AWS opt-in sono attualmente supportati solo tramite AWS SDK e CLI. AWS Per eliminare un Multi-Region

Access Point utilizzando i bucket in una regione opt-in, assicurati di specificare quali regioni AWS opt-in può utilizzare per prime il tuo account. Altrimenti, se provi a eliminare un Multi-Region Access Point che utilizza bucket in regioni con AWS opt-in disabilitato, riceverai un messaggio di errore.

Utilizzo della console S3

Per eliminare un punto di accesso Multi-Region

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso).
3. Seleziona il pulsante di opzione accanto al nome del tuo Multi-Region Access Point.
4. Scegliere Elimina.
5. Nella finestra di dialogo Elimina punto di Multi-Region accesso, inserisci il nome del AWS bucket che desideri eliminare.

Note

Assicurati di inserire un nome valido per il bucket. In caso contrario, il pulsante Elimina verrà disabilitato.

6. Scegli Elimina per confermare l'eliminazione del tuo Multi-Region Access Point.

Utilizzo di AWS CLI

È possibile utilizzare il AWS CLI per eliminare un punto di Multi-Region accesso. Questa azione non elimina i bucket associati all' Multi-Region Access Point, ma solo l' Multi-Region Access Point stesso. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control delete-multi-region-access-point --account-id 123456789012 --details  
Name=example-multi-region-access-point-name
```

Configurazione di un punto di accesso multiregionale da utilizzare con AWS PrivateLink

Puoi utilizzare i punti di accesso multi-regione per instradare il traffico delle richieste Amazon S3 tra Regioni AWS. Ogni endpoint globale del punto di accesso multi-regione instrada il traffico delle richieste di dati Amazon S3 da più fonti senza dover creare configurazioni di rete complesse con endpoint distinti. Queste origini del traffico delle richieste di dati includono:

- Traffico con origine in un cloud privato virtuale (VPC)
- Il traffico proveniente dai data center locali viaggia attraverso AWS PrivateLink
- Traffico proveniente dalla rete Internet pubblica

Se stabilisci una AWS PrivateLink connessione a un punto di accesso multiregionale S3, puoi instradare le richieste S3 verso AWS, o tra più Regioni AWS, tramite una connessione privata utilizzando una semplice architettura e configurazione di rete. Quando si utilizza AWS PrivateLink, non è necessario configurare una connessione peering VPC.

Argomenti

- [Configurazione delle Regioni con consenso esplicito con punti di accesso multi-Regione](#)
- [Configurazione di un Multi-Region Access Point da utilizzare con AWS PrivateLink](#)
- [Rimozione dell'accesso a un punto di accesso multi-regione da un endpoint VPC](#)

Configurazione delle Regioni con consenso esplicito con punti di accesso multi-Regione

Una regione AWS opt-in è una regione che non è abilitata per impostazione predefinita nel tuo AWS account. Al contrario, le regioni abilitate per impostazione predefinita sono note come Regioni AWS regioni commerciali.

Per iniziare a utilizzare i punti di accesso multiregionali nelle regioni AWS opzionali, devi abilitare manualmente la regione opt-in per il tuo AWS account prima di creare il punto di accesso multiregionale. Dopo aver abilitato la Regione con consenso esplicito, è possibile creare i punti di accesso multi-Regione con bucket presenti nella Regione con consenso esplicito selezionata. Per istruzioni su come abilitare o disabilitare una regione opzionale per il tuo AWS account o la tua AWS organizzazione, vedi [Abilitare o disabilitare una regione per gli account autonomi](#) o [Abilitare o disabilitare](#) una regione nell'organizzazione.

 Note

Le regioni con accesso a punti di accesso multiregionali sono attualmente supportate solo tramite `awscli` e `AWS SDKs`.

I punti di accesso multiregionali S3 supportano le seguenti regioni opzionali: AWS

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Jakarta)
- Asia Pacific (Melbourne)
- Asia Pacific (Hyderabad)
- Canada West (Calgary)
- Europe (Zurich)
- Europe (Milan)
- Europe (Spain)
- Israel (Tel Aviv)
- Middle East (Bahrain)
- Middle East (UAE)

 Note

Non sono previsti costi aggiuntivi per l'abilitazione di una Regione con consenso esplicito. Tuttavia, la creazione o l'utilizzo di una risorsa tramite un punto di accesso multi-Regione comporta dei costi di fatturazione.

Utilizzo di un punto di accesso multiregionale in una regione con attivazione AWS

Per eseguire un'[operazione sul piano dati](#) sul punto di accesso multiregionale, tutti gli AWS account associati devono abilitare le regioni opt-in che fanno parte del punto di accesso multiregionale. Questo requisito si applica all'account richiedente, al proprietario del punto di accesso multi-Regione, ai proprietari del bucket S3 e al proprietario dell'endpoint VPC. Se uno di questi account non abilita

le Regioni AWS con consenso esplicito, le richieste dei punti di accesso multi-Regione hanno esito negativo. Per ulteriori informazioni sugli errori `InvalidToken` o `AllAccessDisabled`, consulta [Elenco dei codici di errore](#).

Note

[Le operazioni del piano di controllo \(control-plane\)](#), come l'aggiornamento della policy dei punti di accesso multi-Regione o l'aggiornamento della configurazione del failover, non sono influenzate dallo stato della Regione con consenso esplicito di una Regione che fa parte del punto di accesso multi-Regione. Inoltre, non è necessario disabilitare alcuna Regione con consenso esplicito attiva prima di eliminare un punto di accesso multi-Regione.

Disattivazione di una regione con opt-in attivo AWS

Se si disabilita una Regione con consenso esplicito che fa parte del punto di accesso multi-Regione, le richieste indirizzate a questa Regione generano un errore `403 AllAccessDisabled`. Per disabilitare in modo sicuro una Regione con consenso esplicito, è consigliabile individuare prima una Regione alternativa nella configurazione del punto di accesso multi-Regione verso cui indirizzare il traffico. È quindi possibile utilizzare i controlli di failover del punto di accesso multi-Regione per contrassegnare la Regione alternativa come attiva e la Regione da disabilitare come passiva. Dopo aver modificato i controlli di failover, è possibile disabilitare la Regione con consenso esplicito.

Attivazione di una regione di AWS opt-in precedentemente disabilitata

Per abilitare una AWS regione di attivazione precedentemente disattivata per il punto di accesso multiregionale, assicurati di aggiornare le impostazioni dell'account AWS . Dopo aver riabilitato la Regione con consenso esplicito, esegui l'operazione API [PutMultiRegionAccessPointPolicy](#) per applicare la policy dei punti di accesso multi-Regione alla regione con consenso esplicito.

Se si accede al punto di accesso multiregionale tramite un endpoint VPC, si consiglia di aggiornare la politica VPCE e utilizzare l'operazione API per applicare [ModifyVpcEndpoint](#) la politica degli endpoint VPC aggiornata alla regione di opt-in riabilitata.

Politica sui punti di accesso multiregionali e account multipli AWS

Se la politica relativa ai punti di accesso multiregionali consente l'accesso a più AWS account, tutti gli account richiedenti devono inoltre abilitare le stesse regioni di opt-in nelle impostazioni dell'account. Se l'account richiedente invia una richiesta di punto di accesso multi-Regione senza abilitare le

Regioni con consenso esplicito che fanno parte del punto di accesso multi-Regione, viene generato un errore 400 `InvalidToken`.

AWS considerazioni relative alla regione che prevede l'opt-in

Quando si accede a un punto di accesso multi-Regione da una Regione con consenso esplicito, è opportuno tenere presente quanto segue:

- Quando si abilita una Regione con consenso esplicito, è possibile creare un punto di accesso multi-Regione utilizzando i bucket della Regione con consenso esplicito. Quando si disabilita una Regione con consenso esplicito, il punto di accesso multi-Regione non è più supportato nella Regione con consenso esplicito. Per disabilitare una Regione con consenso esplicito per il punto di accesso multi-Regione, è necessario prima [disabilitare la Regione nell'account](#). Quindi si crea un nuovo punto di accesso multi-Regione con l'elenco preferito di Regioni con consenso esplicito.
- Se si tenta di creare un punto di accesso multi-Regione con una Regione con consenso esplicito disabilitata, viene generato un errore 403 `InvalidRegion`. Dopo aver abilitato la Regione con consenso esplicito, è possibile creare nuovamente il punto di accesso multi-Regione.
- Il numero massimo di Regioni supportate per un punto di accesso multi-Regione è di 17 Regioni. Sono incluse sia le Regioni con consenso esplicito che le Regioni commerciali. Per ulteriori informazioni, consulta [Restrizioni e limitazioni dei punti di accesso multi-Regione](#).
- Le richieste del piano di controllo (control-plane) per punti di accesso multi-Regione funzionano anche se non è abilitata alcuna Regione con consenso esplicito.
- Quando si crea un punto di accesso multi-Regione per la prima volta, è necessario abilitare tutte le Regioni con consenso esplicito che fanno parte del punto di accesso multi-Regione.
- Tutti AWS gli account a cui è concesso l'accesso a un punto di accesso multiregionale S3 tramite la politica relativa ai punti di accesso multiregionali devono abilitare anche le stesse regioni opt-in che fanno parte del punto di accesso multiregionale.

Configurazione di un Multi-Region Access Point da utilizzare con AWS PrivateLink

AWS PrivateLink ti fornisce una connettività privata ad Amazon S3 utilizzando indirizzi IP privati nel tuo cloud privato virtuale (VPC). Puoi effettuare il provisioning di uno o più endpoint di interfaccia all'interno del tuo VPC per connetterti agli access point di Amazon S3. Multi-Region

Puoi creare endpoint `com.amazonaws.s3-global.accesspoint` per gli access point tramite, o SDK. Multi-Region Console di gestione AWS AWS CLI AWS Per saperne di più su come configurare un

endpoint di interfaccia per Access Point, consulta [Interface VPC endpoint nella Guida per l' Multi-Region utente VPC](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html). <https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html>

Per effettuare richieste a un Multi-Region Access Point tramite gli endpoint di interfaccia, segui questi passaggi per configurare il VPC e l'Access Point. Multi-Region

Per configurare un Multi-Region Access Point da utilizzare con AWS PrivateLink

1. Crea o disponi di un endpoint VPC appropriato in grado di connettersi agli Multi-Region Access Point. Per ulteriori informazioni sulla creazione di endpoint VPC, consulta [Endpoint VPC di interfaccia](#) nella Guida per l'utente di VPC.

 Important

Assicurati di creare un endpoint `com.amazonaws.s3-global.accesspoint`. Altri tipi di endpoint non possono accedere agli access Multi-Region point.

Dopo la creazione di questo endpoint VPC, tutte le richieste di Multi-Region Access Point nel VPC vengono indirizzate a questo endpoint se il DNS privato è abilitato per l'endpoint. Questo è abilitato per impostazione predefinita.

2. Se la policy dell' Multi-Region Access Point non supporta le connessioni dagli endpoint VPC, sarà necessario aggiornarla.
3. Verifica che le singole policy dei bucket consentano l'accesso agli utenti dell' Multi-Region Access Point.

Ricorda che gli Multi-Region Access Point funzionano indirizzando le richieste ai bucket, non soddisfacendo le richieste stesse. Questo è importante da ricordare perché l'originatore della richiesta deve disporre delle autorizzazioni per l' Multi-Region Access Point e poter accedere ai singoli bucket dell'Access Point. Multi-Region In caso contrario, la richiesta potrebbe essere instradata a un bucket in cui l'origine non dispone delle autorizzazioni per soddisfare la richiesta. Un Multi-Region Access Point e i bucket associati possono essere di proprietà dello stesso o di un altro account. AWS Tuttavia, i VPC di account diversi possono utilizzare un Multi-Region Access Point se le autorizzazioni sono configurate correttamente.

Per questo motivo, la policy degli endpoint VPC deve consentire l'accesso sia all' Multi-Region Access Point che a ciascun bucket sottostante che si desidera sia in grado di soddisfare le richieste. Ad esempio, supponiamo di avere un Multi-Region Access Point con l'alias `mfzwi23gnjvgw.mrap`

È supportato dai bucket `amzn-s3-demo-bucket1` e `amzn-s3-demo-bucket2`, tutti di proprietà dell'account AWS `123456789012`. In questo caso, le seguenti policy dell'endpoint VPC consente ai bucket di supporto di soddisfare le richieste `GetObject` dal VPC fatte a `mfzwi23gnjvgw.mrap`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Read-buckets-and-MRAP-VPCE-policy",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        "arn:aws:s3:::amzn-s3-demo-bucket2/*",
        "arn:aws:s3:::111122223333:accesspoint/mfzwi23gnjvgw.mrap/object/*"
      ]
    }
  ]
}
```

Come accennato in precedenza, è inoltre necessario assicurarsi che la policy dell' Multi-Region Access Point sia configurata per supportare l'accesso tramite un endpoint VPC. Non è necessario specificare l'endpoint VPC che richiede l'accesso. La seguente politica di esempio concederebbe l'accesso a qualsiasi richiedente che tenti di utilizzare l' Multi-Region Access Point per le richieste. `GetObject`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Open-read-MRAP-policy",
      "Effect": "Allow",
      "Principal": "*",
```

```
    "Action": [
      "s3:GetObject"
    ],
    "Resource": "arn:aws:s3::111122223333:accesspoint/mfzwi23gnjvgw.mrap/
object/*"
  ]
}
```

E, naturalmente, i singoli bucket avrebbero bisogno di una policy per supportare l'accesso delle richieste inviate tramite l'endpoint VPC. La seguente politica di esempio concede l'accesso in lettura a qualsiasi utente anonimo. Ciò includerebbe le richieste effettuate tramite l'endpoint VPC.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Public-read",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket1",
        "arn:aws:s3::amzn-s3-demo-bucket2/*"
      ]
    }
  ]
}
```

Per informazioni sulla modifica di una policy dell'endpoint VPC, consulta [Controllare l'accesso ai servizi con endpoint VPC](#) nella Guida per l'utente di VPC.

Rimozione dell'accesso a un punto di accesso multi-regione da un endpoint VPC

Se sei proprietario di un punto di accesso multi-regione e desideri rimuovere l'accesso a tale punto da un endpoint di interfaccia, devi specificare una nuova policy di accesso per il punto di accesso multi-regione che impedisca l'accesso alle richieste provenienti dagli endpoint VPC. Tuttavia, se i bucket nel punto di accesso multi-regione supportano le richieste tramite endpoint VPC, essi continueranno a supportarle. Se desideri impedire il supporto, devi aggiornare anche le policy dei

bucket. L'impostazione di una nuova policy di accesso al punto di accesso multi-regione impedisce l'accesso solo a tale punto di accesso e non ai bucket sottostanti.

Note

Non puoi eliminare una policy di accesso per un punto di accesso multi-area. Per rimuovere l'accesso a un punto di accesso multi-area, devi fornire una nuova policy di accesso con l'accesso modificato come desideri.

Invece di aggiornare la policy di accesso per il punto di accesso multi-regione, puoi aggiornare le policy di bucket per impedire le richieste tramite gli endpoint VPC. In questo caso, gli utenti potrebbero comunque accedere al punto di accesso multi-regione tramite l'endpoint VPC. Tuttavia, se viene instradata a un bucket la cui policy impedisce l'accesso, la richiesta al punto di accesso multi-regione genera un messaggio di errore.

Effettuare richieste tramite un punto di Multi-Region accesso

Come altre risorse, gli Multi-Region Access Point di Amazon S3 dispongono di Amazon Resource Names (ARN). Puoi utilizzare questi ARN per indirizzare le richieste agli Multi-Region Access Point utilizzando AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API Amazon S3. Puoi anche utilizzare questi ARN per identificare i punti di accesso nelle politiche di Multi-Region controllo degli accessi. L'ARN di un Multi-Region Access Point non include né rivela il nome dell' Multi-Region Access Point. Per ulteriori informazioni sull'utilizzo degli ARN, consulta [Amazon Resource Name \(ARN\)](#) nella Riferimenti generali di AWS.

Note

L'alias Multi-Region Access Point e l'ARN non possono essere usati in modo intercambiabile.

Multi-Region Gli Access Point ARN utilizzano il seguente formato:

`arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias`

Di seguito sono riportati alcuni esempi di Multi-Region Access Point ARN:

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw`.mrappresenta l' Multi-Region Access Point con l'alias `mfzwi23gnjvgw.mrap`, di proprietà di. Account AWS 123456789012

- `arn:aws:s3::123456789012:accesspoint/*` rappresenta tutti i punti di Multi-Region accesso dell'account 123456789012. Questo ARN corrisponde a tutti gli Multi-Region Access Point per account 123456789012, ma non corrisponde a nessun punto di accesso Amazon S3 regionale perché l'ARN non include un. Regione AWS Al contrario, l'ARN `arn:aws:s3:us-west-2:123456789012:accesspoint/*` corrisponde a tutti i punti di accesso Amazon S3 regionali nella us-west-2 regione dell'123456789012account, ma non corrisponde Multi-Region a nessun punto di accesso.

Gli ARN per gli oggetti a cui si accede tramite un punto di Multi-Region accesso utilizzano il seguente formato:

`arn:aws:s3::account_id:accesspoint/MultiRegionAccessPoint_alias//key`

Come per gli Multi-Region Access Point ARN, gli ARN per gli oggetti a cui si accede tramite Multi-Region Access Point non includono un. Regione AWS Ecco alcuni esempi.

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01` rappresenta l'oggetto con chiave -01, a cui si accede tramite l' Multi-Region Access Point con l'alias `mfzwi23gnjvgw.mrap`, di proprietà dell'account. 123456789012
- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap/*` rappresenta tutti gli oggetti a cui è possibile accedere tramite l' Multi-Region Access Point con l'alias `mfzwi23gnjvgw.mrap`, in account. 123456789012
- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01/finance/` *rappresenta tutti gli oggetti a cui è possibile accedere tramite -01/finance/ l' Multi-Region Access Point con l'alias `mfzwi23gnjvgw.mrap`, in account. 123456789012

Multi-Region nomi host degli Access Point

Puoi accedere ai dati in Amazon S3 tramite un punto di Multi-Region accesso utilizzando il nome host del punto di accesso. Multi-Region Le richieste possono essere indirizzate a questo nome host dalla rete Internet pubblica. Se hai configurato uno o più gateway Internet per l' Multi-Region Access Point, le richieste possono anche essere indirizzate a questo nome host da un cloud privato virtuale (VPC). Per ulteriori informazioni sulla creazione di endpoint di interfaccia VPC da utilizzare con gli Multi-Region Access Point, consulta. [Configurazione di un Multi-Region Access Point da utilizzare con AWS PrivateLink](#)

Per effettuare richieste tramite un punto di Multi-Region accesso da un VPC utilizzando un endpoint VPC, puoi usare AWS PrivateLink. Quando si effettuano richieste a un punto di Multi-Region accesso utilizzando AWS PrivateLink, non è possibile utilizzare direttamente un nome DNS (Regional DOMAIN NAME SYSTEM) specifico dell'endpoint che termina con `region.vpce.amazonaws.com`. Questo nome host non ha un certificato associato ad esso, quindi non può essere utilizzato direttamente. Puoi comunque utilizzare il sistema dei nomi di dominio (DNS) pubblico dell'endpoint VPC come destinazione di CNAME o ALIAS. In alternativa, puoi abilitare il DOMAIN NAME SYSTEM (DNS) privato sull'endpoint e utilizzare il nome DNS (`MultiRegionAccessPoint_alias.accesspoint.s3-global.amazonaws.com` DOMAIN NAME SYSTEM) standard del punto di Multi-Region accesso, come descritto in questa sezione.

Quando effettui richieste all'API per le operazioni sui dati di Amazon S3 (ad esempio `GetObject`) tramite un punto di Multi-Region accesso, il nome host per la richiesta è il seguente:

`MultiRegionAccessPoint_alias.accesspoint.s3-global.amazonaws.com`

Ad esempio, per effettuare una `GetObject` richiesta tramite il Multi-Region Access Point con l'alias `mfzwi23gnjvgw.mrap`, fai una richiesta al nome host `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`. La porzione `s3-global` del nome host indica che questo nome host non è per una regione specifica.

Effettuare richieste tramite un punto di Multi-Region accesso è simile a effettuare richieste tramite un punto di accesso a regione singola. È tuttavia importante essere consapevoli delle seguenti differenze:

- Multi-Region Gli Access Point ARN non includono un. Regione AWS Seguono il formato `arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias`.
- Per le richieste effettuate tramite operazioni API (queste richieste non richiedono l'uso di un ARN), gli Multi-Region Access Point utilizzano uno schema di endpoint diverso. Lo schema è `MultiRegionAccessPoint_alias.accesspoint.s3-global.amazonaws.com`, ad esempio `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`. Nota le differenze rispetto a un punto di accesso a una regione singola:
 - Multi-Region I nomi host degli Access Point utilizzano il proprio alias, non il nome dell' Multi-Region Access Point.
 - Multi-Region I nomi host degli Access Point non includono l'ID del proprietario. Account AWS
 - Multi-Region I nomi host degli Access Point non includono un. Regione AWS
 - Multi-Region I nomi host degli Access Point includono `s3-global.amazonaws.com` invece di `s3.amazonaws.com`

- Multi-Region Le richieste di Access Point devono essere firmate utilizzando Signature Version 4A (SigV4a). Quando utilizzi gli AWS SDK, l'SDK converte automaticamente un SigV4 in SigV4A. Verifica pertanto che l'[SDK AWS supporti](#) il formato SigV4a come implementazione di firma utilizzata per firmare le richieste globali a livello di Regione AWS . [Per ulteriori informazioni su SigV4a, consulta Firmare le richieste API in. AWS](#)[Riferimenti generali di AWS](#)

Multi-Region Punti di accesso e Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration è una caratteristica che abilita trasferimenti di dati più rapidi a bucket. Transfer Acceleration è configurato a livello di singolo bucket. Per ulteriori informazioni su Transfer Acceleration, consulta [Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#).

Multi-Region Gli access point utilizzano un meccanismo di trasferimento accelerato simile a quello di Transfer Acceleration per l'invio di oggetti di grandi dimensioni sulla rete. AWS Per questo motivo, non è necessario utilizzare Transfer Acceleration quando si inviano richieste tramite un Multi-Region punto di accesso. Queste prestazioni di trasferimento migliorate vengono automaticamente incorporate nell' Multi-Region Access Point.

Argomenti

- [Permissions](#)
- [Multi-Region Restrizioni e limitazioni dell'Access Point](#)
- [Instradamento della richiesta tramite punto di accesso multi-regione](#)
- [Controlli di failover dei punti di Multi-Region accesso Amazon S3](#)
- [Configurazione della replica per l'utilizzo con punti di accesso multi-regione](#)
- [Utilizzo Multi-Region degli access point con operazioni API supportate](#)
- [Monitoraggio e registrazione delle richieste effettuate tramite un punto di accesso multi-regione alle risorse sottostanti](#)

Permissions

Gli Multi-Region Access Point di Amazon S3 possono semplificare l'accesso ai dati per bucket Amazon S3 in più bucket. Regioni AWS Multi-Region Gli access point sono denominati endpoint globali che puoi utilizzare per eseguire operazioni sugli oggetti di accesso ai dati di Amazon S3, come e. GetObject PutObject Ogni Multi-Region Access Point può avere autorizzazioni e controlli di rete distinti per qualsiasi richiesta effettuata tramite l'endpoint globale.

Ogni Multi-Region Access Point può anche applicare una politica di accesso personalizzata che funziona insieme alla policy del bucket collegata al bucket sottostante. Affinché una richiesta tra account abbia esito positivo, le seguenti policy devono consentire l'operazione:

- La politica degli Access Point Multi-Region
- La politica sottostante AWS Identity and Access Management (IAM)
- Policy di bucket sottostante (a cui viene indirizzata la richiesta)

Note

Per le richieste relative allo stesso account, è necessaria solo la policy IAM sottostante, che garantisce l'accesso appropriato.

È possibile configurare qualsiasi policy di Multi-Region Access Point per accettare richieste solo da utenti o gruppi IAM specifici. Per un esempio su come eseguire questa operazione, consulta l'esempio 2 in [the section called “Multi-Region Esempi di politiche relative agli Access Point”](#). Per limitare l'accesso ai dati di Amazon S3 a una rete privata, puoi configurare la policy Multi-Region Access Point in modo che accetti richieste solo da un cloud privato virtuale (VPC).

Ad esempio, supponiamo di effettuare una `GetObject` richiesta tramite un Multi-Region Access Point utilizzando un utente chiamato `AppDataReader` nel tuo account. AWS Per garantire che la richiesta non venga rifiutata, `AppDataReader` all'utente deve essere concessa l'`s3:GetObject` autorizzazione dall' Multi-Region Access Point e da ogni bucket sottostante l' Multi-Region Access Point. `AppDataReader` non sarà in grado di recuperare dati da nessun bucket che non concede questa autorizzazione.

Important

La delega del controllo di accesso per un bucket a una policy di Multi-Region Access Point non modifica il comportamento del bucket quando si accede al bucket direttamente tramite il nome del bucket o Amazon Resource Name (ARN). Tutte le operazioni eseguite direttamente sul bucket continueranno a funzionare come prima. Le restrizioni incluse in una policy di Multi-Region Access Point si applicano solo alle richieste effettuate tramite tale Access Point. Multi-Region

Gestire l'accesso pubblico a un Multi-Region Access Point

Multi-Region I punti di accesso supportano impostazioni indipendenti di blocco dell'accesso pubblico per ciascun punto di Multi-Region accesso. Quando si crea un punto di Multi-Region accesso, è possibile specificare le impostazioni di blocco dell'accesso pubblico applicabili a tale punto di Multi-Region accesso.

Note

Tutte le impostazioni di blocco dell'accesso pubblico abilitate nelle impostazioni di blocco dell'accesso pubblico per questo account (nel proprio account) o nelle impostazioni di blocco pubblico per i bucket esterni rimangono valide anche se le impostazioni indipendenti di blocco dell'accesso pubblico per il punto di Multi-Region accesso sono disabilitate.

Per qualsiasi richiesta effettuata tramite un Multi-Region Access Point, Amazon S3 valuta le impostazioni Block Public Access per:

- Il Multi-Region punto di accesso
- I bucket sottostanti (compresi i bucket esterni)
- L'account proprietario dell' Multi-Region Access Point
- L'account proprietario dei bucket sottostanti (inclusi gli account esterni)

Se una di queste impostazioni indica che la richiesta deve essere bloccata, Amazon S3 rifiuta la richiesta. Per ulteriori informazioni sulla caratteristica di blocco dell'accesso pubblico di Amazon S3, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Important

Per impostazione predefinita, tutte le impostazioni di Blocca accesso pubblico sono abilitate per gli Multi-Region Access Point. È necessario disattivare esplicitamente tutte le impostazioni che non si desidera applicare a un Multi-Region Access Point. Non è possibile modificare le impostazioni di blocco dell'accesso pubblico per un Multi-Region Access Point dopo averlo creato.

Visualizzazione delle impostazioni di blocco dell'accesso pubblico per un punto di Multi-Region accesso

Per visualizzare le impostazioni di blocco dell'accesso pubblico per un punto di Multi-Region accesso

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso).
3. Scegli il nome dell' Multi-Region Access Point che desideri esaminare.
4. Scegli la scheda Autorizzazioni.
5. In Impostazioni di blocco dell'accesso pubblico per questo punto di Multi-Region accesso, rivedi le impostazioni di blocco dell'accesso pubblico per il tuo punto di Multi-Region accesso.

Note

Non puoi modificare le impostazioni di Blocca accesso pubblico dopo la creazione dell' Multi-Region Access Point. Pertanto, se intendi bloccare l'accesso pubblico, assicurati che le tue applicazioni funzionino correttamente senza accesso pubblico prima di creare un Multi-Region Access Point.

Utilizzo di una politica di Multi-Region Access Point

Il seguente esempio di policy Multi-Region Access Point concede a un utente IAM l'accesso per elencare e scaricare file dal tuo Multi-Region Access Point. Per utilizzare questa policy di esempio, sostituisci *user input placeholders* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/JohnDoe"
      },
      "Action": [
```

```

        "s3:ListBucket",
        "s3:GetObject"
    ],
    "Resource": [
        "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
        "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/  
object/*"
    ]
}
]
}

```

Per associare la tua policy Multi-Region Access Point Multi-Region all'Access Point specificato utilizzando AWS Command Line Interface (AWS CLI), usa il seguente `put-multi-region-access-point-policy` comando. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni. Ogni Multi-Region Access Point può avere una sola policy, quindi una richiesta effettuata all'`put-multi-region-access-point-policy` operazione sostituisce qualsiasi policy esistente associata all' Multi-Region Access Point specificato.

AWS CLI

```

aws s3control put-multi-region-access-point-policy
--account-id 111122223333
--details { "Name": "amzn-s3-demo-bucket-MultiRegionAccessPoint",
  "Policy": "{ \"Version\": \"2012-10-17\", \"Statement\": { \"Effect\":
    \"Allow\", \"Principal\": { \"AWS\": \"arn:aws:iam::111122223333:root
  \", \"Action\": [\"s3:ListBucket\", \"s3:GetObject\"], \"Resource\":
    [ \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias\",
    \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/object/*
  \"] } }" }

```

Per esaminare i risultati dell'operazione precedente, utilizza il comando seguente:

AWS CLI

```

aws s3control describe-multi-region-access-point-operation
--account-id 111122223333
--request-token-arn requestArn

```

Per recuperare la politica dell' Multi-Region Access Point, usa il seguente comando:

AWS CLI

```
aws s3control get-multi-region-access-point-policy  
--account-id 111122223333  
--name=amzn-s3-demo-bucket-MultiRegionAccessPoint
```

Modifica della politica dell' Multi-Region Access Point

La policy Multi-Region Access Point (scritta in JSON) fornisce l'accesso allo storage ai bucket Amazon S3 utilizzati con questo Multi-Region Access Point. Puoi consentire o negare a clienti specifici di eseguire varie azioni sul tuo Access Point. Multi-Region Quando una richiesta viene indirizzata a un bucket tramite l' Multi-Region Access Point, si applicano sia le politiche di accesso per l' Multi-Region Access Point che per il bucket. La policy di accesso più restrittiva ha sempre la precedenza.

Note

Se un bucket contiene oggetti di proprietà di altri account, la politica dell' Multi-Region Access Point non si applica agli oggetti di proprietà di altri. Account AWS

Dopo aver applicato un criterio Multi-Region Access Point, il criterio non può essere eliminato. È possibile modificare la policy o creare una nuova policy che sovrascriva quella esistente.

Per modificare la politica dell' Multi-Region Access Point

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso).
3. Scegli il nome dell' Multi-Region Access Point per il quale desideri modificare la policy.
4. Scegli la scheda Autorizzazioni.
5. Scorri verso il basso fino alla sezione relativa alla politica dell' Multi-Region Access Point. Scegli Edit (Modifica) per aggiornare la policy (in JSON).

6. Viene visualizzata la pagina Modifica policy Multi-Region Access Point. Puoi immettere la policy direttamente nel campo di testo oppure puoi scegliere Add statement (Aggiungi istruzione) per selezionare gli elementi della policy da un elenco a discesa.

Note

La console visualizza automaticamente l' Multi-Region Access Point Amazon Resource Name (ARN), che puoi utilizzare nella policy. Ad esempio, le politiche Multi-Region degli Access Point, consulta [the section called “Multi-Region Esempi di politiche relative agli Access Point”](#).

Multi-Region Esempi di politiche relative agli Access Point

Politiche relative alle risorse di supporto per Amazon S3 Multi-Region Access Points AWS Identity and Access Management (IAM). Puoi utilizzare queste politiche per controllare l'uso dell' Multi-Region Access Point per risorsa, utente o altre condizioni. Affinché un'applicazione o un utente possa accedere agli oggetti tramite un Multi-Region Access Point, sia l' Multi-Region Access Point che il bucket sottostante devono consentire lo stesso accesso.

Per consentire lo stesso accesso sia all' Multi-Region Access Point che al bucket sottostante, effettuate una delle seguenti operazioni:

- (Consigliato) Per semplificare i controlli di accesso quando si utilizza un Multi-Region Access Point Amazon S3, delega il controllo degli accessi per il bucket Amazon S3 all'Access Point. Multi-Region Per un esempio su come eseguire questa operazione, consulta l'esempio 1 in questa sezione.
- Aggiungi le stesse autorizzazioni contenute nella policy Multi-Region Access Point alla policy del bucket sottostante.

Important

La delega del controllo di accesso per un bucket a una policy di Multi-Region Access Point non modifica il comportamento del bucket quando si accede al bucket direttamente tramite il nome del bucket o Amazon Resource Name (ARN). Tutte le operazioni eseguite direttamente sul bucket continueranno a funzionare come prima. Le restrizioni incluse in una policy di

Multi-Region Access Point si applicano solo alle richieste effettuate tramite tale Access Point.
Multi-Region

Example 1 — Delega dell'accesso a punti di Multi-Region accesso specifici nella tua policy bucket (per lo stesso account o per più account)

Il seguente esempio di bucket policy garantisce l'accesso completo a un Access Point specifico. Multi-Region Ciò significa che tutti gli accessi a questo bucket sono controllati dalle politiche allegate all'Access Point. Multi-Region Si consiglia di configurare i bucket in questo modo per tutti i casi d'uso che non richiedono l'accesso diretto al bucket. È possibile utilizzare questa struttura di policy a bucket per gli Multi-Region Access Point nello stesso account o in un altro account.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "*" },
      "Action": "*",
      "Resource": [ "arn:aws:s3:::amzn-s3-demo-bucket", "arn:aws:s3:::amzn-s3-
demo-bucket/*" ],
      "Condition": {
        "StringEquals": { "s3:DataAccessPointArn" :
"arn:aws:s3:::111122223333:accesspoint/example-multi-region-access-point" }
      }
    }
  ]
}
```

 Note

Se ci sono più punti di Multi-Region accesso a cui stai concedendo l'accesso, assicurati di elencare ogni punto di Multi-Region accesso.

Example 2 — Concedere a un account l'accesso a un Multi-Region Access Point nella tua politica sugli Multi-Region Access Point

La seguente politica sugli Multi-Region Access Point consente **123456789012** all'account di elencare e leggere gli oggetti contenuti nell' Multi-Region Access Point definito da.

MultiRegionAccessPoint_ARN

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/JohnDoe"
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
        "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/  
object/*"
      ]
    }
  ]
}
```

Example 3 — Politica Multi-Region degli Access Point che consente la pubblicazione dei bucket

La seguente politica di Multi-Region Access Point consente **123456789012** all'account di elencare gli oggetti contenuti nell' Multi-Region Access Point definito da. **MultiRegionAccessPoint_ARN**

Multi-Region Restrizioni e limitazioni dell'Access Point

Multi-Region Gli access point in Amazon S3 presentano le seguenti restrizioni e limitazioni.

Nomi e alias

Multi-Region I nomi degli access point devono soddisfare i seguenti requisiti:

- Devono essere univoci all'interno di un singolo AWS account.
- Devono iniziare con un numero o una lettera minuscola.
- Devono contenere da 3 a 50 caratteri.
- Non possono iniziare o terminare con un trattino (-).
- Non possono contenere trattini bassi (_), lettere maiuscole o punti (.).
- Non possono essere modificati dopo la creazione.

Multi-Region Gli alias degli Access Point (che sono diversi dal nome di un Multi-Region Access Point) vengono generati automaticamente da Amazon S3 e non possono essere modificati o riutilizzati. Per ulteriori informazioni sulla differenza tra alias di Multi-Region Access Point e nomi di Multi-Region Access Point e le rispettive regole di denominazione, consulta [Regole per la denominazione degli Access Point di Amazon S3 Multi-Region](#)

Accesso a un punto di Multi-Region accesso

Non è possibile accedere ai dati tramite un punto di Multi-Region accesso utilizzando endpoint gateway. Tuttavia, è possibile accedere ai dati tramite un punto di Multi-Region accesso utilizzando gli endpoint dell'interfaccia. Per utilizzarlo AWS PrivateLink, è necessario creare endpoint VPC. Per ulteriori informazioni, consulta [Configurazione di un Multi-Region Access Point da utilizzare con AWS PrivateLink](#). Tuttavia, tieni presente che il protocollo IPv6 non è supportato.

Per utilizzare gli Multi-Region Access Point con Amazon CloudFront, devi configurare l' Multi-Region Access Point come tipo di Custom Origin distribuzione. Per ulteriori informazioni sui vari tipi di origine, consulta [Usare varie origini con le CloudFront distribuzioni](#). Per ulteriori informazioni sull'utilizzo degli Multi-Region Access Point con Amazon CloudFront, consulta [Creazione di un'applicazione attiva, attiva e basata sulla prossimità in più regioni nello Storage Blog](#). AWS

Note

I bucket S3 su Outposts non sono supportati.

Firma AWS Richieste API

Per firmare una richiesta AWS API, il tuo Multi-Region Access Point deve soddisfare i seguenti requisiti minimi:

Note

Multi-Region Gli Access Point non supportano richieste anonime.

- Supporto di Transport Layer Security (TLS) versione 1.2.
 - Supporto di Signature Version 4 (SigV4A): questa versione di SigV4 consente di firmare richieste per più Regioni AWS. Questa caratteristica è utile nelle operazioni API che potrebbero comportare l'accesso ai dati da una tra più regioni. Quando si utilizza un AWS SDK, si forniscono le proprie credenziali e le richieste agli Multi-Region Access Point utilizzeranno la versione 4A di Signature senza configurazione aggiuntiva. Assicurati di verificare la [compatibilità del tuo SDK AWS](#) con l'algoritmo SigV4a. Per ulteriori informazioni su Sigv4a, consulta [Signing API requests in. AWS](#)
- Riferimenti generali di AWS

Note

Per utilizzare Sigv4a con credenziali di sicurezza temporanee, ad esempio, quando si utilizzano i ruoli AWS Identity and Access Management (IAM), è possibile richiedere le credenziali temporanee da un endpoint Regional (). Servizio di token di sicurezza AWS AWS STS Se si richiedono credenziali temporanee dall'endpoint globale di AWS STS (`sts.amazonaws.com`), è necessario prima impostare la compatibilità regionale dei token di sessione affinché l'endpoint globale sia valido in tutte le Regioni AWS. Per ulteriori informazioni, consulta Managing in an nella IAM User Guide. [AWS STS Regione AWS](#)

Operazioni API di Amazon S3

- CopyObject è supportata come destinazione solo quando si utilizza l' Multi-Region Access Point ARN.
- La funzionalità per le operazioni in batch di S3 non è supportata.

AWS SDK

Alcuni AWS SDK non sono supportati. Per confermare quali AWS SDK sono supportati per gli Multi-Region Access Point, vedi [Compatibilità con AWS gli SDK](#).

Service Quotas

Tieni presente le seguenti limitazioni delle quote di servizio:

- È previsto un massimo di 100 punti di Multi-Region accesso per account.
- Esiste un limite di 17 regioni per un singolo punto di Multi-Region accesso.

Creazione, eliminazione o modifica di un Multi-Region punto di accesso

Quando crei, elimini o modifichi un punto di Multi-Region accesso, tieni presente le seguenti regole e restrizioni:

- Dopo aver creato un Multi-Region Access Point, non puoi aggiungere, modificare o rimuovere bucket dalla configurazione del punto di Multi-Region accesso. Per modificare i bucket, è necessario eliminare l'intero Multi-Region Access Point e crearne uno nuovo. Se un bucket con più account nel tuo Multi-Region Access Point viene eliminato, l'unico modo per riconnetterlo è ricreare il bucket, utilizzando lo stesso nome e la stessa regione in quell'account.
- I bucket sottostanti (nello stesso account) utilizzati in un Multi-Region Access Point possono essere eliminati solo dopo l'eliminazione di un Access Point. Multi-Region

Supporto delle Regioni

Richieste del piano di controllo (control-plane)

Tutte le richieste del piano di controllo per creare o mantenere i punti di Multi-Region accesso devono essere indirizzate alla US West (Oregon) regione. Per le richieste relative al piano dati degli Multi-Region Access Point, non è necessario specificare le regioni.

Per il piano di controllo del failover dell' Multi-Region Access Point, le richieste devono essere indirizzate a una delle cinque regioni supportate:

- US East (N. Virginia)
- US West (Oregon)
- Asia Pacific (Sydney)

- Asia Pacific (Tokyo)
- Europe (Ireland)

Regioni abilitate per impostazione predefinita

Multi-Region L'Access Point supporta i bucket con le seguenti impostazioni predefinite Regioni AWS ([abilitate di default](#) nel tuo): Account AWS

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- South America (São Paulo)

AWS Regioni attivate

Il tuo Multi-Region Access Point supporta anche i bucket con i seguenti opt-in Regioni AWS (che sono [disabilitati per impostazione predefinita](#) nel tuo): Account AWS

- Africa (Cape Town)
- Asia Pacific (Hong Kong)

- Asia Pacific (Jakarta)
- Asia Pacific (Melbourne)
- Asia Pacific (Hyderabad)
- Canada West (Calgary)
- Europe (Zurich)
- Europe (Milan)
- Europe (Spain)
- Israel (Tel Aviv)
- Middle East (Bahrain)
- Middle East (UAE)

Note

Non sono previsti costi aggiuntivi per l'abilitazione di una Regione con consenso esplicito. Tuttavia, la creazione o l'utilizzo di una risorsa in un Multi-Region Access Point comporta costi di fatturazione.

Una regione con attivazione deve essere abilitata manualmente durante la configurazione o la creazione dell'Access Point. Multi-Region Per ulteriori informazioni sui comportamenti di opt-in regionali per gli Multi-Region Access Point, consulta [Configurazione delle Regioni con consenso esplicito con punti di accesso multi-Regione](#) Per informazioni su come abilitare una regione con opt-in nella tua Account AWS, consulta [Abilitare o disabilitare una regione per account autonomi](#) nella Guida di riferimento per la gestione degli AWS account.

Instradamento della richiesta tramite punto di accesso multi-regione

Quando effettui una richiesta tramite un punto di accesso multi-regione, Amazon S3 individua i bucket associati al punto di accesso multi-regione più vicini. Amazon S3 indirizza quindi la richiesta a quel bucket, indipendentemente dalla regione AWS in cui si trova.

Dopo che il punto di accesso multi-regione instrada la richiesta al bucket più vicino, Amazon S3 elabora la richiesta come se fosse stata eseguita direttamente su tale bucket. I punti di accesso multi-regione non rilevano il contenuto dei dati di un bucket Amazon S3. Pertanto, il bucket che riceve la richiesta potrebbe non contenere i dati richiesti. Per creare set di dati coerenti nei bucket Amazon S3

associati a un punto di accesso multi-regione, puoi configurare la replica tra regioni di Amazon S3 (CRR). Quindi qualsiasi bucket può soddisfare la richiesta correttamente.

Amazon S3 indirizza le richieste dei punti di accesso multi-regione in base alle seguenti regole:

- Amazon S3 ottimizza le richieste da evadere in base alla prossimità. Esamina i bucket supportati dal punto di accesso multi-regione e inoltra la richiesta al bucket più vicino.
- Se la richiesta specifica una risorsa esistente (ad esempio `GetObject`), Amazon S3 non considera il nome dell'oggetto durante l'adempimento della richiesta. Ciò significa che un oggetto potrebbe esistere in un bucket nel punto di accesso multi-regione, ma la richiesta verrà instradata a un bucket che non contiene l'oggetto. Questo scenario restituirà un messaggio di errore 404 al client.

Per evitare errori 404, ti consigliamo di configurare la replica tra regioni di Amazon S3 (S3 CRR) per i bucket. La replica consente infatti di risolvere il problema potenziale che nasce quando l'oggetto desiderato si trova in un bucket del punto di accesso multi-regione, ma non si trova nel bucket specifico a cui è stata instradata la richiesta. Per maggiori informazioni sulla configurazione della replica, consulta [Configurazione della replica per l'utilizzo con punti di accesso multi-regione](#).

Per garantire che le richieste vengano soddisfatte utilizzando gli oggetti specifici desiderati, è inoltre consigliabile attivare il controllo delle versioni dei bucket e includere gli ID delle versioni nelle richieste. In questo modo sei sicuro di disporre della versione corretta dell'oggetto che stai cercando. I bucket con la funzione di controllo delle versioni abilitata consentono di ripristinare gli oggetti che sono stati sovrascritti per errore. Per ulteriori informazioni, consulta [Utilizzo della funzione Controllo delle versioni nei bucket S3](#).

- Se la richiesta prevede di creare una risorsa (ad esempio `PutObject` o `CreateMultipartUpload`), Amazon S3 la esegue utilizzando il bucket più vicino. Ad esempio, considera un'azienda di video che vuole supportare i caricamenti video da qualsiasi parte del mondo. Quando un utente invia una richiesta PUT al punto di accesso multi-regione, l'oggetto viene inserito nel bucket più vicino. Per rendere il video caricato disponibile ad altre persone in tutto il mondo per il download con la latenza più bassa, puoi utilizzare la funzionalità di replica tra regioni di S3 (S3 CRR) con replica bidirezionale. L'uso di questa funzionalità con la replica tra regioni mantiene sincronizzato il contenuto di tutti i bucket associati al punto di accesso multi-regione. Per ulteriori informazioni sulla replica con i punti di accesso multi-regione, consulta [Configurazione della replica per l'utilizzo con punti di accesso multi-regione](#).

Controlli di failover dei punti di Multi-Region accesso Amazon S3

Con i controlli di failover degli Multi-Region Access Point di Amazon S3, puoi mantenere la continuità aziendale durante le interruzioni del traffico regionale, fornendo allo stesso tempo alle tue applicazioni un'architettura multiregionale per soddisfare le esigenze di conformità e ridondanza. Se il traffico regionale viene interrotto, puoi utilizzare i controlli di failover degli Access Point per selezionare quale punto di Multi-Region accesso di Amazon S3 Multi-Region elaborerà Regioni AWS le richieste di accesso e storage ai dati.

Per supportare il failover, puoi configurare Multi-Region l'Access Point in una configurazione attiva-passiva, con il traffico che fluisce verso la regione attiva in condizioni normali e una regione passiva in standby per il failover.

Ad esempio, per eseguire il failover verso una Regione AWS regione a tua scelta, sposti il traffico dalla tua regione principale (attiva) a quella secondaria (passiva). In una configurazione attiva-passiva come questa, un bucket è attivo e accetta traffico, mentre l'altro bucket è passivo e non accetta traffico. Il bucket passivo viene utilizzato per il ripristino di emergenza. Quando si avvia il failover, tutto il traffico (ad esempio le richieste GET o PUT) viene indirizzato al bucket nello stato attivo (in una regione) e allontanato dal bucket nello stato passivo (in un'altra regione).

Se hai abilitato S3 Cross-Region Replication (CRR) con regole di replica bidirezionale, puoi mantenere i bucket sincronizzati durante un failover. Inoltre, se il CRR è abilitato in una configurazione attiva-attiva, gli Multi-Region access point Amazon S3 possono anche recuperare i dati dalla posizione del bucket più vicina, migliorando così le prestazioni delle applicazioni.

Regione AWS supporto

Con i controlli di failover degli Multi-Region Access Points di Amazon S3, i bucket S3 possono trovarsi in una qualsiasi delle 17 regioni in cui sono supportati gli Access Point. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiRegionAccessPointRestrictions.html> Multi-Region È possibile avviare il failover in due regioni qualsiasi contemporaneamente.

Note

Sebbene il failover venga avviato solo tra due regioni contemporaneamente, puoi aggiornare separatamente gli stati di routing per più regioni contemporaneamente nel tuo Access Point. Multi-Region

I seguenti argomenti dimostrano come utilizzare e gestire i controlli di failover degli Access Point di Amazon S3 Multi-Region .

Argomenti

- [Stati di routing degli Multi-Region Access Points di Amazon S3](#)
- [Utilizzo dei controlli di failover degli Access Point di Amazon S3 Multi-Region](#)
- [Il failover di Amazon S3 Multi-Region Access Point controlla gli errori](#)

Stati di routing degli Multi-Region Access Points di Amazon S3

La configurazione di failover degli Multi-Region Access Point di Amazon S3 determina lo stato di routing degli Access Point utilizzati con Regioni AWS l'Access Point. Multi-Region Puoi configurare il tuo Multi-Region Access Point di Amazon S3 in uno stato attivo-attivo o in uno stato attivo-passivo.

- **Active-active**— In una configurazione attiva-attiva, tutte le richieste vengono inviate automaticamente alla zona più vicina del tuo Access Point. Regione AWS Multi-Region Dopo che l' Multi-Region Access Point è stato configurato per essere in uno stato attivo/attivo, tutte le regioni possono ricevere traffico. Se si verifica un'interruzione del traffico in una configurazione attiva-attiva, il traffico di rete verrà automaticamente reindirizzato a una delle regioni attive.
- **Active-passive**— In una configurazione attiva-passiva, le regioni attive dell' Multi-Region Access Point ricevono traffico e quelle passive no. Se intendi utilizzare i controlli di failover S3 per avviare il failover in una situazione di emergenza, configura i tuoi Multi-Region Access Point in una configurazione attiva-passiva mentre stai testando ed esegui la pianificazione del disaster recovery.

Utilizzo dei controlli di failover degli Access Point di Amazon S3 Multi-Region

Questa sezione spiega come gestire e utilizzare i controlli di failover degli Multi-Region Access Points di Amazon S3 utilizzando. Console di gestione AWS

Sono disponibili due controlli di failover nella sezione di configurazione del failover nella pagina dei dettagli dell' Multi-Region Access Point in Console di gestione AWS: Modifica dello stato del routing e Failover. Puoi utilizzare questi controlli nel modo seguente:

- **Modifica lo stato del routing:** puoi modificare manualmente gli stati di routing di un massimo di 17 Regioni AWS in una singola richiesta per il tuo Multi-Region Access Point scegliendo Modifica lo stato del routing. È possibile utilizzare Edit routing status (Modifica stato di instradamento) per i seguenti scopi:

- Per impostare o modificare gli stati di routing di una o più regioni nel tuo Access Point Multi-Region
- Per creare una configurazione di failover per il tuo Multi-Region Access Point configurando due regioni in uno stato attivo-passivo
- Per eseguire manualmente il failover delle regioni
- Per scambiare manualmente il traffico tra regioni
- Failover: quando si avvia il failover scegliendo Failover, si aggiornano solo gli stati di instradamento di due regioni già configurate per essere in uno stato attivo-passivo. Durante un failover avviato scegliendo Failover, gli stati di instradamento tra le due regioni vengono scambiati automaticamente.

Modifica dello stato di routing delle regioni del tuo Access Point Multi-Region

Puoi aggiornare manualmente gli stati di routing fino a 17 Regioni AWS in una singola richiesta per il tuo Multi-Region Access Point scegliendo Modifica lo stato del routing nella sezione di configurazione del failover nella pagina dei dettagli del tuo Multi-Region Access Point. Tuttavia, quando si avvia il failover scegliendo Failover, si aggiornano solo gli stati di instradamento di due regioni già configurate per essere in uno stato attivo-passivo. Durante un failover avviato scegliendo Failover, gli stati di instradamento tra le due regioni vengono scambiati automaticamente.

È possibile utilizzare Edit routing status (Modifica stato di instradamento) (come descritto nella procedura seguente) per i seguenti scopi:

- Per impostare o modificare gli stati di routing di una o più regioni del tuo Access Point Multi-Region
- Per creare una configurazione di failover per il tuo Multi-Region Access Point configurando due regioni in uno stato attivo-passivo
- Per eseguire manualmente il failover delle regioni
- Per scambiare manualmente il traffico tra regioni

Utilizzo della console S3

Per aggiornare lo stato di routing delle regioni del tuo Access Point Multi-Region

1. Accedi alla console di AWS gestione.
2. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.

3. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso).
4. Scegli l' Multi-Region Access Point che desideri aggiornare.
5. Scegli la scheda Replication and failover (Replica e failover).
6. Seleziona una o più regioni di cui desideri modificare lo stato di instradamento.

Note

Per avviare il failover, almeno una regione Regione AWS deve essere designata come attiva e una regione deve essere designata come passiva nel punto di Multi-Region accesso.

7. Scegli Edit routing status (Modifica stato di instradamento).
8. Nella finestra di dialogo visualizzata, seleziona Active (Attivo) o Passive (Passivo) per l'opzione Routing status (Stato instradamento) per ciascuna regione.

Uno stato attivo consente di indirizzare il traffico verso la regione. Uno stato passivo impedisce che qualsiasi traffico venga indirizzato verso la regione.

Se state creando una configurazione di failover per il punto di Multi-Region accesso o avviando il failover, almeno una Regione AWS deve essere designata come attiva e una regione deve essere designata come passiva nel punto di accesso. Multi-Region

9. Scegli Save routing status (Salva stato di instradamento). Il reindirizzamento del traffico richiede circa 2 minuti.

Dopo aver inviato lo stato di routing del Regioni AWS tuo Multi-Region Access Point, puoi verificare le modifiche allo stato del routing. Per verificare queste modifiche, accedi ad Amazon CloudWatch all'indirizzo <https://console.aws.amazon.com/cloudwatch/> per monitorare lo spostamento del traffico di richieste di dati di Amazon S3 (ad esempio, GET e PUT richieste) tra regioni attive e passive. Le connessioni esistenti non verranno interrotte durante il failover. Le connessioni esistenti continueranno fino a raggiungere lo stato di operazione riuscita o errore.

Utilizzo di AWS CLI

Note

Puoi eseguire i comandi di AWS CLI routing Multi-Region degli Access Point su una di queste cinque regioni:

- ap-southeast-2
- ap-northeast-1
- us-east-1
- us-west-2
- eu-west-1

Il comando di esempio seguente aggiorna la configurazione corrente del percorso dell' Multi-Region Access Point. Per aggiornare lo stato attivo o passivo di un bucket, imposta il valore TrafficDialPercentage su 100 per attivo e su 0 per passivo. In questo esempio, *amzn-s3-demo-bucket1* è impostato su attivo e *amzn-s3-demo-bucket2* su passivo. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 123456789012
--mrp MultiRegionAccessPoint_ARN
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2
                ,TrafficDialPercentage=0
```

Il comando di esempio seguente consente di ottenere la configurazione di routing aggiornata dell' Multi-Region Access Point. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrp MultiRegionAccessPoint_ARN
```

Avvio del failover

Quando avvii il failover scegliendo Failover nella sezione di configurazione del failover nella pagina dei dettagli dell' Multi-Region Access Point, il traffico delle richieste di Amazon S3 viene automaticamente spostato su un traffico alternativo. Regione AWS Il processo di failover viene completato entro 2 minuti.

Puoi avviare un failover su due Regioni AWS regioni qualsiasi contemporaneamente (delle 17 regioni in cui sono supportati gli [Access Point](#)). Multi-Region Gli eventi di failover vengono quindi registrati in AWS CloudTrail. Una volta completato il failover, puoi monitorare il traffico di Amazon S3 e qualsiasi aggiornamento del routing del traffico verso la nuova regione attiva in Amazon. CloudWatch

Important

Per mantenere sincronizzati tutti i metadati e gli oggetti tra i bucket durante la replica dei dati, si consiglia di creare regole di replica bidirezionali e abilitare la sincronizzazione delle modifiche della replica prima di configurare i controlli di failover.

Two-way le regole di replica aiutano a garantire che quando i dati vengono scritti nel bucket Amazon S3 in cui il traffico viene reindirizzato, tali dati vengano poi replicati nuovamente nel bucket di origine. La sincronizzazione delle modifiche delle repliche aiuta a garantire che i metadati degli oggetti siano sincronizzati anche tra i bucket durante la replica bidirezionale. Per maggiori informazioni sulla configurazione della replica per supportare il failover, consulta [the section called “Replica del bucket”](#).

Per avviare il failover tra bucket replicati

1. Accedi alla console di gestione. AWS
2. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
3. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso).
4. Scegli l' Multi-Region Access Point che desideri utilizzare per avviare il failover.
5. Scegli la scheda Replication and failover (Replica e failover).
6. Scorri verso il basso fino alla sezione Failover configuration (Configurazione failover) e selezionane due Regioni AWS.

Note

Per avviare il failover, almeno una Regione AWS deve essere designata come **attivo** e una regione deve essere designata come **passiva** nel punto di accesso. Multi-Region Uno stato attivo consente di indirizzare il traffico verso una regione. Uno stato passivo impedisce che qualsiasi traffico venga indirizzato verso la regione.

7. Scegli Failover.

8. Nella finestra di dialogo, scegli di nuovo Failover per avviare il processo di failover. Durante questo processo, gli stati di instradamento delle due regioni vengono scambiati automaticamente. Tutto il nuovo traffico viene indirizzato alla regione che diventa attiva e il traffico smette di essere indirizzato verso la regione che diventa passiva. Il reindirizzamento del traffico richiede circa 2 minuti.

Dopo aver avviato il processo di failover, puoi verificare le variazioni a livello di traffico.

Per verificare queste modifiche, accedi ad Amazon CloudWatch all'indirizzo <https://console.aws.amazon.com/cloudwatch/> per monitorare lo spostamento del traffico di richieste di dati di Amazon S3 (ad esempio, GET e PUT richieste) tra regioni attive e passive. Le connessioni esistenti non verranno interrotte durante il failover. Le connessioni esistenti continueranno fino a raggiungere lo stato di operazione riuscita o errore.

Visualizzazione dei controlli di routing degli Access Point di Amazon S3 Multi-Region

Utilizzo della console S3

Per visualizzare i controlli di routing per il tuo Access Point Amazon S3 Multi-Region

1. Accedi alla console di AWS gestione.
2. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
3. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso).
4. Scegli l' Multi-Region Access Point che desideri esaminare.
5. Scegli la scheda Replication and failover (Replica e failover). Questa pagina mostra i dettagli della configurazione del routing e il riepilogo dell' Multi-Region Access Point, le regole di replica associate e le metriche di replica. Puoi vedere lo stato del instradamento delle tue regioni nella sezione Failover configuration (Configurazione failover).

Utilizzo di AWS CLI

Il AWS CLI comando di esempio seguente ottiene la configurazione corrente del percorso dell' Multi-Region Access Point per la regione specificata. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
```

```
--mrp MultiRegionAccessPoint_ARN
```

Note

Questo comando può essere eseguito solo su queste cinque regioni:

- `ap-southeast-2`
- `ap-northeast-1`
- `us-east-1`
- `us-west-2`
- `eu-west-1`

Il failover di Amazon S3 Multi-Region Access Point controlla gli errori

Quando aggiorni la configurazione di failover per il tuo Multi-Region Access Point, potresti riscontrare uno di questi errori:

- HTTP 400 Bad Request: questo errore può verificarsi se si immette un ARN dell' Multi-Region Access Point non valido durante l'aggiornamento della configurazione di failover. È possibile confermare Multi-Region l'ARN dell'Access Point esaminando la politica dell'Access Point. Multi-Region Per rivedere o aggiornare la politica dell' Multi-Region Access Point, vedi [Modifica della politica](#) dell' Multi-Region Access Point. Questo errore può verificarsi anche se utilizzi una stringa vuota o una stringa casuale durante l'aggiornamento dei controlli di failover dell' Multi-Region Access Point di Amazon S3. Assicurati di utilizzare il formato ARN dell' Multi-Region Access Point:

```
arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias
```

- HTTP 503 Slow Down (HTTP 503 - Rallentamento): questo errore si verifica se si inviano troppe richieste in un breve periodo di tempo. Le richieste rifiutate genereranno un errore.
- Conflitto HTTP 409: questo errore si verifica quando due o più richieste simultanee di aggiornamento della configurazione del percorso sono destinate a un singolo Access Point. Multi-Region La prima richiesta ha esito positivo, ma tutte le altre richieste hanno esito negativo e ciò genera un errore.
- Metodo HTTP 405 non consentito: questo errore si verifica quando si seleziona un punto di accesso con un solo Regione AWS punto di Multi-Region accesso all'avvio del failover. È necessario selezionare due regioni prima di poter avviare il failover. In caso contrario, viene restituito un errore.

Configurazione della replica per l'utilizzo con punti di accesso multi-regione

Quando effettui una richiesta all'endpoint di un punto di accesso multi-regione, Amazon S3 instrada automaticamente la richiesta al bucket più vicino. Per questa decisione, Amazon S3 non prende in considerazione il contenuto della richiesta. Se esegui una richiesta GET per un oggetto, la richiesta potrebbe essere instradata a un bucket che non dispone di una copia dell'oggetto. In questo caso, riceverai un errore con il codice di stato HTTP 404 (Non trovato). Per ulteriori informazioni sull'instradamento delle richieste ai punti di accesso multi-regione, consulta [the section called "Instradamento della richiesta"](#).

Se desideri che il punto di accesso multi-regione sia in grado di recuperare l'oggetto indipendentemente dal bucket che riceve la richiesta, devi configurare la replica tra regioni di Amazon S3 (CRR).

Ad esempio, considera un punto di accesso multi-regione con tre bucket:

- Un bucket denominato *amzn-s3-demo-bucket1* nella regione US West (Oregon) che contiene l'oggetto `my-image.jpg`
- Un bucket denominato *amzn-s3-demo-bucket2* nella regione Asia Pacific (Mumbai) che contiene l'oggetto `my-image.jpg`
- Un bucket denominato *amzn-s3-demo-bucket* nella regione Europe (Frankfurt) che non contiene l'oggetto `my-image.jpg`

In questa situazione, se esegui una richiesta `GetObject` per l'oggetto `my-image.jpg`, il successo della richiesta dipende dal bucket che la riceve. Poiché Amazon S3 non considera il contenuto della richiesta, potrebbe instradare la richiesta `GetObject` al bucket *amzn-s3-demo-bucket* se è il bucket più vicino che risponde. Anche se l'oggetto si trova in un bucket nel punto di accesso multi-regione, otterrai un errore 404 (non trovato) perché il singolo bucket che ha ricevuto la richiesta non ha l'oggetto.

L'attivazione della replica tra regioni (CRR) consente di evitare questo risultato. Con le regole di replica appropriate, l'oggetto `my-image.jpg` viene copiato nel bucket *amzn-s3-demo-bucket*. Pertanto, se Amazon S3 instrada la tua richiesta a quel bucket, ora puoi recuperare l'oggetto.

La replica funziona normalmente con i bucket assegnati a un punto di accesso multi-regione. Amazon S3 non esegue alcuna gestione speciale con i bucket che si trovano in punti di accesso multi-regione. Per ulteriori informazioni sulla configurazione della replica nei bucket, consulta [Panoramica della configurazione della replica in tempo reale](#).

Suggerimenti per l'utilizzo della replica con i punti di accesso multi-regione

Per ottimizzare le prestazioni di replica in caso di utilizzo dei punti di accesso multi-regione, consigliamo quanto segue:

- Configurare la funzionalità di controllo del tempo di replica di S3 (S3 RTC). Per eseguire la replica dei dati in regioni diverse in un arco di tempo prevedibile, puoi utilizzare S3 RTC. S3 RTC replica il 99,99% dei nuovi oggetti archiviati in Amazon S3 entro 15 minuti, secondo un Accordo sul Livello di Servizio (SLA). Per ulteriori informazioni, consulta [the section called “Utilizzo di S3 Replication Time Control”](#). Non vi sono costi aggiuntivi per S3 RTC. Per ulteriori informazioni, consulta la pagina [Prezzi di Amazon S3](#).
- Utilizza la replica bidirezionale per supportare la sincronizzazione dei bucket quando questi vengono aggiornati tramite il punto di accesso multi-regione. Per ulteriori informazioni, consulta [the section called “Creare regole di replica bidirezionale per il punto di accesso multi-regione”](#).
- Crea punti di accesso multi-regione multi-account per replicare i dati in bucket in Account AWS distinti. Questo approccio prevede la separazione a livello di account, in modo che i dati possano essere accessibili e replicati su diversi account in regioni diverse dal bucket di origine. La configurazione di punti di accesso multi-regione multi-account non comporta costi aggiuntivi. Se sei proprietario di un bucket ma non possiedi il punto di accesso multi-regione, paghi solo i costi di richiesta e trasferimento dei dati. I proprietari di punti di accesso multi-regione pagano i costi di instradamento dei dati e accelerazione di Internet. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).
- Abilita la sincronizzazione delle modifiche delle repliche per ogni regola di replica per mantenere sincronizzate anche le modifiche dei metadati degli oggetti. Per ulteriori informazioni, consulta [Abilitazione della sincronizzazione delle modifiche alla replica](#).
- Abilita i CloudWatch parametri di Amazon per [monitorare gli eventi di replica](#). CloudWatch si applicano le tariffe relative ai parametri. Per ulteriori informazioni, consulta i [CloudWatchprezzi di Amazon](#).

Argomenti

- [Creare una regola di replica unidirezionale per il punto di accesso multi-regione](#)
- [Creare regole di replica bidirezionale per il punto di accesso multi-regione](#)
- [Visualizzare regole di replica bidirezionale per il punto di accesso multi-regione](#)

Creare una regola di replica unidirezionale per il punto di accesso multi-regione

Le regole di replica consentono la copia asincrona e automatica di oggetti tra bucket. Una regola di replica unidirezionale aiuta a garantire che i dati vengano replicati completamente da un bucket di origine in un bucket Regione AWS di destinazione in un'altra regione. Quando è configurata la replica unidirezionale, viene creata una regola di replica dal bucket di origine (*amzn-s3-demo-bucket*) al bucket di destinazione (*amzn-s3-demo-bucket*). Come tutte le regole di replica, puoi applicare la regola di replica unidirezionale all'intero bucket Amazon S3 o a un sottoinsieme di oggetti filtrati per prefisso o tag oggetto.

Important

Ti consigliamo di utilizzare la replica unidirezionale se gli utenti utilizzeranno solo gli oggetti nei bucket di destinazione. Se gli utenti caricheranno o modificheranno gli oggetti nei bucket di destinazione, utilizza la replica bidirezionale per mantenere sincronizzati tutti i bucket. Ti consigliamo anche di utilizzare la replica bidirezionale se prevedi di usare il punto di accesso multi-regione per il failover. Per configurare la replica bidirezionale, consulta [the section called "Creare regole di replica bidirezionale per il punto di accesso multi-regione"](#).

Per creare una regola di replica bidirezionale per il punto di accesso multi-regione

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso multi-regione).
3. Scegli il nome del punto di accesso multi-regione.
4. Scegli la scheda Replication and failover (Replica e failover).
5. Scorri verso il basso fino alla sezione Replication rules (Regole di replica) e quindi scegli Create replication rules (Crea regole di replica). Assicurati di disporre di autorizzazioni sufficienti per creare la regola di replica; in caso contrario, il controllo delle versioni verrà disabilitato.

Note

Puoi creare regole di replica solo per i bucket gestiti dal tuo account. Per creare regole di replica per i bucket esterni, saranno i relativi proprietari a dover creare tali regole.

6. Nella pagina Creazione di regole di replica, scegli il modello Replica oggetti da uno o più bucket di origine a uno o più bucket di destinazione.

 Important

Quando crei regole di replica utilizzando questo modello, tali regole sostituiscono qualsiasi regola di replica esistente già assegnata al bucket.

Per aggiungere o modificare le regole di replica esistenti anziché sostituirle, vai alla scheda Management (Gestione) di ciascun bucket nella console, quindi modifica le regole nella sezione Replication rules (Regole di replica). Puoi anche aggiungere o modificare le regole di replica esistenti utilizzando l'API AWS CLI SDKs, o REST. Per ulteriori informazioni, consulta [Elementi del file di configurazione della replica](#).

7. Nella sezione Origine e destinazione, in Bucket di origine, seleziona uno o più bucket da cui desideri eseguire la replica degli oggetti. Tutti i bucket (di origine e di destinazione) scelti per la replica devono avere la funzionalità S3 Controllo delle versioni abilitata e ogni bucket deve trovarsi in una Regione AWS diversa. Per ulteriori informazioni sulla funzionalità S3 di controllo delle versioni, consulta [Utilizzo della funzione Controllo delle versioni nei bucket S3](#).

In Bucket di destinazione, seleziona uno o più bucket in cui desideri eseguire la replica degli oggetti.

8. Nella sezione Replication rule configuration (Configurazione regole di replica), scegli se la regola di replica sarà abilitata (opzione Enabled) o disabilitata (opzione Disabled) al momento della creazione.

 Note

Non è possibile immettere un nome nella casella Replication rule name (Nome regola di replica). I nomi delle regole di replica vengono generati in base alla configurazione definita dall'utente quando crea la regola di replica.

9. Nella sezione Scope (Ambito), scegli l'ambito appropriato per la replica.
 - Per replicare l'intero bucket, scegli Apply to all objects in the bucket (Applica a tutti gli oggetti nel bucket).
 - Per replicare un sottoinsieme di oggetti nel bucket, scegli Limit the scope of this rule using one or more filters (Limita l'ambito di questa regola utilizzando uno o più filtri).

Puoi filtrare gli oggetti utilizzando un prefisso, tag di oggetti o una combinazione di entrambi.

- Per limitare la replica a tutti gli oggetti con nomi che iniziano con la stessa stringa (ad esempio, `pictures`), immetti un prefisso nella casella Prefix (Prefisso).

Se specifichi un prefisso corrispondente al nome di una cartella, devi utilizzare un delimitatore, ad esempio `/` (barra), per indicarne il livello nella gerarchia (ad esempio, `pictures/`). Per ulteriori informazioni sui prefissi, consulta [Organizzazione degli oggetti utilizzando i prefissi](#).

- Per replicare tutti gli oggetti contenenti uno o più tag di oggetto, seleziona Add tag (Aggiungi tag) e specifica la coppia valore-chiave nelle caselle. Per aggiungere un altro tag, ripeti la procedura. Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#).

10. Scorri verso il basso fino alla sezione Additional replication options (Opzioni di replica aggiuntive) e seleziona le opzioni di replica che desideri applicare.

Note

Ti consigliamo di applicare le seguenti opzioni:

- Replication time control (RTC) (Controllo tempo di replica [RTC]): per replicare i dati in regioni diverse in un intervallo di tempo prevedibile, puoi utilizzare la funzionalità di controllo del tempo di replica di S3 (S3 RTC). S3 RTC replica il 99,99% dei nuovi oggetti archiviati in Amazon S3 entro 15 minuti, secondo un Accordo sul Livello di Servizio (SLA). Per ulteriori informazioni, consulta [the section called “Utilizzo di S3 Replication Time Control”](#).
- Metriche e notifiche di replica: abilita i parametri di Amazon per monitorare gli CloudWatch eventi di replica.
- Replica del contrassegno di eliminazione: i contrassegni di eliminazione creati dalle operazioni di eliminazione di S3 verranno replicati. I contrassegni di eliminazione creati dalle regole del ciclo di vita non vengono replicati. Per ulteriori informazioni, consulta [Replica dei contrassegni di eliminazione tra i bucket](#).

Sono previsti costi aggiuntivi per S3 RTC e i parametri e le notifiche di replica. CloudWatch Per ulteriori informazioni, consulta i prezzi di [Amazon S3 e i prezzi di Amazon CloudWatch](#).

11. Se stai scrivendo una nuova regola di replica che sostituisce una esistente, seleziona I acknowledge that by choosing Create replication rules, these existing replication rules will be overwritten (Riconosco che scegliendo Crea regole di replica, queste regole di replica esistenti verranno sovrascritte).
12. Scegli Creazione di regole di replica per creare e salvare la nuova regola di replica unidirezionale.

Creare regole di replica bidirezionale per il punto di accesso multi-regione

Le regole di replica consentono la copia asincrona e automatica di oggetti tra bucket. Una regola di replica bidirezionale garantisce che i dati vengano sincronizzati completamente tra due o più bucket in Regioni AWS diverse. Per impostare la replica bidirezionale, viene creata una regola di replica dal bucket di origine (DOC-EXAMPLE-BUCKET-1) al bucket contenente le repliche (DOC-EXAMPLE-BUCKET-2). Quindi, viene creata una seconda regola di replica dal bucket contenente le repliche (DOC-EXAMPLE-BUCKET-2) al bucket di origine (DOC-EXAMPLE-BUCKET-1).

Come tutte le regole di replica, puoi applicare la regola di replica bidirezionale all'intero bucket Amazon S3 o a un sottoinsieme di oggetti filtrati per prefisso o tag di oggetto. Puoi anche mantenere sincronizzate le modifiche dei metadati dei tuoi oggetti [abilitando la sincronizzazione delle modifiche delle repliche](#) per ogni regola di replica. Puoi abilitare la sincronizzazione delle modifiche alla replica tramite la console Amazon S3, AWS CLI AWS SDKs l'API REST di Amazon S3 oppure. AWS CloudFormation

Per monitorare l'avanzamento della replica di oggetti e metadati degli oggetti in Amazon CloudWatch, abilita le metriche e le notifiche di replica S3. Per maggiori informazioni, consulta [Monitoraggio dell'avanzamento con i parametri di replica e le notifiche di eventi Amazon S3](#).

Per creare una regola di replica bidirezionale per il punto di accesso multi-regione

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso multi-regione).
3. Scegli il nome del punto di accesso multi-regione da aggiornare.
4. Scegli la scheda Replication and failover (Replica e failover).
5. Scorri verso il basso fino alla sezione Replication rules (Regole di replica) e quindi scegli Create replication rules (Crea regole di replica).

6. Nella pagina Create replication rules (Crea regole di replica), scegli il modello Replicate objects among all specified buckets (Replica oggetti tra tutti i bucket specificati). Il modello Replicate objects among all specified buckets (Replica oggetti tra tutti i bucket specificati) imposta la replica bidirezionale (con funzionalità di failover) per i bucket.

 Important

Quando crei regole di replica utilizzando questo modello, tali regole sostituiscono qualsiasi regola di replica esistente già assegnata al bucket.

Per aggiungere o modificare le regole di replica esistenti anziché sostituirle, vai alla scheda Management (Gestione) di ciascun bucket nella console, quindi modifica le regole nella sezione Replication rules (Regole di replica). Puoi anche aggiungere o modificare le regole di replica esistenti utilizzando AWS CLI AWS SDKs, o l'API REST di Amazon S3. Per ulteriori informazioni, consulta [Elementi del file di configurazione della replica](#).

7. Nella sezione Buckets (Bucket), seleziona almeno due bucket da cui desideri replicare gli oggetti. Tutti i bucket scelti per la replica devono avere la funzionalità S3 di controllo delle versioni abilitata e ogni bucket deve trovarsi in una Regione AWS diversa. Per ulteriori informazioni sulla funzionalità S3 di controllo delle versioni, consulta [Utilizzo della funzione Controllo delle versioni nei bucket S3](#).

 Note

Assicurati di disporre delle autorizzazioni di lettura e replica necessarie per eseguire la replica; in caso contrario, verranno restituiti errori. Per ulteriori informazioni, consulta [Creazione di un ruolo IAM](#).

8. Nella sezione Replication rule configuration (Configurazione regole di replica), scegli se la regola di replica sarà abilitata (opzione Enabled) o disabilitata (opzione Disabled) al momento della creazione.

 Note

Non è possibile immettere un nome nella casella Replication rule name (Nome regola di replica). I nomi delle regole di replica vengono generati in base alla configurazione definita dall'utente quando crea la regola di replica.

9. Nella sezione Scope (Ambito), scegli l'ambito appropriato per la replica.

- Per replicare l'intero bucket, scegli Apply to all objects in the bucket (Applica a tutti gli oggetti nel bucket).
- Per replicare un sottoinsieme di oggetti nel bucket, scegli Limit the scope of this rule using one or more filters (Limita l'ambito di questa regola utilizzando uno o più filtri).

Puoi filtrare gli oggetti utilizzando un prefisso, tag di oggetti o una combinazione di entrambi.

- Per limitare la replica a tutti gli oggetti con nomi che iniziano con la stessa stringa (ad esempio, pictures), immetti un prefisso nella casella Prefix (Prefisso).

Se si immette un prefisso corrispondente al nome di una cartella, è necessario utilizzare / (barra) come ultimo carattere (ad esempio, pictures/).

- Per replicare tutti gli oggetti contenenti uno o più tag di oggetto, seleziona Add tag (Aggiungi tag) e specifica la coppia valore-chiave nelle caselle. Per aggiungere un altro tag, ripeti la procedura. Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#).

10. Scorri verso il basso fino alla sezione Additional replication options (Opzioni di replica aggiuntive) e seleziona le opzioni di replica che desideri applicare.

 Note

Ti consigliamo di applicare le seguenti opzioni, soprattutto se intendi configurare il tuo punto di accesso multi-regione in modo che supporti il failover:

- Replication time control (RTC) (Controllo tempo di replica [RTC]): per replicare i dati in regioni diverse in un intervallo di tempo prevedibile, puoi utilizzare la funzionalità di controllo del tempo di replica di S3 (S3 RTC). S3 RTC replica il 99,99% dei nuovi oggetti archiviati in Amazon S3 entro 15 minuti, secondo un Accordo sul Livello di Servizio (SLA). Per ulteriori informazioni, consulta [the section called "Utilizzo di S3 Replication Time Control"](#).
- Metriche e notifiche di replica: abilita i parametri di Amazon per monitorare gli CloudWatch eventi di replica.
- Replica del contrassegno di eliminazione: i contrassegni di eliminazione creati dalle operazioni di eliminazione di S3 verranno replicati. I contrassegni di eliminazione creati dalle regole del ciclo di vita non vengono replicati. Per ulteriori informazioni, consulta [Replica dei contrassegni di eliminazione tra i bucket](#).

- **Replica modification sync (Sincronizzazione modifiche repliche):** abilita la sincronizzazione delle modifiche delle repliche per ogni regola di replica per mantenere sincronizzate anche le modifiche dei metadati degli oggetti. Per ulteriori informazioni, consulta [Abilitazione della sincronizzazione delle modifiche alla replica](#).

Sono previsti costi aggiuntivi per S3 RTC e i parametri e le notifiche di replica. CloudWatch Per ulteriori informazioni, consulta i prezzi di [Amazon S3 e i prezzi](#) di [Amazon CloudWatch](#).

11. Se stai scrivendo una nuova regola di replica che sostituisce una esistente, seleziona I acknowledge that by choosing Create replication rules, these existing replication rules will be overwritten (Riconosco che scegliendo Crea regole di replica, queste regole di replica esistenti verranno sovrascritte).
12. Scegli Create replication rules (Crea regole di replica) per creare e salvare le nuove regole di replica bidirezionale.

Visualizzare regole di replica bidirezionale per il punto di accesso multi-regione

Con i punti di accesso multi-regione, puoi impostare regole di replica unidirezionale o bidirezionale. Per informazioni su come gestire le regole di replica, consulta [Gestione delle regole di replica utilizzando la console di Amazon S3](#).

Per visualizzare regole di replica bidirezionale per il punto di accesso multi-regione

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Multi-Region Access Points (Punti di accesso multi-regione).
3. Scegli il nome del punto di accesso multi-regione.
4. Scegli la scheda Replication and failover (Replica e failover).
5. Scorri verso il basso fino alla sezione Regole di replica. In questa sezione sono elencate tutte le regole di replica create per il punto di accesso multi-regione.

 Note

Se al punto di accesso multi-regione corrente hai aggiunto un bucket da un altro account, devi ottenere l'autorizzazione `s3:GetBucketReplication` dal proprietario del bucket per visualizzare le regole di replica per tale bucket.

Utilizzo Multi-Region degli access point con operazioni API supportate

Amazon S3 fornisce una serie di operazioni per gestire gli Multi-Region access point. Amazon S3 elabora alcune di queste operazioni in modo sincrono e alcune in modo asincrono. Quando richiami un'operazione asincrona, per prima cosa Amazon S3 autorizza in modo sincrono l'operazione richiesta. Se l'autorizzazione ha esito positivo, Amazon S3 restituisce un token che puoi utilizzare per monitorare lo stato di avanzamento e i risultati dell'operazione richiesta.

 Note

Le richieste effettuate tramite la console Amazon S3 sono sempre sincrone. La console attende il completamento della richiesta prima di consentire l'invio di un'altra richiesta.

Puoi visualizzare lo stato attuale e i risultati delle operazioni asincrone utilizzando la console oppure puoi utilizzare `DescribeMultiRegionAccessPointOperation` gli AWS SDK o l'API AWS CLI REST. Amazon S3 fornisce un token di tracciamento nella risposta a un'operazione asincrona. Includi quel token di tracciamento come argomento per `DescribeMultiRegionAccessPointOperation`. Quando includi il token di monitoraggio, Amazon S3 restituisce lo stato corrente e i risultati dell'operazione specificata, inclusi eventuali errori o informazioni pertinenti sulla risorsa. Amazon S3 esegue le operazioni `DescribeMultiRegionAccessPointOperation` in modo sincrono.

Tutte le richieste del piano di controllo per creare o gestire punti di Multi-Region accesso devono essere indirizzate alla regione. `US West (Oregon)` Per le richieste relative al piano dati degli Multi-Region Access Point, non è necessario specificare le regioni. Per il piano di controllo del failover dell' Multi-Region Access Point, la richiesta deve essere indirizzata a una delle cinque regioni supportate. Per ulteriori informazioni sulle regioni supportate Multi-Region dagli Access Point, vedere. [Multi-Region Restrizioni e limitazioni dell'Access Point](#)

Inoltre, è necessario concedere l'`s3:ListAllMyBuckets` autorizzazione all'utente, al ruolo o all'altra entità AWS Identity and Access Management (IAM) che effettua una richiesta per gestire un Multi-Region Access Point.

I seguenti esempi dimostrano come utilizzare gli Multi-Region Access Point con operazioni compatibili in Amazon S3.

Argomenti

- [Multi-Region Compatibilità degli Access Point con Servizi AWS and AWS SDK](#)
- [Multi-Region Compatibilità degli Access Point con le operazioni S3](#)
- [Visualizza la configurazione di routing del tuo Multi-Region Access Point](#)
- [Aggiornare la policy di bucket Amazon S3 sottostante](#)
- [Aggiornare la configurazione del percorso di un Multi-Region Access Point](#)
- [Aggiungi un oggetto a un bucket nel tuo Access Point Multi-Region](#)
- [Recupera oggetti dal tuo Access Point Multi-Region](#)
- [Elenca gli oggetti archiviati in un bucket sottostante il tuo Access Point Multi-Region](#)
- [Usa un URL prefirmato con Access Points Multi-Region](#)
- [Usa un bucket configurato con Requester Pays with Access Points Multi-Region](#)

Multi-Region Compatibilità degli Access Point con Servizi AWS and AWS SDK

Per utilizzare un Multi-Region Access Point con applicazioni che richiedono un nome di bucket Amazon S3, utilizza l'Amazon Resource Name (ARN) dell' Multi-Region Access Point quando effettui richieste utilizzando un SDK. AWS Per verificare quali AWS SDK sono compatibili con gli Multi-Region Access Point, consulta Compatibilità con gli SDK. [AWS](#)

Multi-Region Compatibilità degli Access Point con le operazioni S3

Puoi utilizzare le seguenti operazioni API del piano dati di Amazon S3 per eseguire azioni sugli oggetti nei bucket associati al tuo Multi-Region Access Point. Le seguenti operazioni S3 possono accettare ARN di Multi-Region Access Point:

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CreateMultipartUpload](#)

- [DeleteObject](#)
- [DeleteObjectTagging](#)
- [GetObject](#)
- [GetObjectAcl](#)
- [GetObjectLegalHold](#)
- [GetObjectRetention](#)
- [GetObjectTagging](#)
- [HeadObject](#)
- [ListMultipartUploads](#)
- [ListObjectsV2](#)
- [ListParts](#)
- [PutObject](#)
- [PutObjectAcl](#)
- [PutObjectLegalHold](#)
- [PutObjectRetention](#)
- [PutObjectTagging](#)
- [RestoreObject](#)
- [UploadPart](#)

 Note

Multi-Region Gli Access Points supportano le operazioni di copia utilizzando gli Multi-Region Access Point solo come destinazione quando si utilizza l' Multi-Region Access Point ARN.

Puoi utilizzare le seguenti operazioni sul piano di controllo di Amazon S3 per creare e gestire i tuoi Multi-Region Access Point:

- [CreateMultiRegionAccessPoint](#)
- [DescribeMultiRegionAccessPointOperation](#)
- [GetMultiRegionAccessPoint](#)
- [GetMultiRegionAccessPointPolicy](#)

- [GetMultiRegionAccessPointPolicyStatus](#)
- [GetMultiRegionAccessPointRoutes](#)
- [ListMultiRegionAccessPoints](#)
- [PutMultiRegionAccessPointPolicy](#)
- [SubmitMultiRegionAccessPointRoutes](#)

Visualizza la configurazione di routing del tuo Multi-Region Access Point

AWS CLI

Il comando di esempio seguente recupera la configurazione del percorso dell' Multi-Region Access Point in modo da poter visualizzare gli stati di routing correnti per i bucket. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
```

SDK for Java

Il seguente codice SDK per Java recupera la configurazione del percorso dell' Multi-Region Access Point in modo da poter visualizzare gli stati di routing correnti per i bucket. Per utilizzare questa sintassi di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider)
    .build();

GetMultiRegionAccessPointRoutesRequest request =
    GetMultiRegionAccessPointRoutesRequest.builder()
        .accountId("111122223333")
        .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
        .build();

GetMultiRegionAccessPointRoutesResponse response =
    s3ControlClient.getMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

Il seguente SDK per il JavaScript codice recupera la configurazione del percorso dell' Multi-Region Access Point in modo da poter visualizzare gli stati di routing correnti per i bucket. Per utilizzare questa sintassi di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
const REGION = 'us-east-1'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new GetMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
      })
    )
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()
```

SDK for Python

Il seguente codice SDK per Python recupera la configurazione del percorso dell' Multi-Region Access Point in modo che tu possa vedere gli stati di routing correnti per i tuoi bucket. Per utilizzare questa sintassi di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
s3.get_multi_region_access_point_routes(
    AccountId=111122223333,
    Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap)['Routes']
```

Aggiornare la policy di bucket Amazon S3 sottostante

Per garantire un accesso adeguato, devi anche aggiornare la policy di bucket Amazon S3 sottostante. Gli esempi seguenti delegano il controllo degli accessi alla policy Access Point. Multi-Region Dopo aver delegato il controllo degli accessi alla policy Multi-Region Access Point, la policy bucket non viene più utilizzata per il controllo degli accessi quando le richieste vengono effettuate tramite l' Multi-Region Access Point.

Ecco un esempio di policy bucket che delega il controllo degli accessi alla policy Access Point. Multi-Region Per utilizzare questa policy di bucket, sostituisci *user input placeholders* con le tue informazioni. Per applicare questa politica tramite il AWS CLI `put-bucket-policy` comando, come mostrato nell'esempio successivo, salva la politica in un file, ad esempio, `policy.json`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::444455556666:root"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:DataAccessPointAccount": "444455556666"
        }
      }
    }
  ]
}
```

Il seguente comando di esempio `put-bucket-policy` associa la policy del bucket S3 aggiornata al bucket S3:

```
aws s3api put-bucket-policy
--bucket amzn-s3-demo-bucket
--policy file:///tmp/policy.json
```

Aggiornare la configurazione del percorso di un Multi-Region Access Point

Il comando di esempio seguente aggiorna la configurazione del percorso dell' Multi-Region Access Point. Multi-Region I comandi di route dell'Access Point possono essere eseguiti nelle seguenti cinque regioni:

- `ap-southeast-2`
- `ap-northeast-1`
- `us-east-1`
- `us-west-2`
- `eu-west-1`

In una configurazione di routing di Multi-Region Access Point, è possibile impostare i bucket su uno stato di routing attivo o passivo. A differenza dei bucket passivi, i bucket attivi ricevono traffico. È possibile impostare lo stato di instradamento di un bucket impostando il valore `TrafficDialPercentage` del bucket su `100` per attivo o su `0` per passivo.

AWS CLI

Il comando di esempio seguente aggiorna la configurazione di routing dell' Multi-Region Access Point. In questo esempio, *amzn-s3-demo-bucket1* è impostato sullo stato attivo e *amzn-s3-demo-bucket2* su passivo. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                  Bucket=amzn-s3-demo-bucket2,TrafficDialPercentage=0
```

SDK for Java

Il seguente codice SDK per Java aggiorna la configurazione di routing dell' Multi-Region Access Point. Per utilizzare questa sintassi di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.ap-southeast-2)
    .credentialsProvider(credentialsProvider)
    .build();

SubmitMultiRegionAccessPointRoutesRequest request =
    SubmitMultiRegionAccessPointRoutesRequest.builder()
        .accountId("111122223333")
        .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
        .routeUpdates(
            MultiRegionAccessPointRoute.builder()
                .region("eu-west-1")
                .trafficDialPercentage(100)
                .build(),
            MultiRegionAccessPointRoute.builder()
                .region("ca-central-1")
                .bucket("111122223333")
                .trafficDialPercentage(0)
                .build()
        )
        .build();

SubmitMultiRegionAccessPointRoutesResponse response =
    s3ControlClient.submitMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

Il seguente SDK per il JavaScript codice aggiorna la configurazione del percorso dell' Multi-Region Access Point. Per utilizzare questa sintassi di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
const REGION = 'ap-southeast-2'

const s3ControlClient = new S3ControlClient({
  region: REGION
})
```



```

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new SubmitMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
        RouteUpdates: [
          {
            Region: 'eu-west-1',
            TrafficDialPercentage: 100,
          },
          {
            Region: 'ca-central-1',
            Bucket: 'amzn-s3-demo-bucket1',
            TrafficDialPercentage: 0,
          },
        ],
      })
    )
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()

```

SDK for Python

Il seguente codice SDK per Python aggiorna la configurazione del percorso dell' Multi-Region Access Point. Per utilizzare questa sintassi di esempio, sostituisci *user input placeholders* con le tue informazioni.

```

s3.submit_multi_region_access_point_routes(
    AccountId=111122223333,
    Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap,
    RouteUpdates= [{
        'Bucket': amzn-s3-demo-bucket,
        'Region': ap-southeast-2,
        'TrafficDialPercentage': 10
    }])

```

Aggiungi un oggetto a un bucket nel tuo Access Point Multi-Region

Per aggiungere un oggetto al bucket associato all' Multi-Region Access Point, puoi utilizzare l'[PutObject](#) operazione. Per mantenere sincronizzati tutti i bucket nell' Multi-Region Access Point, abilita [Cross-Region Replication](#).

Note

Per utilizzare questa operazione, è necessario disporre dell'`s3:PutObject` autorizzazione per l' Multi-Region Access Point. Per ulteriori informazioni sui requisiti di autorizzazione dell' Multi-Region Access Point, vedere [Permissions](#).

AWS CLI

Nel seguente esempio, la richiesta del piano dati viene caricata *example.txt* nell' Multi-Region Access Point specificato. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api put-object --bucket
arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --key example.txt --
body example.txt
```

SDK for Java

```
S3Client s3Client = S3Client.builder()
    .build();

PutObjectRequest objectRequest = PutObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example.txt")
    .build();

s3Client.putObject(objectRequest, RequestBody.fromString("Hello S3!"));
```

SDK for JavaScript

```
const client = new S3Client({});

async function putObjectExample() {
```

```
const command = new PutObjectCommand({
  Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
  Key: "example.txt",
  Body: "Hello S3!",
});

try {
  const response = await client.send(command);
  console.log(response);
} catch (err) {
  console.error(err);
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.put_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
    Key='example.txt',
    Body='Hello S3!'
)
```

Recupera oggetti dal tuo Access Point Multi-Region

Per recuperare oggetti dall' Multi-Region Access Point, è possibile utilizzare l'[GetObject](#) operazione.

Note

Per utilizzare questa operazione API, è necessario disporre dell'`s3:GetObject` autorizzazione per l' Multi-Region Access Point. Per ulteriori informazioni sui requisiti per le autorizzazioni degli Multi-Region Access Point, vedere [Permissions](#).

AWS CLI

Il seguente esempio di richiesta del piano dati viene recuperato *example.txt* dall' Multi-Region Access Point specificato e lo scarica come *downloaded_example.txt*. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api get-object --bucket
arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --
key example.txt downloaded_example.txt
```

SDK for Java

```
S3Client s3 = S3Client
    .builder()
    .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example.txt")
    .build();

s3Client.getObject(getObjectRequest);
```

SDK for JavaScript

```
const client = new S3Client({})

async function getObjectExample() {
    const command = new GetObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt"
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.get_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
```

```
    Key='example.txt'  
  )
```

Elenca gli oggetti archiviati in un bucket sottostante il tuo Access Point Multi-Region

Per restituire un elenco di oggetti archiviati in un bucket sottostante l' Multi-Region Access Point, usa l'[ListObjectsV2](#) operazione. Nel comando di esempio seguente, tutti gli oggetti per l' Multi-Region Access Point specificato vengono elencati utilizzando l'ARN per l' Multi-Region Access Point. In questo caso, l'ARN dell' Multi-Region Access Point è:

```
arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap
```

Note

Per utilizzare questa operazione API, è necessario disporre dell'`s3:ListBucket` autorizzazione per l' Multi-Region Access Point e il bucket sottostante. Per ulteriori informazioni sui requisiti per le autorizzazioni degli Multi-Region Access Point, vedere [Permissions](#)

AWS CLI

Il seguente esempio di richiesta del piano dati elenca gli oggetti nel bucket che sta alla base dell' Multi-Region Access Point specificato dall'ARN. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3api list-objects-v2 --bucket  
arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap
```

SDK for Java

```
S3Client s3Client = S3Client.builder()  
    .build();  
  
String bucketName = "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap";  
  
ListObjectsV2Request listObjectsRequest = ListObjectsV2Request  
    .builder()  
    .bucket(bucketName)
```

```
.build();

s3Client.listObjectsV2(listObjectsRequest);
```

SDK for JavaScript

```
const client = new S3Client({});

async function listObjectsExample() {
  const command = new ListObjectsV2Command({
    Bucket: "arn:aws:s3:::123456789012:accesspoint/abcdef0123456.mrap",
  });

  try {
    const response = await client.send(command);
    console.log(response);
  } catch (err) {
    console.error(err);
  }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.list_objects_v2(
    Bucket='arn:aws:s3:::123456789012:accesspoint/abcdef0123456.mrap'
)
```

Usa un URL prefirmato con Access Points Multi-Region

Puoi utilizzare un URL prefirmato per generare un URL che consenta ad altri di accedere ai tuoi bucket Amazon S3 tramite un punto di accesso Amazon S3. Multi-Region Quando crei un URL prefirmato, associalo a un'operazione sugli oggetti specifica come un caricamento S3 (`PutObject`) o un download S3 (`GetObject`). L'URL prefirmato può essere condiviso e gli utenti che dispongono dell'autorizzazione di accesso possono eseguire l'azione incorporata nell'URL come se fossero l'utente di firma originale.

Gli URL prefirmati hanno una data di scadenza. Una volta raggiunta la scadenza, l'URL non funzionerà più.

Prima di utilizzare gli Multi-Region access point S3 con URL prefirmati, verifica la compatibilità dell'SDK con l'[AWS algoritmo SigV4a](#). Verifica che la tua versione SDK supporti SigV4a come implementazione di firma utilizzata per firmare le richieste globali a livello di Regione AWS . Per ulteriori informazioni sugli URL prefirmati, consulta [Condivisione di oggetti mediante URL prefirmati](#).

Gli esempi seguenti mostrano come utilizzare gli Access Point con URL prefirmati. Multi-Region Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

AWS CLI

```
aws s3 presign
arn:aws:s3::123456789012:accesspoint/MultiRegionAccessPoint_alias/example-file.txt
```

SDK for Python

```
import logging
import boto3
from botocore.exceptions import ClientError

s3_client = boto3.client('s3',aws_access_key_id='xxx',aws_secret_access_key='xxx')
s3_client.generate_presigned_url(HttpMethod='PUT',ClientMethod="put_object",
    Params={'Bucket':'arn:aws:s3::123456789012:accesspoint/
abcdef0123456.mrap', 'Key':'example-file'})
```

SDK for Java

```
S3Presigner s3Presigner = S3Presigner.builder()
    .credentialsProvider(StsAssumeRoleCredentialsProvider.builder()
        .refreshRequest(assumeRole)
        .stsClient(stsClient)
        .build())
    .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example-file")
    .build();

GetObjectPresignRequest preSignedReq = GetObjectPresignRequest.builder()
    .getObjectRequest(getObjectRequest)
    .signatureDuration(Duration.ofMinutes(10))
    .build();
```

```
PresignedGetObjectRequest presignedGetObjectRequest =  
    s3Presigner.presignGetObject(preSignedReq);
```

Note

Per utilizzare Sigv4a con credenziali di sicurezza temporanee, ad esempio quando utilizzi i ruoli IAM, assicurati di richiedere le credenziali temporanee da un endpoint regionale in (), anziché da un endpoint globale. Servizio di token di sicurezza AWS AWS STS Se utilizzi l'endpoint globale for AWS STS (sts.amazonaws.com), AWS STS genererà credenziali temporanee da un endpoint globale, che non è supportato da Sig4A. Di conseguenza, verrà restituito un errore. Per risolvere questo problema, utilizza uno degli endpoint regionali elencati per. [AWS STS](#)

Usa un bucket configurato con Requester Pays with Access Points Multi-Region

Se un bucket S3 associato Multi-Region ai tuoi Access Point è [configurato per utilizzare Requester Pays](#), il richiedente pagherà la richiesta del bucket, il download e tutti i costi relativi agli Access Point. Multi-Region Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Ecco un esempio di richiesta di data plane a un Multi-Region Access Point connesso a un bucket Requester Pays.

AWS CLI

Per scaricare oggetti da un Multi-Region Access Point connesso a un bucket Requester Pays, devi specificarlo `--request-payer requester` come parte della richiesta. [get-object](#) Inoltre, devi specificare il nome del file nel bucket e la posizione in cui archiviare il file scaricato.

```
aws s3api get-object --bucket MultiRegionAccessPoint_ARN --request-payer requester  
--key example-file-in-bucket.txt example-location-of-downloaded-file.txt
```

SDK for Java

Per scaricare oggetti da un Multi-Region Access Point connesso a un bucket Requester Pays, è necessario specificarlo `RequestPayer.REQUESTER` come parte della richiesta. `GetObject` È inoltre necessario specificare il nome del file nel bucket e la posizione in cui deve essere archiviato.


```
GetObjectResponse getObjectResponse = s3Client.getObject(GetObjectRequest.builder()  
    .key("example-file.txt")  
    .bucket("arn:aws:s3:  
123456789012:accesspoint/abcdef0123456.mrap")  
    .requestPayer(RequestPayer.REQUESTER)  
    .build()  
).response();
```

Monitoraggio e registrazione delle richieste effettuate tramite un punto di accesso multi-regione alle risorse sottostanti

Amazon S3 registra le richieste effettuate tramite i punti di accesso multi-regione e le richieste effettuate alle operazioni API che li gestiscono, ad esempio `CreateMultiRegionAccessPoint` e `GetMultiRegionAccessPointPolicy`. Le richieste effettuate ad Amazon S3 tramite un punto di accesso multiregionale vengono visualizzate nei log di accesso al server Amazon S3 e nei log con il nome host del punto di accesso multiregionale AWS CloudTrail. Il nome host di un punto di accesso ha il formato `MRAP_alias.accesspoint.s3-global.amazonaws.com`. Ad esempio, supponiamo di disporre della seguente configurazione di bucket e punto di accesso multi-regione:

- Un bucket denominato `my-bucket-usw2` nella regione `us-west-2` che contiene l'oggetto `my-image.jpg`
- Un bucket denominato `my-bucket-aps1` nella regione `ap-south-1` che contiene l'oggetto `my-image.jpg`
- Un bucket denominato `my-bucket-euc1` nella regione `eu-central-1` che non contiene un oggetto denominato `my-image.jpg`.
- Un punto di accesso multi-regione denominato `my-mrap` con l'alias `mfzwi23gnjvgw.mrap` configurato per soddisfare le richieste da tutti e tre i bucket.
- L'ID del tuo account è. AWS 123456789012

Una richiesta eseguita per recuperare `my-image.jpg` direttamente attraverso uno qualsiasi dei bucket appare nei registri con il nome host `bucket_name.s3.Region.amazonaws.com`.

Se invece esegui la richiesta tramite il punto di accesso multi-regione, Amazon S3 determina innanzitutto quali bucket nelle diverse regioni si trovano più vicini. Dopo che Amazon S3 determina i bucket utilizzare per eseguire la richiesta, invia la richiesta a tale bucket e registra l'operazione utilizzando il nome host del punto di accesso multi-regione. In questo esempio, se Amazon S3

inoltre la richiesta a `my-bucket-aps1`, i tuoi log riporteranno una richiesta GET riuscita per `my-image.jpg` da `my-bucket-aps1`, utilizzando `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com` come nome host.

Important

I punti di accesso multi-regione non rilevano il contenuto dei dati dei bucket sottostanti. Pertanto, il bucket che riceve la richiesta potrebbe non contenere i dati richiesti. Se Amazon S3 determina che il bucket `my-bucket-euc1` è il più vicino, i log includeranno una richiesta GET non riuscita per `my-image.jpg` da `my-bucket-euc1`, utilizzando `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com` come nome host. Se la richiesta è stata invece instradata a `my-bucket-usw2`, i tuoi log indicherebbero una richiesta GET riuscita.

Per ulteriori informazioni sui log degli accessi al server Amazon S3, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#). Per ulteriori informazioni su AWS CloudTrail, vedi [Cos'è AWS CloudTrail?](#) nella Guida AWS CloudTrail per l'utente.

Monitoraggio e registrazione delle richieste effettuate alle operazioni API di gestione dei punti di accesso multi-regione

Amazon S3 fornisce diverse operazioni API per gestire i punti di accesso multi-regione, come `CreateMultiRegionAccessPoint` e `GetMultiRegionAccessPointPolicy`. Quando effettui richieste a queste operazioni API utilizzando AWS Command Line Interface (AWS CLI) o l'API REST di Amazon S3 AWS SDKs, Amazon S3 elabora queste richieste in modo asincrono. Se disponi delle autorizzazioni appropriate per la richiesta, Amazon S3 restituisce un token per queste richieste. Puoi usare questo token con `DescribeAsyncOperation` per semplificare la visualizzazione dello stato delle operazioni asincrone in corso. Amazon S3 elabora le richieste `DescribeAsyncOperation` in modo sincrono. Per visualizzare lo stato delle richieste asincrone, puoi utilizzare la console Amazon S3 o l'API REST AWS CLI. SDKs

Note

La console visualizza solo lo stato delle richieste asincrone effettuate nei 14 giorni precedenti. Per visualizzare lo stato delle richieste precedenti, usa l'API, o AWS CLI REST SDKs.

Le operazioni di gestione asincrona possono avere uno tra diversi stati:

NEW

Amazon S3 ha ricevuto la richiesta e si sta preparando per eseguire l'operazione.

IN_PROGRESS

Amazon S3 sta attualmente eseguendo l'operazione.

SUCCESS

L'operazione è stata completata. La risposta include informazioni rilevanti, ad esempio l'alias del punto di accesso multi-regione per una richiesta `CreateMultiRegionAccessPoint`.

FAILED

L'operazione ha avuto esito negativo. La risposta include un messaggio di errore che indica il motivo dell'errore.

Utilizzo AWS CloudTrail con punti di accesso multiregionali

Puoi utilizzarlo AWS CloudTrail per visualizzare, cercare, scaricare, archiviare, analizzare e rispondere alle attività degli account nell'intera AWS infrastruttura. Con i punti di accesso multiregionali e CloudTrail la registrazione, puoi identificare quanto segue:

- Chi o cosa ha eseguito l'operazione e l'operazione eseguita
- Le risorse utilizzate
- Quando si è verificato l'evento
- Altri dettagli relativi all'evento

Puoi utilizzare queste informazioni di registrazione per aiutarti ad analizzare e rispondere alle attività che si sono verificate nei punti di accesso multi-regione.

Come configurare i punti di accesso AWS CloudTrail multiregionali

Per abilitare CloudTrail la registrazione per qualsiasi operazione relativa alla creazione o alla manutenzione di punti di accesso multiregionali, è necessario configurare la CloudTrail registrazione per registrare gli eventi nella regione Stati Uniti occidentali (Oregon). Devi impostare la configurazione della registrazione in questo modo indipendentemente dalla regione in cui ti trovi quando esegui la richiesta o dalle regioni supportate dal punto di accesso multi-regione. Tutte le richieste di creazione o gestione di un punto di accesso multi-regione vengono instradate attraverso la regione Stati Uniti occidentali (Oregon). Ti consigliamo di aggiungere questa regione a un trail

esistente o crearne uno nuovo che contenga questa regione e tutte le regioni associate al punto di accesso multi-regione.

Amazon S3 registra le richieste eseguite tramite un punto di accesso multi-regione e quelle eseguite alle operazioni API che gestiscono i punti di accesso, ad esempio `CreateMultiRegionAccessPoint` e `GetMultiRegionAccessPointPolicy`. Quando si registrano queste richieste tramite un punto di accesso multiregionale, esse vengono visualizzate nei AWS CloudTrail registri con il nome host del punto di accesso multiregionale. Ad esempio, se effettui richieste a un bucket tramite un punto di accesso multiregionale con l'alias `mfzwi23gnjvgw.mrap`, le voci nel registro avranno un nome host di CloudTrail `.mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`

I punti di accesso multiregionali instradano le richieste al bucket più vicino. A causa di questo comportamento, quando si esaminano CloudTrail i log di un punto di accesso multiregionale, si notano le richieste inviate ai bucket sottostanti. Alcune di queste richieste potrebbero corrispondere a richieste dirette al bucket non instradate attraverso il punto di accesso multi-regione. Considera questa eventualità quando esami il traffico. Quando un bucket si trova in un punto di accesso multi-regione, è comunque possibile effettuare richieste direttamente a tale bucket senza passare attraverso il punto di accesso multi-regione.

Esistono eventi asincroni coinvolti nella creazione e nella gestione dei punti di accesso multi-regione. Le richieste asincrone non hanno eventi di completamento nel registro. CloudTrail Per ulteriori informazioni sul monitoraggio delle richieste asincrone, consulta [Monitoraggio e registrazione delle richieste effettuate alle operazioni API di gestione dei punti di accesso multi-regione](#).

[Per ulteriori informazioni su AWS CloudTrail, consulta What is? AWS CloudTrail](#) nella Guida AWS CloudTrail per l'utente.

Conservazione di più versioni degli oggetti con Controllo delle versioni S3

La funzione Controllo delle versioni in Amazon S3 è un modo per conservare più versioni di un oggetto nello stesso bucket. Puoi utilizzare la funzione Controllo delle versioni S3 per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nei tuoi bucket. Con la funzione Controllo delle versioni si può facilmente eseguire il ripristino dopo errori dell'applicazione e operazioni non intenzionali dell'utente. Quando abiliti la funzione Controllo delle versioni del bucket, se Amazon S3 riceve più richieste di scrittura per lo stesso oggetto contemporaneamente, vengono archiviati tutti gli oggetti.

Versioning-enabled i bucket possono aiutarti a recuperare oggetti da cancellazioni o sovrascritture accidentali. Ad esempio, se elimini un oggetto, Amazon S3 inserisce un contrassegno di eliminazione invece di rimuovere l'oggetto in modo permanente. Il contrassegno di eliminazione diventa la versione corrente dell'oggetto. La sovrascrittura di un oggetto genera una nuova versione dell'oggetto nel bucket. È sempre possibile ripristinare la versione precedente. Per ulteriori informazioni, consulta [Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata](#).

Per impostazione predefinita, la funzione Controllo delle versioni S3 è disabilitata nei bucket ed è necessario abilitarlo esplicitamente. Per ulteriori informazioni, consulta [Abilitazione della funzione Controllo delle versioni sui bucket](#).

Note

- L'API SOAP non supporta la funzione Controllo delle versioni S3. Il supporto di SOAP su HTTP non viene più utilizzato, ma è ancora disponibile su HTTPS. Le nuove funzioni di Amazon S3 non sono supportate per SOAP.
- A ogni versione archiviata e trasferita di un oggetto si applicano le tariffe Amazon S3 normali. Ogni versione di un oggetto è l'intero oggetto e non semplicemente la sua versione precedente con qualche differenza. Per questo motivo, se sono presenti tre versioni di un oggetto memorizzate verranno addebitati tre oggetti.

Bucket senza versione, con funzione Controllo delle versioni e con funzione Controllo delle versioni sospesa

I bucket possono trovarsi in uno dei tre stati:

- Senza versione (impostazione predefinita)
- Versioning-enabled
- Versioning-suspended

Puoi abilitare e sospendere la funzione Controllo delle versioni a livello di bucket. Dopo aver abilitato la funzione Controllo delle versioni del bucket, non è possibile riportare il bucket nello stato senza versione. Tuttavia puoi sospendere la funzione Controllo delle versioni su tali bucket.

La funzione Controllo delle versioni si applica a tutti (mai solo ad alcuni) oggetti del bucket. Quando si abilita il controllo delle versioni in un bucket, tutti i nuovi oggetti vengono sottoposti al controllo

versioni e viene assegnato un ID versione univoco. Gli oggetti già presenti nel bucket al momento in cui è stato abilitato il controllo delle versioni verranno successivamente sempre sottoposti al controllo versioni e verrà loro assegnato un ID versione univoco quando vengono modificati da richieste future. Tieni presente quanto segue:

- Gli oggetti che sono stati archiviati nel bucket prima dell'impostazione dello stato della funzione Controllo delle versioni hanno un ID versione null. Quando si abilita la funzione Controllo delle versioni, gli oggetti esistenti nel bucket non si modificano. Ciò che cambia è il modo in cui Amazon S3 gestirà gli oggetti delle richieste future. Per ulteriori informazioni, consulta [Utilizzo di oggetti in un bucket che supporta la funzione Controllo delle versioni](#).
- Il proprietario del bucket (o un qualsiasi utente con le autorizzazioni appropriate) può sospendere la funzione Controllo delle versioni per interrompere l'accumulo di versioni. Quando si sospende la funzione Controllo delle versioni, gli oggetti esistenti nel bucket non si modificano. Ciò che cambia è il modo in cui Amazon S3 gestirà gli oggetti delle richieste future. Per ulteriori informazioni, consulta [Utilizzo di oggetti di un bucket con funzione Controllo delle versioni sospesa](#).

Utilizzo della funzione Controllo delle versioni S3 con il ciclo di vita di S3

La funzione Controllo delle versioni degli oggetti consente, insieme al ciclo di vita di S3, di personalizzare il metodo di conservazione dei dati e di controllare i costi di storage. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#). Per informazioni sulla creazione di configurazioni del ciclo di vita di S3 utilizzando, AWS SDK o l'API REST Console di gestione AWS AWS CLI, consulta. [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#)

Important

Se nel bucket senza funzione Controllo delle versioni è presente una configurazione del ciclo di vita per la scadenza dell'oggetto e si vuole mantenere lo stesso comportamento di eliminazione permanente che si applica quando la funzione Controllo delle versioni è abilitata, è necessario aggiungere una configurazione di scadenza non corrente. La configurazione del ciclo di vita per la scadenza non corrente gestisce le eliminazioni delle versioni non correnti dell'oggetto nel bucket abilitato per il controllo delle versioni. (Un bucket abilitato per il controllo delle versioni mantiene una versione dell'oggetto corrente e zero o più versioni dell'oggetto non correnti.) Per ulteriori informazioni, consulta [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#).

Per informazioni sull'utilizzo della funzione Controllo delle versioni S3, fai riferimento agli argomenti di seguito.

Argomenti

- [Come funzionano il Controllo delle versioni S3](#)
- [Abilitazione della funzione Controllo delle versioni sui bucket](#)
- [Configurazione dell'eliminazione di MFA](#)
- [Utilizzo di oggetti in un bucket che supporta la funzione Controllo delle versioni](#)
- [Utilizzo di oggetti di un bucket con funzione Controllo delle versioni sospesa](#)
- [Risoluzione dei problemi relativi al controllo delle versioni](#)

Come funzionano il Controllo delle versioni S3

Puoi utilizzare il controllo delle versioni S3 per mantenere più versioni di un oggetto in un unico bucket e ripristinare gli oggetti che vengono accidentalmente eliminati o sovrascritti. Ad esempio, se applichi il controllo delle versioni S3 a un bucket, si verificano le seguenti modifiche:

- Se anziché rimuovere un oggetto in modo permanente lo elimini, Amazon S3 inserisce un contrassegno di eliminazione che diventa la versione corrente dell'oggetto. È quindi possibile ripristinare la versione precedente. Per ulteriori informazioni, consulta [Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata](#).
- Se sovrascrivi un oggetto, Amazon S3 aggiunge una nuova versione dell'oggetto nel bucket. La versione precedente rimane nel bucket e diventa una versione non corrente. Puoi ripristinare la versione precedente.

Note

A ogni versione archiviata e trasferita di un oggetto si applicano le tariffe Amazon S3 normali. Ogni versione di un oggetto è l'intero oggetto e non la sua versione precedente con qualche differenza. Per questo motivo, se sono presenti tre versioni di un oggetto memorizzate verranno addebitati tre oggetti.

A ogni bucket S3 creato è associata una sottorisorsa per la funzione Controllo delle versioni. (Per ulteriori informazioni, consulta [Opzioni di configurazione dei bucket per uso generico](#).) Per

impostazione predefinita, il bucket è senza versione, di conseguenza la sottorisorsa per la funzione Controllo delle versioni archivia una configurazione vuota della funzione Controllo delle versioni.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</VersioningConfiguration>
```

Per abilitare il controllo delle versioni, puoi inviare una richiesta ad Amazon S3 con una configurazione del controllo delle versioni con lo stato Enabled.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

Per sospendere la funzione Controllo delle versioni, si imposterà il valore dello stato su Suspended.

Note

Quando abiliti il controllo delle versioni in un bucket per la prima volta, potrebbe essere necessario un breve periodo di tempo per la propagazione completa della modifica. Durante la propagazione di questa modifica, è possibile che si verifichino gli errori HTTP 404 NoSuchKey intermittenti nelle richieste agli oggetti creati o aggiornati dopo l'abilitazione del controllo delle versioni. Ti consigliamo di attendere 15 minuti dopo aver abilitato il controllo delle versioni prima di eseguire operazioni di scrittura (PUT o DELETE) sugli oggetti nel bucket.

Il proprietario del bucket e tutti gli utenti autorizzati AWS Identity and Access Management (IAM) possono abilitare il controllo delle versioni. Il proprietario del bucket è colui Account AWS che ha creato il bucket. Per ulteriori informazioni sulle autorizzazioni, consultare [Identity and Access Management per Amazon S3](#).

Per ulteriori informazioni sull'abilitazione e la disabilitazione del controllo delle versioni di S3 utilizzando l'API Console di gestione AWS, AWS Command Line Interface (AWS CLI) o REST, vedere [the section called “Abilitazione della funzione Controllo delle versioni sui bucket”](#)

Argomenti

- [ID versione](#)
- [Flussi di lavoro per la funzione Controllo delle versioni](#)

ID versione

Se si abilita la funzione Controllo delle versioni del bucket, Amazon S3 genera automaticamente un ID versione univoco per l'oggetto archiviato. Ad esempio, un bucket può contenere due oggetti con la stessa chiave (nome dell'oggetto) ma ID versione diverso, ad esempio `photo.gif` (versione 111111) e `photo.gif` (versione 121212).

Un bucket abilitato al controllo delle versioni che ha due oggetti con la stessa chiave ma ID di versione diversi.

Ogni oggetto ha un ID versione, indipendentemente dal fatto che Controllo delle versioni S3 sia abilitato o meno. Se il controllo delle versioni S3 non è abilitato, Amazon S3 imposta il valore dell'ID versione su `null`. Se si attiva la funzione Controllo delle versioni S3, Amazon S3 assegna un valore ID versione per l'oggetto. Questo valore distingue l'oggetto dalle altre versioni della stessa chiave.

Quando si attiva la funzione Controllo delle versioni S3 in un bucket esistente, gli oggetti già archiviati nel bucket rimangono invariati. Gli ID versione (`null`), il contenuto e le autorizzazioni non sono cambiati. Dopo aver abilitato il controllo delle versioni S3, ogni oggetto aggiunto al bucket ottiene un ID versione che lo distingue dalle altre versioni della stessa chiave.

Solo Amazon S3 genera gli ID versione che non possono essere modificati. Gli ID di versione sono stringhe Unicode, UTF-8 codificate e opache lunghe URL-ready non più di 1.024 byte. Di seguito è riportato un esempio:

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

Note

Per semplicità, gli altri esempi in questo argomento utilizzano ID molto più brevi.

Flussi di lavoro per la funzione Controllo delle versioni

Se si esegue l'operazione PUT su un oggetto in un bucket abilitato per il controllo delle versioni, la versione non corrente non viene sovrascritta. Come mostrato nella seguente figura, quando viene eseguita un'operazione PUT per una nuova versione di `photo.gif` in un bucket che già contiene un oggetto con lo stesso nome:

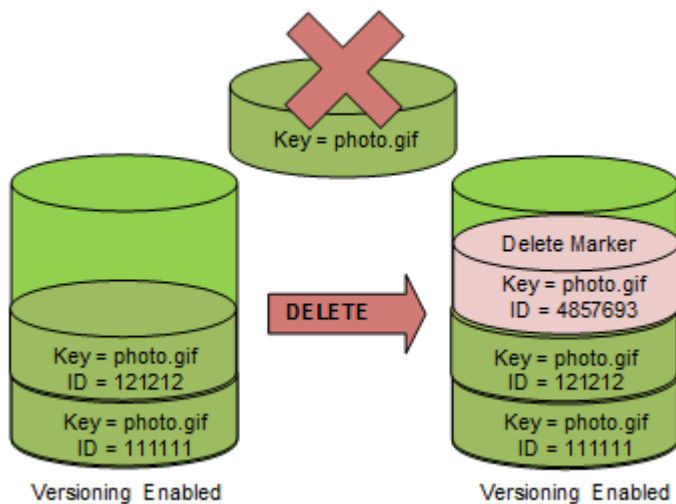
- L'oggetto originale (ID = 111111) rimane nel bucket.

- Amazon S3 genera un nuovo ID versione (121212) e aggiunge nel bucket questa versione più recente dell'oggetto.

Come funziona il controllo delle versioni di S3 quando si trova un oggetto in un bucket abilitato per il controllo delle versioni. PUT

Con questa funzionalità è possibile recuperare la versione precedente di un oggetto che è stato accidentalmente sovrascritto o eliminato.

Quando esegui l'operazione DELETE per un oggetto, tutte le versioni rimangono nel bucket e Amazon S3 inserisce un contrassegno di eliminazione, come mostrato nell'illustrazione seguente.



Il contrassegno di eliminazione diventa la versione corrente dell'oggetto. Per default, le richieste GET recuperano la versione più recente archiviata. L'esecuzione di una richiesta GET `Object` quando la versione corrente è un contrassegno di eliminazione restituisce un errore 404 `Not Found`, come mostrato nell'illustrazione seguente.

Una `GetObject` richiesta di un indicatore di eliminazione che restituisce un errore 404 (`Not Found`).

È possibile, tuttavia, eseguire un'operazione GET su una versione non corrente di un oggetto specificando l'ID versione corrispondente. Nell'illustrazione seguente viene eseguita un'operazione GET su una versione specifica dell'oggetto (111111). Amazon S3 restituisce la versione dell'oggetto anche se non è la versione corrente.

Per ulteriori informazioni, consulta [Recupero delle versioni degli oggetti da un bucket con funzione Controllo delle versioni abilitata](#).

Come funziona S3 Versioning quando si ha una versione non corrente in GET un bucket abilitato al versioning.

È possibile eliminare in modo permanente un oggetto specificando la versione che si desidera eliminare. Soltanto il proprietario del bucket di Amazon S3 o un utente IAM può eliminare definitivamente una versione. Se l'operazione DELETE specifica `versionId`, la versione dell'oggetto viene eliminata definitivamente e Amazon S3 non inserisce un contrassegno di eliminazione. Come elimina definitivamente DELETE `versionId` una versione specifica dell'oggetto.

Puoi aggiungere un ulteriore livello di sicurezza configurando un bucket per abilitare l'eliminazione con autenticazione a più fattori (MFA). Quando abiliti l'eliminazione MFA per un bucket, il proprietario del bucket deve includere due tipi di autenticazione in qualsiasi richiesta per eliminare una versione o modificare lo stato del controllo delle versioni del bucket. Per ulteriori informazioni, consulta [Configurazione dell'eliminazione di MFA](#).

Quando vengono create nuove versioni per un oggetto?

Le nuove versioni vengono create solo quando esegui l'operazione PUT per un nuovo oggetto. Tieni presente che alcune azioni, come `CopyObject`, funzionano implementando un'operazione PUT.

Alcune azioni che modificano l'oggetto corrente non creano una nuova versione perché non eseguono l'operazione PUT di un nuovo oggetto. Ciò include azioni come la modifica dei tag su un oggetto.

Important

Se rilevi un aumento significativo nel numero di risposte HTTP 503 (servizio non disponibile) ricevute per le richieste PUT o DELETE di Amazon S3 in un bucket con il controllo delle versioni S3 abilitato, è possibile che esistano uno o più oggetti nel bucket per i quali sono presenti milioni di versioni. Per ulteriori informazioni, consulta la sezione sul controllo delle versioni S3 in [Risoluzione dei problemi relativi al controllo delle versioni](#).

Abilitazione della funzione Controllo delle versioni sui bucket

È possibile utilizzare la funzione Controllo delle versioni S3 per mantenere più versioni di un oggetto in un bucket. Questa sezione fornisce esempi di come abilitare il controllo delle versioni su un bucket utilizzando la console, l'API REST, gli AWS SDK e (). AWS Command Line Interface AWS CLI

Note

Dopo aver abilitato il controllo delle versioni in un bucket per la prima volta, potrebbero essere necessari fino a 15 minuti per la propagazione completa della modifica nel sistema S3.

Durante questo periodo, le richieste GET per oggetti creati o aggiornati dopo aver abilitato il controllo delle versioni possono causare errori HTTP 404 NoSuchKey. È consigliabile attendere 15 minuti dopo aver abilitato il controllo delle versioni prima di eseguire operazioni di scrittura (PUT o DELETE) sugli oggetti nel bucket. Questo periodo di attesa consente di evitare potenziali problemi con la visibilità degli oggetti e il controllo delle versioni.

Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#). Per informazioni sull'utilizzo di oggetti che si trovano in bucket con la funzione Controllo delle versioni abilitata, consulta [Utilizzo di oggetti in un bucket che supporta la funzione Controllo delle versioni](#).

Per ulteriori informazioni su come utilizzare la funzionalità S3 di controllo delle versioni per proteggere i dati, consulta [Tutorial: Protezione dei dati su Amazon S3 da eliminazioni accidentali o bug delle applicazioni mediante le funzionalità S3 di controllo delle versioni, blocco degli oggetti e replica](#).

A ogni bucket S3 creato è associata una sottorisorsa per la funzione Controllo delle versioni. (Per ulteriori informazioni, consulta [Opzioni di configurazione dei bucket per uso generico](#).) Per impostazione predefinita, il bucket è senza versione, di conseguenza la sottorisorsa per la funzione Controllo delle versioni archivia una configurazione vuota della funzione Controllo delle versioni.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</VersioningConfiguration>
```

Per abilitare la funzione Controllo delle versioni, è possibile inviare una richiesta ad Amazon S3 con una configurazione della funzione che include lo stato.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

Per sospendere la funzione Controllo delle versioni, si imposterà il valore dello stato su Suspended.

Il proprietario del bucket e tutti gli utenti autorizzati possono abilitare il controllo delle versioni. Il proprietario del bucket è colui Account AWS che ha creato il bucket (l'account root). Per ulteriori informazioni sulle autorizzazioni, consultare [Identity and Access Management per Amazon S3](#).

Le sezioni seguenti forniscono maggiori dettagli sull'abilitazione del controllo delle versioni di S3 utilizzando la console e gli SDK AWS CLI. AWS

Utilizzo della console S3

Segui questi passaggi per utilizzare per abilitare il controllo delle versioni su Console di gestione AWS un bucket S3.

Come abilitare o disabilitare il controllo delle versioni su un bucket per uso generico S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket per il quale desideri abilitare il controllo delle versioni.
4. Scegliere Properties (Proprietà).
5. In Bucket Versioning (Funzione Controllo delle versioni del bucket) scegliere Edit (Modifica).
6. Scegliere Suspend (Sospendi) o Enable (Abilita), quindi scegliere Save changes (Salva modifiche).

Note

Puoi utilizzare l' AWS autenticazione a più fattori (MFA) con controllo delle versioni. Quando utilizzi l'MFA con controllo delle versioni, devi fornire le tue chiavi Account AWS di accesso e un codice valido dal dispositivo MFA dell'account per eliminare definitivamente una versione dell'oggetto o sospendere o riattivare il controllo delle versioni.

Per utilizzare l'autenticazione MFA con la funzione Controllo delle versioni, abilita MFA Delete. Non è possibile abilitare MFA Delete utilizzando la Console di gestione AWS. È necessario utilizzare () o l'API AWS Command Line Interface .AWS CLI Per ulteriori informazioni, consulta [Configurazione dell'eliminazione di MFA](#).

Utilizzo di AWS CLI

L'esempio seguente abilita il controllo delle versioni su un bucket per uso generico S3.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-configuration Status=Enabled
```

L'esempio seguente abilita il controllo delle versioni S3 e l'eliminazione dell'autenticazione a più fattori (MFA) su un bucket per un dispositivo MFA fisico. Per i dispositivi MFA fisici, nel parametro `--mfa`, inserisci una concatenazione del numero di serie del dispositivo MFA, uno spazio e il valore visualizzato sul dispositivo di autenticazione.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "SerialNumber 123456"
```

L'esempio seguente abilita il controllo delle versioni S3 e l'eliminazione dell'autenticazione a più fattori (MFA) su un bucket per un dispositivo MFA virtuale. Per i dispositivi MFA virtuali, nel parametro `--mfa`, inserisci una concatenazione dell'ARN del dispositivo MFA, uno spazio e il valore visualizzato sul dispositivo di autenticazione.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "arn:aws:iam::account-id:mfa/root-account-mfa-device 123789"
```

Note

L'utilizzo dell'eliminazione di MFA richiede un dispositivo di autenticazione fisico o virtuale approvato. Per ulteriori informazioni sull'utilizzo dell'eliminazione di MFA in Amazon S3, consulta [Configurazione dell'eliminazione di MFA](#).

Per ulteriori informazioni sull'abilitazione del controllo delle versioni utilizzando il AWS CLI, vedere <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3api/put-bucket-versioning.html> `put-bucket-versioning` nel Command Reference. AWS CLI

Utilizzo di AWS SDK

Gli esempi seguenti abilitano il controllo delle versioni su un bucket e quindi recuperano lo stato delle versioni utilizzando i tasti e the. AWS SDK per Java AWS SDK per .NET Per informazioni sull'utilizzo di altri SDK AWS , consulta il [Centro Developer di AWS](#).

.NET

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using System;
```

```
using Amazon.S3;
using Amazon.S3.Model;

namespace s3.amazon.com.docsamples
{
    class BucketVersioningConfiguration
    {
        static string bucketName = "**** bucket name ****";

        public static void Main(string[] args)
        {
            using (var client = new AmazonS3Client(Amazon.RegionEndpoint.USEast1))
            {
                try
                {
                    EnableVersioningOnBucket(client);
                    string bucketVersioningStatus =
RetrieveBucketVersioningConfiguration(client);
                }
                catch (AmazonS3Exception amazonS3Exception)
                {
                    if (amazonS3Exception.ErrorCode != null &&
                        (amazonS3Exception.ErrorCode.Equals("InvalidAccessKeyId")
                        ||
                        amazonS3Exception.ErrorCode.Equals("InvalidSecurity")))
                    {
                        Console.WriteLine("Check the provided AWS Credentials.");
                        Console.WriteLine(
                            "To sign up for service, go to http://aws.amazon.com/s3");
                    }
                    else
                    {
                        Console.WriteLine(
                            "Error occurred. Message:'{0}' when listing objects",
                            amazonS3Exception.Message);
                    }
                }
            }

            Console.WriteLine("Press any key to continue...");
            Console.ReadKey();
        }

        static void EnableVersioningOnBucket(IAmazonS3 client)
```

```
{

    PutBucketVersioningRequest request = new PutBucketVersioningRequest
    {
        BucketName = bucketName,
        VersioningConfig = new S3BucketVersioningConfig
        {
            Status = VersionStatus.Enabled
        }
    };

    PutBucketVersioningResponse response =
client.PutBucketVersioning(request);
}

static string RetrieveBucketVersioningConfiguration(IAmazonS3 client)
{
    GetBucketVersioningRequest request = new GetBucketVersioningRequest
    {
        BucketName = bucketName
    };

    GetBucketVersioningResponse response =
client.GetBucketVersioning(request);
    return response.VersioningConfig.Status;
}
}
```

Java

Per istruzioni su come creare e testare un campione funzionante, consulta [Getting Started](#) nella AWS SDK per Java Developer Guide.

```
import java.io.IOException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Region;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.AmazonS3Exception;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
```



```

import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;

public class BucketVersioningConfigurationExample {
    public static String bucketName = "**** bucket name ****";
    public static AmazonS3Client s3Client;

    public static void main(String[] args) throws IOException {
        s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
        s3Client.setRegion(Region.getRegion(Regions.US_EAST_1));
        try {

            // 1. Enable versioning on the bucket.
            BucketVersioningConfiguration configuration =
                new BucketVersioningConfiguration().withStatus("Enabled");

            SetBucketVersioningConfigurationRequest setBucketVersioningConfigurationRequest
            =
                new SetBucketVersioningConfigurationRequest(bucketName, configuration);

            s3Client.setBucketVersioningConfiguration(setBucketVersioningConfigurationRequest);

            // 2. Get bucket versioning configuration information.
            BucketVersioningConfiguration conf =
            s3Client.getBucketVersioningConfiguration(bucketName);
            System.out.println("bucket versioning configuration status:    " +
            conf.getStatus());

            } catch (AmazonS3Exception amazonS3Exception) {
                System.out.format("An Amazon S3 error occurred. Exception: %s",
            amazonS3Exception.toString());
            } catch (Exception ex) {
                System.out.format("Exception: %s", ex.toString());
            }
        }
    }
}

```

Python

Nel seguente codice Python di esempio viene creato un bucket Amazon S3, viene abilitato per il controllo delle versioni e viene configurato un ciclo di vita che fa scadere le versioni degli oggetti non simultanee dopo 7 giorni.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
    lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.

    Usage is shown in the usage_demo_single_object function at the end of this
    module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                    configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
```

```
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

Configurazione dell'eliminazione di MFA

Quando si utilizza la funzione Controllo delle versioni S3 nei bucket Amazon S3, puoi aggiungere un altro livello di sicurezza configurando un bucket per abilitare l'eliminazione MFA (autenticazione a più fattori). In tal caso, il proprietario del bucket deve includere due tipi di autenticazione in qualsiasi richiesta per eliminare una versione o modificare lo stato della funzione Controllo delle versioni del bucket.

La cancellazione MFA richiede autenticazione aggiuntiva per le seguenti operazioni:

- Modifica dello stato della funzione Controllo delle versioni del bucket

- Eliminazione permanente della versione di un oggetto

La cancellazione MFA richiede due forme di autenticazione contemporaneamente:

- Le credenziali di sicurezza
- la sequenza di un numero di serie valido, uno spazio e il codice a sei cifre visualizzato sul dispositivo di autenticazione approvato.

La cancellazione MFA fornisce così una protezione ulteriore, ad esempio se le credenziali di sicurezza fossero compromesse. L'eliminazione di MFA può aiutare a prevenire le eliminazioni accidentali dei bucket richiedendo all'utente che avvia l'azione di eliminazione di dimostrare il possesso fisico di un dispositivo MFA con un codice MFA e aggiungendo un ulteriore livello di interazione e sicurezza all'azione di eliminazione.

Per identificare i bucket con la funzionalità di eliminazione dell'autenticazione a più fattori (MFA) abilitata, puoi utilizzare i parametri di Amazon S3 Storage Lens. S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti. Per ulteriori informazioni, consulta [Valutazione dell'attività e dell'utilizzo dello storage con S3 Storage Lens](#). Per un elenco completo dei parametri, consulta [Glossario dei parametri di S3 Storage](#).

Il proprietario del bucket, colui Account AWS che ha creato il bucket (account root) e tutti gli utenti autorizzati possono abilitare il controllo delle versioni. Tuttavia, solo il proprietario del bucket (account root) può abilitare l'eliminazione di MFA. Per ulteriori informazioni, consulta [Security Access to AWS Using MFA](#) nel Security Blog. AWS

Note

Per utilizzare l'eliminazione MFA con la funzione Controllo delle versioni, abilita MFA Delete. Tuttavia, non è possibile abilitare MFA Delete l'utilizzo la Console di gestione AWS. È necessario utilizzare AWS Command Line Interface (AWS CLI) o l'API.

Per esempi sull'utilizzo dell'eliminazione MFA con il controllo delle versioni, consulta la sezione degli esempi nell'argomento [Abilitazione della funzione Controllo delle versioni sui bucket](#).

Non puoi utilizzare l'eliminazione MFA con le configurazioni del ciclo di vita. Per ulteriori informazioni sulle configurazioni del ciclo di vita e sul modo in cui interagiscono con altre

configurazioni, consulta [Come il ciclo di vita S3 interagisce con altre configurazioni del bucket](#).

Per abilitare o disabilitare la cancellazione MFA si ricorre alla stessa API utilizzata per configurare la funzione Controllo delle versioni di un bucket. Amazon S3 archivia la configurazione della cancellazione MFA nella stessa sottorisorsa della funzione Controllo delle versioni che contiene lo stato della funzione Controllo delle versioni del bucket.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>VersioningState</Status>
  <MfaDelete>MfaDeleteState</MfaDelete>
</VersioningConfiguration>
```

Per usare la cancellazione MFA si può utilizzare un dispositivo MFA fisico o virtuale per generare un codice di autenticazione. L'esempio seguente mostra il codice di autenticazione generato visualizzato su un dispositivo hardware.



L'eliminazione MFA e l'accesso alle MFA-protected API sono funzionalità destinate a fornire protezione per diversi scenari. È possibile configurare l'eliminazione MFA su un bucket per garantire che i dati contenuti nel bucket non possano essere eliminati accidentalmente. MFA-protected L'accesso alle API viene utilizzato per applicare un altro fattore di autenticazione (codice MFA) quando si accede a risorse sensibili di Amazon S3. Puoi richiedere che qualsiasi operazione su tali risorse di Amazon S3 venga eseguita fornendo credenziali temporanee create utilizzando MFA. Per un esempio, consulta [Richiesta dell'autenticazione a più fattori \(MFA\)](#).

Per ulteriori informazioni su come acquistare e attivare un dispositivo di autenticazione, consulta autenticazione. [Multi-factor](#)

Abilitazione del controllo delle versioni S3 e configurazione dell'eliminazione MFA

Utilizzo di AWS CLI

Il numero di serie è il numero che identifica in modo univoco il dispositivo MFA. Per i dispositivi MFA fisici, si tratta del numero di serie univoco fornito con il dispositivo. Per i dispositivi MFA virtuali, il

numero di serie è l'ARN del dispositivo. Per utilizzare i seguenti comandi, sostituisci *user input placeholders* con le tue specifiche informazioni.

L'esempio seguente abilita il controllo delle versioni S3 e l'eliminazione dell'autenticazione a più fattori (MFA) su un bucket per un dispositivo MFA fisico. Per i dispositivi MFA fisici, nel parametro `--mfa`, inserisci una concatenazione del numero di serie del dispositivo MFA, uno spazio e il valore visualizzato sul dispositivo di autenticazione.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "SerialNumber 123456"
```

L'esempio seguente abilita il controllo delle versioni S3 e l'eliminazione dell'autenticazione a più fattori (MFA) su un bucket per un dispositivo MFA virtuale. Per i dispositivi MFA virtuali, nel parametro `--mfa`, inserisci una concatenazione dell'ARN del dispositivo MFA, uno spazio e il valore visualizzato sul dispositivo di autenticazione.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "arn:aws:iam::account-id:mfa/root-account-mfa-device 123789"
```

Per ulteriori informazioni, consulta l'articolo AWS RePost [Come posso attivare l'eliminazione MFA per il mio bucket Amazon S3?](#).

Utilizzo della REST API

Per ulteriori informazioni su come specificare l'eliminazione dell'MFA utilizzando l'API REST di Amazon S3, consulta [PutBucketVersioning](#) Amazon Simple Storage Service API Reference.

Utilizzo di oggetti in un bucket che supporta la funzione Controllo delle versioni

Gli oggetti che sono stati archiviati nel bucket Amazon S3 prima dell'impostazione dello stato della funzione Controllo delle versioni hanno un ID versione `null`. Quando si abilita la funzione Controllo delle versioni, gli oggetti esistenti nel bucket non si modificano. Ciò che cambia è il modo in cui Amazon S3 gestirà gli oggetti delle richieste future.

Trasferimento delle versioni di un oggetto

È possibile definire regole di configurazione del ciclo di vita per gli oggetti con un ciclo di vita ben definito per trasferire le versioni di tali oggetti alla classe di archiviazione S3 Glacier Flexible Retrieval

(Recupero flessibile S3 Glacier) in uno specifico momento del ciclo di vita. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#).

Gli argomenti di questa sezione illustrano varie operazioni sugli oggetti di un bucket che supporta la funzione Controllo delle versioni. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

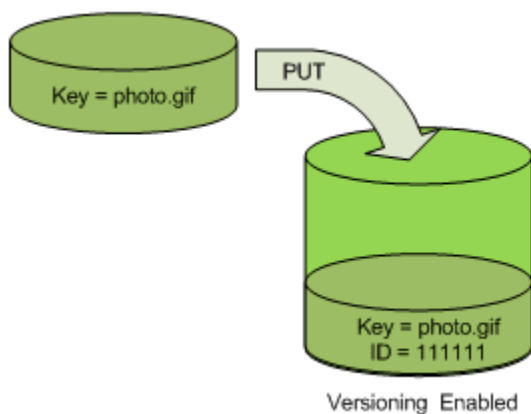
Argomenti

- [Aggiunta di oggetti a bucket che supportano la funzione Controllo delle versioni](#)
- [Elenchi di oggetti in un bucket che supporta la funzione Controllo delle versioni](#)
- [Recupero delle versioni degli oggetti da un bucket con funzione Controllo delle versioni abilitata](#)
- [Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata](#)
- [Configurazione delle autorizzazioni degli oggetti con versione](#)

Aggiunta di oggetti a bucket che supportano la funzione Controllo delle versioni

Dopo aver abilitato la funzione Controllo delle versioni del bucket, Amazon S3 aggiungerà automaticamente un ID versione univoco a ogni oggetto archiviato (utilizzando PUT, POST o CopyObject) nel bucket.

La figura seguente mostra l'aggiunta di un ID univoco a un oggetto da parte di Amazon S3 quando l'oggetto viene aggiunto a un bucket con la funzione Controllo delle versioni abilitata.



Note

I valori degli ID versione assegnati da Amazon S3 sono compatibili con l'URL (possono essere inclusi in un URI).

Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#). Puoi aggiungere versioni degli oggetti a un bucket abilitato per il controllo delle versioni utilizzando la console, gli SDK e l'API REST. AWS

Utilizzo della console

Per istruzioni, consulta [Caricamento degli oggetti](#).

Utilizzo di AWS SDK

Per esempi di caricamento di oggetti utilizzando gli AWS SDK per Java, .NET e PHP, consulta [Caricamento degli oggetti](#). Gli esempi di caricamento di oggetti in bucket senza versione e con funzione Controllo delle versioni abilitata sono identici ma, nel caso dei bucket con funzione Controllo delle versioni abilitata, Amazon S3 assegna un numero di versione. Negli altri casi il numero di versione è null.

Per informazioni sull'utilizzo di altri AWS SDK, consulta il [AWS Developer Center](#).

Utilizzo della REST API

Per aggiungere oggetti a bucket che supportano la funzione Controllo delle versioni

1. Abilitare la funzione Controllo delle versioni del bucket tramite una richiesta `PutBucketVersioning`.

Per ulteriori informazioni, consulta [PutBucketVersioning](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

2. Inviare una richiesta `PUT`, `POST` o `CopyObject` per memorizzare un oggetto nel bucket.

Quando si aggiunge un oggetto a un bucket con la funzione Controllo delle versioni abilitata, Amazon S3 restituisce l'ID versione dell'oggetto nell'intestazione di risposta `x-amz-version-id`, come mostrato nell'esempio di seguito.

```
x-amz-version-id: 3/L4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY
```

Elenchi di oggetti in un bucket che supporta la funzione Controllo delle versioni

Questa sezione fornisce esempi di elenchi di versioni di oggetti di un bucket con funzione Controllo delle versioni abilitata. Amazon S3 archivia le informazioni sulla versione di un oggetto nella sottorisorsa versioni associata al bucket. Per ulteriori informazioni, consulta [Opzioni di configurazione](#)

[dei bucket per uso generico](#). Per elencare gli oggetti in un bucket con il controllo delle versioni abilitato, è necessario disporre dell'autorizzazione `ListBucketVersions`.

Utilizzo della console S3

Segui questi passaggi per utilizzare la console di Amazon S3 per visualizzare le varie versioni di un oggetto.

Per visualizzare più versioni di un oggetto

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Per visualizzare un elenco delle versioni degli oggetti nel bucket, scegli l'opzione Show versions (Mostra versioni).

Per ogni versione dell'oggetto, la console mostra un ID versione univoco, la data e l'ora di creazione della versione e altre proprietà. Gli oggetti archiviati nel bucket prima dell'impostazione dello stato della funzione Controllo delle versioni hanno un ID versione null.

Per elencare gli oggetti senza le versioni, scegliere l'opzione List versions (Elenca versioni) .

Puoi anche visualizzare, scaricare ed eliminare le versioni degli oggetti nel riquadro di panoramica sull'oggetto della console. Per ulteriori informazioni, consulta [Visualizzazione delle proprietà di un oggetto nella console di Amazon S3](#).

Note

Per accedere alle versioni degli oggetti precedenti a 300 versioni, è necessario utilizzare la AWS CLI o l'URL dell'oggetto.

Important

È possibile annullare l'eliminazione di un oggetto solo se è stato eliminato come ultima versione (corrente). Non è possibile annullare l'eliminazione della versione precedente di un oggetto eliminato. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Utilizzo di AWS SDK

Gli esempi di questa sezione mostrano come recuperare un elenco di oggetti da un bucket con funzione Controllo delle versioni abilitata. Ogni richiesta restituisce fino a 1.000 versioni, a meno che non sia stato specificato un valore inferiore. Se il bucket contiene un numero di versioni superiore a tale limite, sarà necessario inviare una serie di richieste per recuperare un elenco di tutte le versioni. Questo processo di restituzione di risultati in "pagine" è chiamato paginazione.

Per illustrare il funzionamento della paginazione, gli esempi limitano ogni risposta a due versioni di un oggetto. Dopo aver recuperato la prima pagina di risultati, ogni esempio verifica se l'elenco delle versioni è troncato. In caso affermativo, l'esempio continua recuperando pagine fino al recupero di tutte le versioni.

Note

Gli esempi seguenti operano anche con un bucket che non ha la funzione Controllo delle versioni abilitata o per gli oggetti che non hanno versioni specifiche. In questi casi Amazon S3 restituisce l'elenco di oggetti con la versione ID null.

Per informazioni sull'utilizzo di altri AWS SDK, consulta il [AWS Developer Center](#).

Java

Per istruzioni su come creare e testare un campione funzionante, consulta [Getting Started](#) nella AWS SDK per Java Developer Guide.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListVersionsRequest;
import com.amazonaws.services.s3.model.S3VersionSummary;
import com.amazonaws.services.s3.model.VersionListing;

public class ListKeysVersioningEnabledBucket {

    public static void main(String[] args) {
```

```
Regions clientRegion = Regions.DEFAULT_REGION;
String bucketName = "**** Bucket name ****";

try {
    AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
        .withCredentials(new ProfileCredentialsProvider())
        .withRegion(clientRegion)
        .build();

    // Retrieve the list of versions. If the bucket contains more versions
    // than the specified maximum number of results, Amazon S3 returns
    // one page of results per request.
    ListVersionsRequest request = new ListVersionsRequest()
        .withBucketName(bucketName)
        .withMaxResults(2);
    VersionListing versionListing = s3Client.listVersions(request);
    int numVersions = 0, numPages = 0;
    while (true) {
        numPages++;
        for (S3VersionSummary objectSummary :
versionListing.getVersionSummaries()) {
            System.out.printf("Retrieved object %s, version %s\n",
                objectSummary.getKey(),
                objectSummary.getVersionId());
            numVersions++;
        }
        // Check whether there are more pages of versions to retrieve. If
        // there are, retrieve them. Otherwise, exit the loop.
        if (versionListing.isTruncated()) {
            versionListing =
s3Client.listNextBatchOfVersions(versionListing);
        } else {
            break;
        }
    }
    System.out.println(numVersions + " object versions retrieved in " +
numPages + " pages");
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it, so it returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
```

```
        e.printStackTrace();
    }
}
}
```

.NET

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella AWS SDK for .NET Developer Guide.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ListObjectsVersioningEnabledBucketTest
    {
        static string bucketName = "**** bucket name ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
        RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main(string[] args)
        {
            s3Client = new AmazonS3Client(bucketRegion);
            GetObjectListWithAllVersionsAsync().Wait();
        }

        static async Task GetObjectListWithAllVersionsAsync()
        {
            try
            {
                ListVersionsRequest request = new ListVersionsRequest()
                {
                    BucketName = bucketName,
                    // You can optionally specify key name prefix in the request
                    // if you want list of object versions of a specific object.
                }
            }
        }
    }
}
```

```
        // For this example we limit response to return list of 2
versions.
        MaxKeys = 2
    };
    do
    {
        ListVersionsResponse response = await
s3Client.ListVersionsAsync(request);
        // Process response.
        foreach (S3ObjectVersion entry in response.Versions)
        {
            Console.WriteLine("key = {0} size = {1}",
                entry.Key, entry.Size);
        }

        // If response is truncated, set the marker to get the next
        // set of keys.
        if (response.IsTruncated)
        {
            request.KeyMarker = response.NextKeyMarker;
            request.VersionIdMarker = response.NextVersionIdMarker;
        }
        else
        {
            request = null;
        }
    } while (request != null);
}
catch (AmazonS3Exception e)
{
    Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
}
catch (Exception e)
{
    Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
}
}
}
```

Utilizzo della REST API

Example- Un elenco di tutte le versioni degli oggetti di un bucket

Per visualizzare un elenco di tutte le versioni degli oggetti in un bucket, utilizzare la sottorisorsa `versions` in una richiesta GET Bucket. Amazon S3 può recuperare fino a 1.000 oggetti e ogni versione di oggetto è conteggiata interamente come oggetto. Quindi se un bucket contiene due chiavi (ad esempio, `photo.gif` e `picture.jpg`) e la prima ha 990 versioni mentre la seconda ne ha 400, con una singola richiesta si potrebbero recuperare tutte le 990 versioni `photo.gif` e solo le 10 più recenti di `picture.jpg`.

Amazon S3 restituisce le versioni degli oggetti nell'ordine inverso rispetto a come sono state archiviate, ovvero l'ultima verrà restituita per prima.

Nella richiesta GET Bucket, includere la sottorisorsa `versions`.

```
GET /?versions HTTP/1.1
Host: bucketName.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 +0000
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Example- Recupero di tutte le versioni di una chiave

Per recuperare un sottoinsieme di versioni di un oggetto, usa i parametri di richiesta per GET Bucket. Per ulteriori informazioni, consulta [GET Bucket](#).

1. Impostare il parametro `prefix` sulla chiave dell'oggetto che si desidera recuperare.
2. Inviare una richiesta GET Bucket utilizzando la sottorisorsa `versions` e `prefix`.

```
GET /?versions&prefix=objectName HTTP/1.1
```

Example- Recupero di oggetti tramite un prefisso

Nell'esempio seguente vengono recuperati gli oggetti la cui chiave è o inizia con `myObject`.

```
GET /?versions&prefix=myObject HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Si possono utilizzare altri parametri di richiesta per recuperare un sottoinsieme di tutte le versioni dell'oggetto. Per ulteriori informazioni, consulta [GET Bucket](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Example- Recupero di un elenco di oggetti aggiuntivi se la risposta viene troncata

Se il numero di oggetti che possono essere restituiti in una richiesta GET supera il valore di `max-keys`, la risposta conterrà `<isTruncated>true</isTruncated>` e includerà la prima chiave (in `NextKeyMarker`) e il primo ID versione (in `NextVersionIdMarker`) che soddisfano la richiesta, ma che non sono stati restituiti. Si utilizzano i valori restituiti come posizione di inizio di una richiesta successiva per recuperare gli ulteriori oggetti che soddisfano la richiesta GET.

Utilizzare la procedura seguente per recuperare gli ulteriori oggetti di un bucket che soddisfano la richiesta `GET Bucket versions` originaria. Per ulteriori informazioni su `key-marker`, `version-id-marker`, `NextKeyMarker` e `NextVersionIdMarker`, consulta la sezione [GET Bucket](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Di seguito sono riportate le risposte aggiuntive che soddisfano la richiesta GET originale:

- Impostare il valore di `key-marker` sulla chiave restituita in `NextKeyMarker` nella risposta precedente.
- Impostare il valore di `version-id-marker` sull'ID versione restituito in `NextVersionIdMarker` nella risposta precedente.
- Inviare una richiesta `GET Bucket versions` utilizzando `key-marker` e `version-id-marker`.

Example- Recupero di oggetto che iniziano con la chiave e l'ID versione specificati

```
GET /?versions&key-marker=myObject&version-id-marker=298459348571 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Utilizzo di AWS CLI

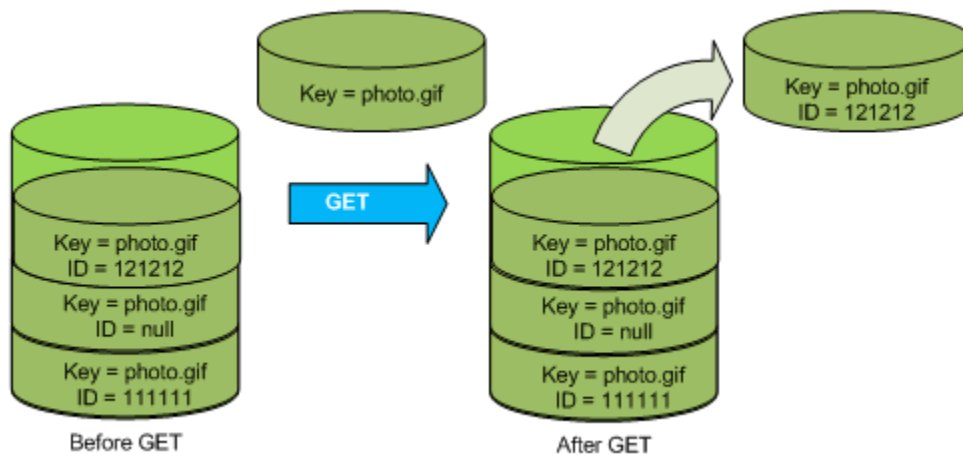
Il comando seguente restituisce i metadati relativi a tutte le versioni degli oggetti in un bucket.

```
aws s3api list-object-versions --bucket amzn-s3-demo-bucket1
```

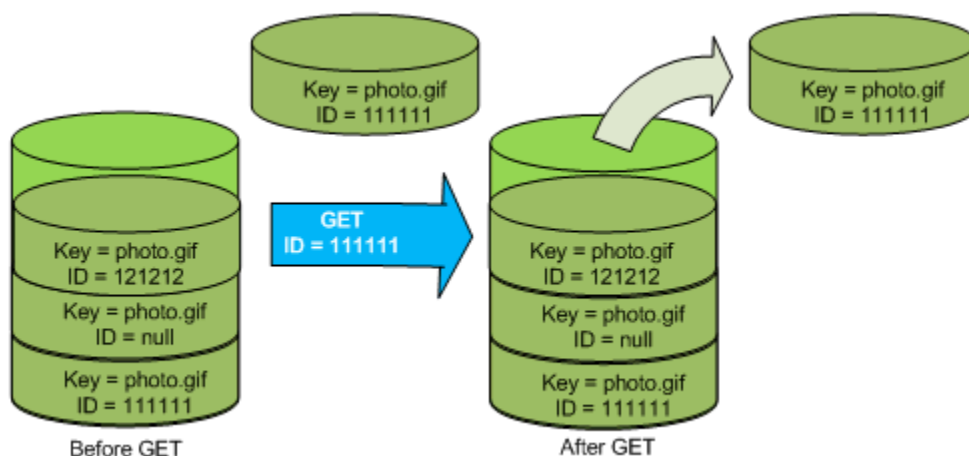
Per ulteriori informazioni su `list-object-versions`, consulta [list-object-versions](#) nel Riferimento ai comandi AWS CLI.

Recupero delle versioni degli oggetti da un bucket con funzione Controllo delle versioni abilitata

La funzione Controllo delle versioni in Amazon S3 è un modo per mantenere più varianti di un oggetto nello stesso bucket. Una richiesta GET semplice consente di recuperare la versione corrente di un oggetto. La figura seguente mostra come GET restituisce la versione corrente dell'oggetto, `photo.gif`.



Per recuperare una specifica versione occorre indicare l'ID versione. La figura seguente mostra una richiesta `GET versionId` che restituisce la versione specificata dell'oggetto (che non è necessariamente la versione corrente).



Puoi recuperare le versioni degli oggetti in Amazon S3 utilizzando la console, gli AWS SDK o l'API REST.

 Note

Per accedere alle versioni degli oggetti precedenti a 300 versioni, è necessario utilizzare la AWS CLI o l'URL dell'oggetto.

Utilizzo della console S3

Puoi ripristinare una versione precedente di un oggetto utilizzando la console Amazon S3 eliminando la versione corrente. L'eliminazione della versione corrente rende la versione precedente la nuova versione corrente.

Per ripristinare una versione precedente eliminando la versione corrente

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti scegliere il nome dell'oggetto.
4. Scegliere le Versioni.

Amazon S3 mostra tutte le versioni per l'oggetto.

5. Seleziona la casella di controllo accanto all'ID della versione corrente (più recente) che desideri eliminare.
6. Scegliere Elimina.
7. Nella finestra di dialogo Elimina oggetti, immettete **permanently delete**, quindi scegliete Elimina oggetti.

Dopo aver eliminato la versione corrente, la versione precedente diventa la versione corrente.

Per scaricare una versione precedente

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti scegliere il nome dell'oggetto.
4. Scegliere le Versioni.

Amazon S3 mostra tutte le versioni per l'oggetto.

5. Selezionare la casella di controllo accanto all' ID versione per le versioni che si desidera recuperare.
6. Scegliere Azioni, scegliere Scarica e salvare l'oggetto.

È anche possibile visualizzare, scaricare ed eliminare le versioni degli oggetti nel pannello di panoramica sull'oggetto. Per ulteriori informazioni, consulta [Visualizzazione delle proprietà di un oggetto nella console di Amazon S3](#).

Note

Per copiare una versione precedente (rendendola la nuova versione corrente), utilizza gli AWS SDK AWS CLI o: questo approccio non è disponibile nella console Amazon S3. Per un esempio, consulta la scheda. AWS CLI

Important

È possibile annullare l'eliminazione di un oggetto solo se è stato eliminato come ultima versione (corrente). Non è possibile annullare l'eliminazione della versione precedente di un oggetto eliminato. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Utilizzo di AWS SDK

Gli esempi per il caricamento di oggetti in bucket senza versione e con funzione Controllo delle versioni abilitata, sono gli stessi. Tuttavia, per i bucket con funzione Controllo delle versioni abilitata, Amazon S3 assegna un numero di versione. Negli altri casi il numero di versione è null.

Per esempi di download di oggetti tramite AWS SDK per Java, .NET e PHP, vedete [Scaricamento di oggetti](#).

Per esempi di elenco della versione degli oggetti utilizzando gli AWS SDK per .NET e Rust, consulta [Elencare la versione degli oggetti in un bucket Amazon S3](#).

Utilizzo della REST API

Per recuperare una specifica versione di un oggetto

1. Impostare `versionId` sull'ID versione dell'oggetto che si desidera recuperare.
2. Inviare una richiesta `GET Object versionId`.

Example- Recupero di un oggetto con versione

La seguente richiesta recupera la versione `L4kqtJlcpXroDTDmpUMLUo` di `my-image.jpg`.

```
GET /my-image.jpg?versionId=L4kqtJlcpXroDTDmpUMLUo HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

È possibile recuperare solo i metadati di un oggetto (non il contenuto). Per informazioni, consulta [the section called “Recupero dei metadati di una versione”](#).

Per informazioni sul ripristino di una versione di un oggetto precedente, consulta [the section called “Ripristino di versioni precedenti”](#).

Recupero dei metadati di una versione di un oggetto

Se si desidera recuperare solo i metadati di un oggetto (e non il suo contenuto), si utilizza l'operazione `HEAD`. Per impostazione predefinita si otterranno i metadati della versione più recente. Per recuperare i metadati di una specifica versione di oggetto si indicherà l'ID versione.

Per recuperare i metadati di una versione di un oggetto

1. Impostare `versionId` sull'ID versione dell'oggetto di cui si desidera recuperare i metadati.
2. Inviare una richiesta `HEAD Object versionId`.

Example- Recupero dei metadati di un oggetto con versione

La richiesta seguente consente di recuperare i metadati della versione `3HL4kqCxf3vjVBH40NrjfkD` di `my-image.jpg`.

```
HEAD /my-image.jpg?versionId=3HL4kqCxf3vjVBH40NrjfkD HTTP/1.1
```

```
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Di seguito è illustrata una risposta di esempio.

```
HTTP/1.1 200 OK
x-amz-id-2: ef8yU9AS1ed40pIszj7UDNEHGran
x-amz-request-id: 318BC8BC143432E5
x-amz-version-id: 3HL4kqtJlcpXroDTDmjVBH40NrjfkD
Date: Wed, 28 Oct 2009 22:32:00 GMT
Last-Modified: Sun, 1 Jan 2006 12:00:00 GMT
ETag: "fba9dede5f27731c9771645a39863328"
Content-Length: 434234
Content-Type: text/plain
Connection: close
Server: AmazonS3
```

Ripristino di versioni precedenti

Puoi utilizzare il controllo delle versioni per recuperare le versioni precedenti di un oggetto. Esistono due metodi per farlo:

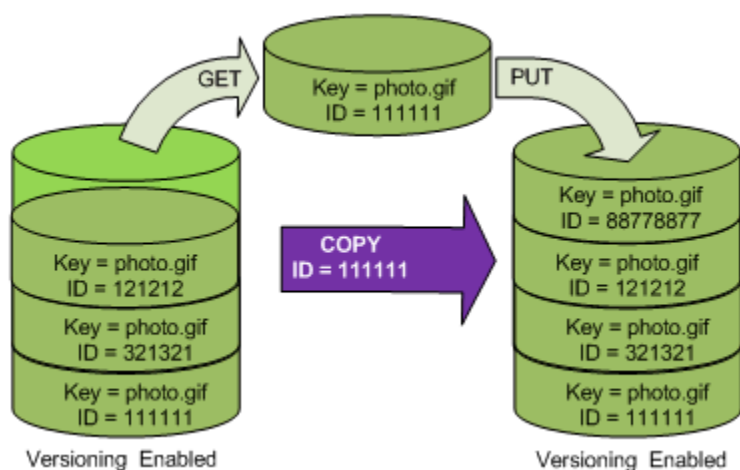
- Copiare una versione precedente dell'oggetto nello stesso bucket.

La copia diventa la versione corrente dell'oggetto e vengono conservate tutte le sue versioni.

- Eliminare definitivamente la versione corrente dell'oggetto.

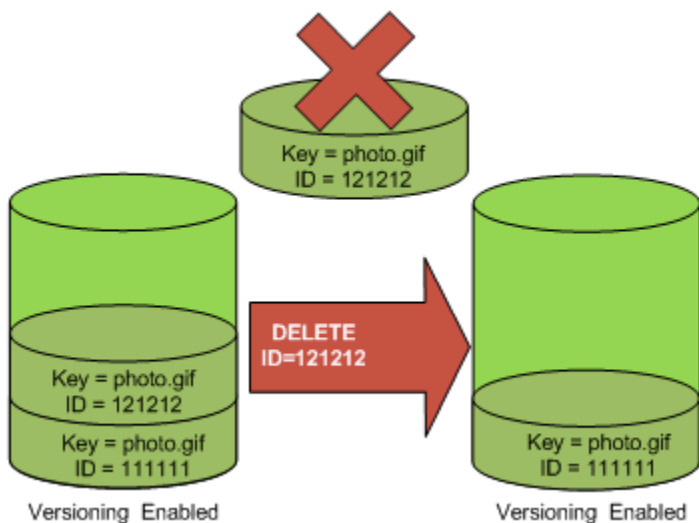
Così facendo, in effetti, la versione precedente diventa la versione corrente dell'oggetto.

Poiché vengono mantenute tutte le versioni dell'oggetto, è possibile trasformare una qualsiasi versione precedente nella versione corrente copiando una specifica versione dell'oggetto nello stesso bucket. Nella figura seguente l'oggetto di origine (ID = 111111) viene copiato nello stesso bucket. Amazon S3 fornisce un nuovo ID (88778877), che diventa la versione corrente dell'oggetto. In questo modo il bucket conterrà sia la versione originaria dell'oggetto (111111) che la sua copia (88778877). Per ulteriori informazioni su come ottenere una versione precedente e quindi caricarla per renderla la versione corrente, consulta [Recupero delle versioni degli oggetti da un bucket con funzione Controllo delle versioni abilitata](#) e [Caricamento di oggetti](#).



Una richiesta GET successiva recupera la versione 88778877.

La figura seguente mostra come l'eliminazione della versione corrente (121212) di un oggetto consente di lasciare la versione precedente (111111) come oggetto corrente. Per ulteriori informazioni sull'eliminazione di un oggetto, consulta [Eliminazione di un singolo oggetto](#).



Una richiesta GET successiva recupera la versione 111111.

Note

Per ripristinare le versioni degli oggetti in batch, puoi [utilizzare l'operazione CopyObject](#). L'operazione CopyObject copia ogni oggetto specificato nel manifesto. Tuttavia tieni presente che gli oggetti non vengono necessariamente copiati nello stesso ordine in cui appaiono nel manifesto. Per i bucket con versioni, se è importante mantenere l'ordine della

versione current/non corrente, è necessario copiare prima tutte le versioni non correnti. Quindi, al termine del primo processo, copia le versioni correnti in un processo successivo.

Come ripristinare le versioni precedenti degli oggetti

Per ulteriori indicazioni sul ripristino di oggetti eliminati, consulta [Come posso recuperare un oggetto Amazon S3 che è stato eliminato in un bucket abilitato al controllo delle versioni?](#) AWS re:Post nel Knowledge Center.

Utilizzo della console S3

Puoi ripristinare una versione precedente di un oggetto utilizzando la console Amazon S3 eliminando la versione corrente. L'eliminazione della versione corrente rende la versione precedente la nuova versione corrente.

Per ripristinare una versione precedente eliminando la versione corrente

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti scegliere il nome dell'oggetto.
4. Scegliere le Versioni.

Amazon S3 mostra tutte le versioni per l'oggetto.

5. Seleziona la casella di controllo accanto all'ID della versione corrente (più recente) che desideri eliminare.
6. Scegliere Elimina.
7. Nella finestra di dialogo Elimina oggetti, immettete **permanently delete**, quindi scegliete Elimina oggetti.

Dopo aver eliminato la versione corrente, la versione precedente diventa la versione corrente.

Per scaricare una versione precedente

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.

2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti scegliere il nome dell'oggetto.
4. Scegliere le Versioni.

Amazon S3 mostra tutte le versioni per l'oggetto.

5. Selezionare la casella di controllo accanto all' ID versione per le versioni che si desidera recuperare.
6. Scegliere Azioni, scegliere Scarica e salvare l'oggetto.

È anche possibile visualizzare, scaricare ed eliminare le versioni degli oggetti nel pannello di panoramica sull'oggetto. Per ulteriori informazioni, consulta [Visualizzazione delle proprietà di un oggetto nella console di Amazon S3](#).

Note

Per copiare una versione precedente (rendendola la nuova versione corrente), utilizza gli AWS SDK AWS CLI o: questo approccio non è disponibile nella console Amazon S3. Per un esempio, consulta la scheda. AWS CLI

Important

È possibile annullare l'eliminazione di un oggetto solo se è stato eliminato come ultima versione (corrente). Non è possibile annullare l'eliminazione della versione precedente di un oggetto eliminato. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Utilizzo di AWS CLI

Per ripristinare una versione precedente copiandola sul posto, usa il `copy-object` comando. Per il `--copy-source` parametro, specificate l'ID della versione precedente che desiderate ripristinare:

```
aws s3api copy-object \  
  --bucket amzn-s3-demo-bucket \  
  --key my-object.jpg \  
  --copy-source amzn-s3-demo-bucket/my-object.jpg?versionId=previous-version-id
```

Viene creata una nuova versione corrente dell'oggetto con il contenuto della versione precedente specificata. Amazon S3 conserva tutte le versioni esistenti.

Utilizzo di AWS SDK

Per informazioni sull'utilizzo di altri AWS SDK, consulta il [AWS Developer Center](#).

Python

Il seguente esempio di codice Python ripristina la versione precedente di un oggetto con versione eliminando tutte le versioni che si sono succedute dopo la versione di rollback specificata.

```
def rollback_object(bucket, object_key, version_id):
    """
    Rolls back an object to an earlier version by deleting all versions that
    occurred after the specified rollback version.

    Usage is shown in the usage_demo_single_object function at the end of this
    module.

    :param bucket: The bucket that holds the object to roll back.
    :param object_key: The object to roll back.
    :param version_id: The version ID to roll back to.
    """
    # Versions must be sorted by last_modified date because delete markers are
    # at the end of the list even when they are interspersed in time.
    versions = sorted(
        bucket.object_versions.filter(Prefix=object_key),
        key=attrgetter("last_modified"),
        reverse=True,
    )

    logger.debug(
        "Got versions:\n%s",
        "\n".join(
            [
                f"\t{version.version_id}, last modified {version.last_modified}"
                for version in versions
            ]
        ),
    )

    if version_id in [ver.version_id for ver in versions]:
        print(f"Rolling back to version {version_id}")
```



```
for version in versions:
    if version.version_id != version_id:
        version.delete()
        print(f"Deleted version {version.version_id}")
    else:
        break

print(f"Active version is now {bucket.Object(object_key).version_id}")
else:
    raise KeyError(
        f"{version_id} was not found in the list of versions for "
        f"{object_key}."
    )
```

Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata

È possibile eliminare le versioni degli oggetti dai bucket Amazon S3 ogni volta che si desidera. Si possono anche definire regole di configurazione del ciclo di vita per oggetti con un ciclo di vita ben definito per fare in modo che Amazon S3 forzi la scadenza delle versioni correnti di un oggetto o che rimuova le versioni dell'oggetto non correnti in modo permanente. Se il bucket ha la funzionalità Controllo delle versioni abilitata o sospesa, le operazioni di configurazione del ciclo di vita agiscono nel modo seguente:

- L'operazione `Expiration` si applica alla versione corrente dell'oggetto. Aniché eliminare la versione corrente dell'oggetto, Amazon S3 la conserva come versione non corrente aggiungendo un contrassegno di eliminazione, che quindi diventa la versione corrente.
- L'operazione `NoncurrentVersionExpiration` si applica solo alle versioni non correnti di un oggetto e Amazon S3 rimuove queste versioni in modo permanente. Non è possibile ripristinare gli oggetti rimossi in modo permanente.

Per ulteriori informazioni sul ciclo di vita S3, consulta [Gestione del ciclo di vita degli oggetti](#) e [Esempi di configurazioni del ciclo di vita S3](#).

Per visualizzare il numero di versioni di oggetti correnti e non correnti presenti nei tuoi bucket, puoi utilizzare i parametri di Amazon S3 Storage Lens. S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di

organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti. Per ulteriori informazioni, consulta la sezione [Utilizzo di S3 Storage Lens per ottimizzare i costi di archiviazione](#). Per un elenco completo dei parametri, consulta [Glossario dei parametri di S3 Storage](#).

Note

A ogni versione archiviata e trasferita di un oggetto, incluse le versioni dell'oggetto non corrente, si applicano le tariffe Amazon S3 normali. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

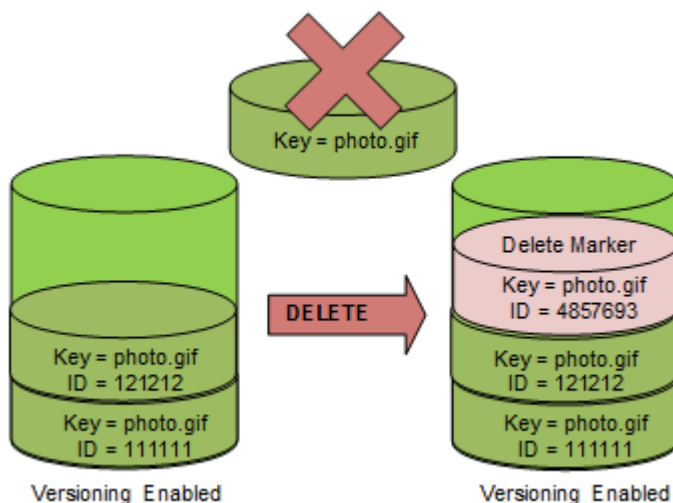
Eliminare casi di utilizzo delle richieste

Una richiesta DELETE può essere usata nei seguenti casi d'uso:

- Quando la funzione Controllo delle versioni è abilitata, un semplice DELETE non può eliminare un oggetto in modo permanente. (Una richiesta DELETE semplice è una richiesta che non specifica un ID versione.) Invece di eliminare l'oggetto, Amazon S3 inserisce un contrassegno di eliminazione nel bucket e tale contrassegno diventa la versione corrente dell'oggetto, con un nuovo ID.

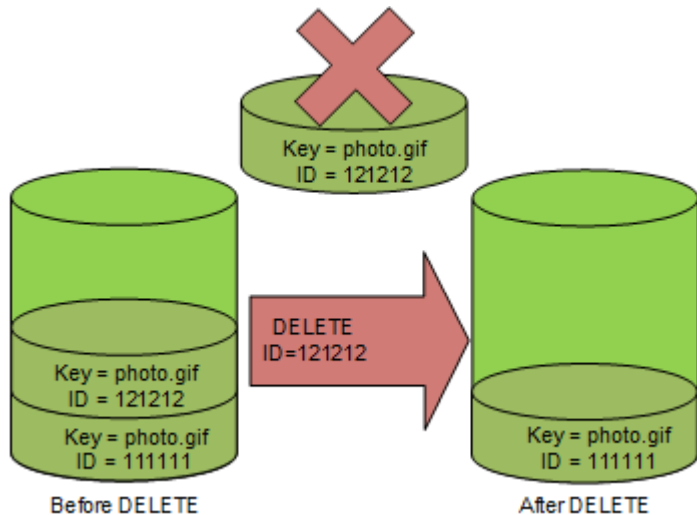
Quando si prova a utilizzare la funzione GET di un oggetto la cui versione corrente è un contrassegno di eliminazione, Amazon S3 si comporta come se l'oggetto fosse stato eliminato (anche se non è stato cancellato) e restituisce un errore 404. Per ulteriori informazioni, consulta [Utilizzo dei contrassegni di eliminazione](#).

La figura seguente mostra una richiesta DELETE semplice che non rimuove effettivamente l'oggetto specificato. Anziché rimuovere l'oggetto, Amazon S3 inserisce un contrassegno di eliminazione.



- Per eliminare oggetti con versione in modo permanente occorre usare `DELETE Object versionId`.

La figura seguente mostra una richiesta che l'eliminazione della versione specificata di un oggetto rimuove tale oggetto in modo permanente.



Per eliminare le versioni degli oggetti

Puoi eliminare le versioni degli oggetti in Amazon S3 utilizzando la console, gli AWS SDK, l'API REST o il AWS Command Line Interface

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
3. Nell'elenco Oggetti scegliere il nome dell'oggetto.
4. Scegliere le Versioni.

Amazon S3 mostra tutte le versioni per l'oggetto.

5. Seleziona la casella di controllo accanto a Version ID (ID versione) per le versioni che desideri recuperare.
6. Scegliere Elimina.
7. In Eliminare definitivamente gli oggetti? , immettere **permanently delete**.

 Warning

Quando si elimina definitivamente una versione di un oggetto, l'azione non può essere annullata.

8. Scegliere Delete objects (Elimina oggetti).

Amazon S3 elimina la versione dell'oggetto.

Utilizzo di AWS SDK

Per esempi di eliminazione di oggetti utilizzando gli AWS SDK per Java, .NET e PHP, consulta [Eliminazione di oggetti Amazon S3](#). Gli esempi per l'eliminazione di oggetti in bucket senza versione e con funzione Controllo delle versioni abilitata sono gli stessi. Tuttavia, per i bucket con funzione Controllo delle versioni abilitata, Amazon S3 assegna un numero di versione. Negli altri casi il numero di versione è null.

Per informazioni sull'utilizzo di altri AWS SDK, consulta il [AWS Developer Center](#).

Python

Nell'esempio di codice Python seguente viene illustrata l'eliminazione permanente di un oggetto con versione eliminando tutte le sue versioni.

```
def permanently_delete_object(bucket, object_key):
    """
    Permanently deletes a versioned object by deleting all of its versions.

    Usage is shown in the usage_demo_single_object function at the end of this
    module.

    :param bucket: The bucket that contains the object.
    :param object_key: The object to delete.
    """
    try:
        bucket.object_versions.filter(Prefix=object_key).delete()
        logger.info("Permanently deleted all versions of object %s.", object_key)
    except ClientError:
        logger.exception("Couldn't delete all versions of %s.", object_key)
        raise
```

Utilizzo della REST API

Per eliminare una versione specifica di un oggetto

- In una richiesta DELETE, specificare l'ID versione.

Example- Eliminazione di una versione specifica

Nell'esempio seguente viene eliminata la versione UI0RUnfnd89493jJFJ di photo.gif.

```
DELETE /photo.gif?versionId=UI0RUnfnd89493jJFJ HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
Content-Type: text/plain
Content-Length: 0
```

Utilizzo di AWS CLI

Il comando seguente elimina un oggetto denominato test.txt da un bucket denominato *amzn-s3-demo-bucket1*. Per rimuovere una versione specifica di un oggetto, devi essere il proprietario del bucket e utilizzare la risorsa secondaria ID versione.

```
aws s3api delete-object --bucket amzn-s3-demo-bucket1 --key test.txt --version-id versionID
```

Per ulteriori informazioni su delete-object, consulta [delete-object](#) nel Riferimento ai comandi AWS CLI .

Per ulteriori informazioni sull'eliminazione delle versioni degli oggetti, consulta gli argomenti riportati di seguito.

- [Utilizzo dei contrassegni di eliminazione](#)
- [Rimozione dei contrassegni di eliminazione per rendere corrente una versione precedente](#)
- [Eliminazione di un oggetto da un bucket con cancellazione MFA abilitata](#)

Utilizzo dei contrassegni di eliminazione

In Amazon S3, un contrassegno di eliminazione è il segnaposto (o contrassegno) di un oggetto con controllo delle versioni specificato in una richiesta DELETE semplice. Una richiesta DELETE semplice è una richiesta che non specifica un ID versione. Poiché l'oggetto si trova in un bucket con funzione Controllo delle versioni abilitata, non viene eliminato. Ma il contrassegno di eliminazione fa sì che Amazon S3 si comporti come se l'oggetto fosse stato eliminato. Puoi utilizzare una chiamata DELETE API di Amazon S3 su un contrassegno di eliminazione. A tale scopo, è necessario effettuare la DELETE richiesta utilizzando un utente o un ruolo AWS Identity and Access Management (IAM) con le autorizzazioni appropriate.

I contrassegni di eliminazione sono dotati di un nome chiave (o chiave) e di un ID versione, come qualsiasi altro oggetto. Tuttavia, differiscono da altri oggetti nei modi seguenti:

- Un contrassegno di eliminazione non dispone di dati associati.
- Un contrassegno di eliminazione non è associato a un valore della lista di controllo degli accessi (ACL).
- Se invii una richiesta GET per un contrassegno di eliminazione, la richiesta GET non recupera nulla perché un contrassegno di eliminazione non contiene dati. In particolare, quando la richiesta GET non specifica un `versionId`, viene visualizzato un errore 404 (Not Found).

I contrassegni di eliminazione accumulano un addebito minimo per l'archiviazione in Amazon S3. Le dimensioni di storage di un contrassegno di eliminazione corrispondono a quelle del suo nome delle chiavi. Un nome delle chiavi è una sequenza di caratteri Unicode. La UTF-8 codifica per il nome della chiave aggiunge 1-4 byte di spazio di archiviazione al bucket per ogni carattere del nome. I contrassegni di eliminazione sono archiviati nella classe di archiviazione S3 Standard.

Per scoprire quanti contrassegni di eliminazione sono impostati e in quale classe di archiviazione sono archiviati, puoi usare Amazon S3 Storage Lens. Per ulteriori informazioni, consulta [Monitoraggio dell'attività e dell'utilizzo dello storage con Amazon S3 Storage Lens](#) e [Glossario dei parametri di Amazon S3 Storage Lens](#).

Per ulteriori informazioni sui nomi delle chiavi, consultare [Denominazione di oggetti Amazon S3](#). Per informazioni sull'eliminazione di un contrassegno di eliminazione, consultare [Gestione dei contrassegni di eliminazione](#).

Solo Amazon S3 può creare un contrassegno di eliminazione e compie questa operazione ogni volta che si invia una richiesta `DeleteObject` relativa a un oggetto di un bucket con funzione

Controllo delle versioni abilitata o sospesa. L'oggetto specificato nella richiesta DELETE non viene effettivamente eliminato. Invece il contrassegno di eliminazione diventa la versione corrente dell'oggetto. Il nome della chiave dell'oggetto (o chiave) diventa la chiave del contrassegno di eliminazione.

Quando ottieni un oggetto senza specificare un `versionId` nella richiesta, se la versione corrente è un contrassegno di eliminazione, Amazon S3 risponde con quanto segue:

- Un errore 404 (Not Found)
- Un'intestazione di risposta, `x-amz-delete-marker: true`

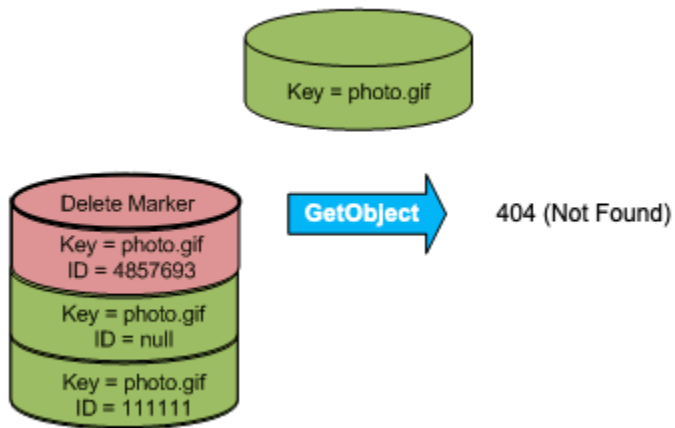
Quando ottieni un oggetto specificando un `versionId` nella richiesta, se la versione specificata è un contrassegno di eliminazione, Amazon S3 risponde con quanto segue:

- Un errore di tipo 405 (metodo non concesso)
- Un'intestazione di risposta, `x-amz-delete-marker: true`
- Un'intestazione di risposta, `Last-Modified: timestamp` (solo quando si utilizzano le operazioni o API) [HeadObject](#) [GetObject](#)

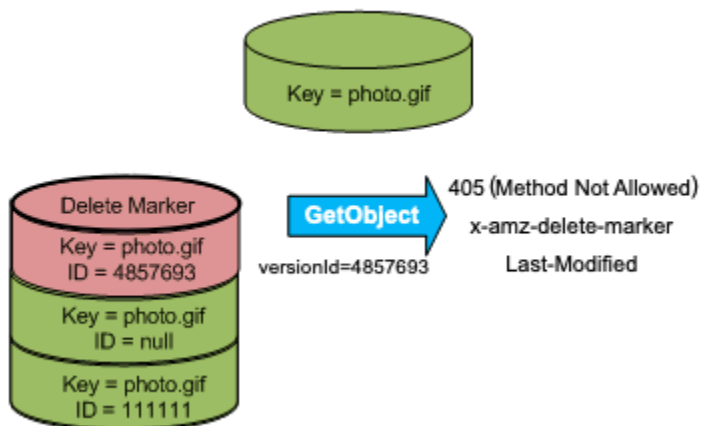
L'intestazione della risposta `x-amz-delete-marker: true` indica che l'oggetto a cui è stato effettuato l'accesso è un contrassegno di eliminazione. Questa intestazione della risposta non restituisce mai `false`, perché quando il valore è `false`, la versione corrente o specificata dell'oggetto non è un indicatore di eliminazione.

L'intestazione della risposta `Last-Modified` fornisce l'ora di creazione dei contrassegni di eliminazione.

La figura seguente mostra come una chiamata API `GetObject` su un oggetto la cui versione corrente è un contrassegno di eliminazione risponde con un errore 404 (Not Found) e l'intestazione della risposta include `x-amz-delete-marker: true`.

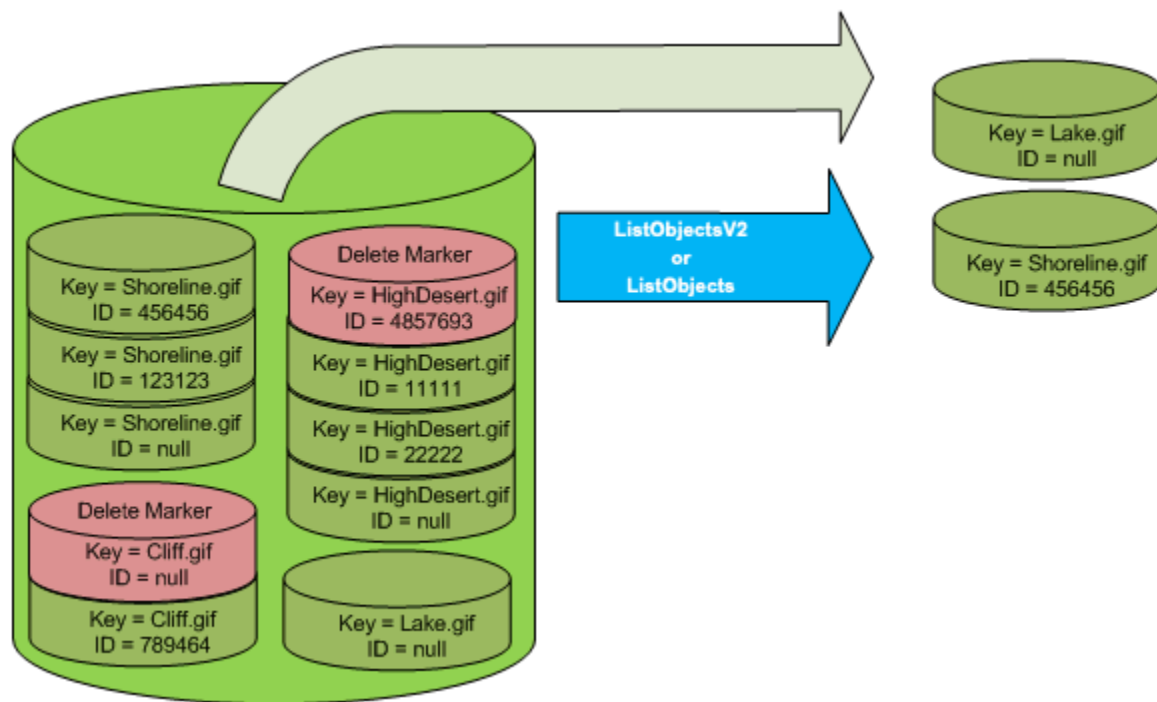


Se effettui una chiamata `GetObject` su un oggetto specificando un `versionId` nella richiesta e se la versione specificata è un contrassegno di eliminazione, Amazon S3 risponde con un errore 405 (Method Not Allowed) e le intestazioni della risposta includono `x-amz-delete-marker: true` e `Last-Modified: timestamp`.



Anche se sovrascritti, gli indicatori di eliminazione rimangono nelle versioni degli oggetti. L'unico modo per ottenere l'elenco degli indicatori di eliminazione (e di altre versioni di un oggetto) è utilizzare una richiesta [ListObjectVersions](#). È possibile effettuare questa richiesta nella Console di gestione AWS elencando gli oggetti di un bucket per uso generico e selezionando Mostra versioni. Per ulteriori informazioni, consulta [Elenchi di oggetti in un bucket che supporta la funzione Controllo delle versioni](#).

La figura seguente mostra che una richiesta [ListObjectsV2](#) o [ListObjects](#) non restituisce gli oggetti la cui versione corrente è un contrassegno di eliminazione.



Gestione dei contrassegni di eliminazione

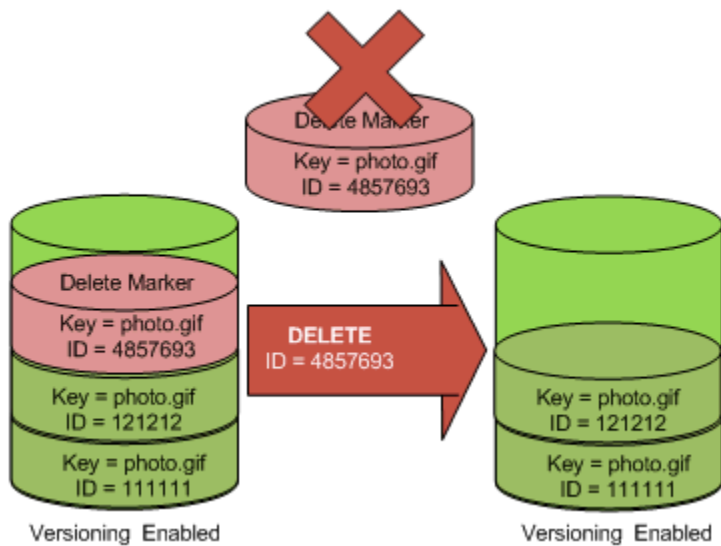
Configurazione del ciclo di vita per ripulire automaticamente i contrassegni di eliminazione scaduti

Un contrassegno di eliminazione oggetto scaduto è un elemento in cui tutte le versioni dell'oggetto vengono eliminate e rimane solo un singolo contrassegno di eliminazione. Se la configurazione relativa al ciclo di vita è impostata per eliminare le versioni correnti oppure l'opzione `ExpiredObjectDeleteMarker` è impostata in modo esplicito, Amazon S3 rimuove il contrassegno di eliminazione dell'oggetto scaduto. Per un esempio, consulta [Rimozione dei contrassegni di eliminazione degli oggetti scaduti in un bucket con il controllo delle versioni abilitato](#).

Rimozione dei contrassegni di eliminazione per rendere corrente una versione precedente

Quando si elimina un oggetto in un bucket che supporta la funzione Controllo delle versioni, tutte le versioni rimangono nel bucket e Amazon S3 crea un contrassegno di eliminazione per l'oggetto. Per annullare l'eliminazione dell'oggetto, è necessario eliminare il contrassegno di eliminazione. Per ulteriori informazioni sulla funzione Controllo delle versioni e sui contrassegni di eliminazione, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Per eliminare definitivamente un contrassegno di eliminazione occorre includere il suo ID versione nella richiesta `DeleteObject versionId`. La figura seguente mostra una richiesta `DeleteObject versionId` che rimuove definitivamente un contrassegno di eliminazione.

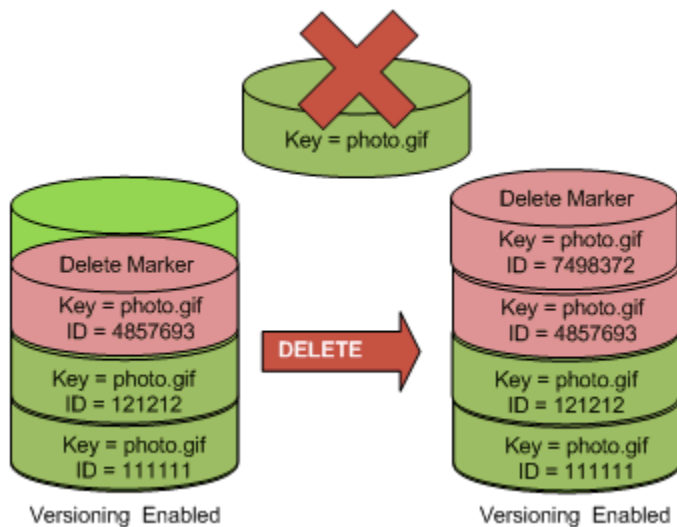


L'effetto della rimozione del contrassegno di eliminazione è che una richiesta GET semplice non recupererà l'ID versione corrente (121212) dell'oggetto.

Note

Se si utilizza una richiesta `DeleteObject` per eliminare un contrassegno di eliminazione (senza specificare l'ID versione del contrassegno), Amazon S3 non elimina il contrassegno, ma PUTs inserisce un altro contrassegno di eliminazione.

Per rimuovere un contrassegno di eliminazione con un ID di versione NULL, è necessario passare il NULL come ID di versione nella richiesta `DeleteObject`. La figura seguente mostra come una semplice richiesta `DeleteObject` effettuata senza un ID di versione, in cui la versione corrente è un marker di eliminazione, non rimuove nulla, ma aggiunge invece un marker di eliminazione ulteriore con un ID di versione univoco (7498372).



Utilizzo della console S3

Utilizzare la seguente procedura per recuperare gli oggetti eliminati che non sono cartelle dal bucket S3, inclusi gli oggetti che si trovano all'interno di tali cartelle.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket scegli il nome del bucket desiderato.
3. Per visualizzare un elenco delle versioni degli oggetti nel bucket, scegliere l'opzione List versions (Elenca versioni). Verranno visualizzati i contrassegni di eliminazione degli oggetti eliminati.
4. Per annullare l'eliminazione di un oggetto, è necessario eliminare il contrassegno di eliminazione. Selezionare la casella di controllo accanto al contrassegno di eliminazione dell'oggetto da recuperare, quindi scegliere Delete (Elimina).
5. Conferma l'eliminazione nella pagina Delete objects (Elimina oggetti) .
 - a. In Permanently delete objects? (Eliminare definitivamente gli oggetti?), specifica **permanently delete**.
 - b. Scegliere Delete objects (Elimina oggetti).

Note

Non puoi utilizzare la console di Amazon S3 per annullare l'eliminazione delle cartelle. È necessario utilizzare l'SDK AWS CLI or. Per gli esempi, consulta [Come posso ripristinare](#)

[un oggetto Amazon S3 eliminato da un bucket con il controllo delle versioni abilitato?](#) nel Knowledge Center di AWS .

Utilizzo di REST API

Per rimuovere definitivamente un contrassegno di eliminazione

1. Impostare `versionId` sull'ID versione del contrassegno di eliminazione che si desidera rimuovere.
2. Inviare una richiesta `DELETE Object versionId`.

Example- Rimozione di un contrassegno di eliminazione

Il seguente esempio consente di rimuovere il contrassegno di eliminazione della versione budget 4857693 di `photo.gif`.

```
DELETE /photo.gif?versionId=4857693 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Quando si elimina un contrassegno di eliminazione, Amazon S3 include nella risposta:

```
204 NoContent
x-amz-version-id: versionID
x-amz-delete-marker: true
```

Utilizzo di AWS SDK

Per informazioni sull'utilizzo di altri AWS SDK, consulta il [AWS Developer Center](#).

Python

Nell'esempio di codice Python seguente viene illustrato come rimuovere un marker di eliminazione da un oggetto, rendendo quindi la versione non corrente più recente la versione corrente dell'oggetto.

```
def revive_object(bucket, object_key):
    """
```

Revives a versioned object that was deleted by removing the object's active delete marker.

A versioned object presents as deleted when its latest version is a delete marker.

By removing the delete marker, we make the previous version the latest version and the object then presents as **not** deleted.

Usage is shown in the `usage_demo_single_object` function at the end of this module.

```
:param bucket: The bucket that contains the object.
:param object_key: The object to revive.
"""

# Get the latest version for the object.
response = s3.meta.client.list_object_versions(
    Bucket=bucket.name, Prefix=object_key, MaxKeys=1
)

if "DeleteMarkers" in response:
    latest_version = response["DeleteMarkers"][0]
    if latest_version["IsLatest"]:
        logger.info(
            "Object %s was indeed deleted on %s. Let's revive it.",
            object_key,
            latest_version["LastModified"],
        )
        obj = bucket.Object(object_key)
        obj.Version(latest_version["VersionId"]).delete()
        logger.info(
            "Revived %s, active version is now %s with body '%s'",
            object_key,
            obj.version_id,
            obj.get()["Body"].read(),
        )
    else:
        logger.warning(
            "Delete marker is not the latest version for %s!", object_key
        )
elif "Versions" in response:
    logger.warning("Got an active version for %s, nothing to do.", object_key)
else:
    logger.error("Couldn't get any version info for %s.", object_key)
```

Eliminazione di un oggetto da un bucket con cancellazione MFA abilitata

Quando configuri l'eliminazione MFA, solo l'utente root può eliminare definitivamente le versioni degli oggetti o modificare la configurazione del controllo delle versioni sul bucket S3. È necessario utilizzare un dispositivo MFA per autenticare l'utente root a eseguire l'azione di eliminazione.

Se la configurazione della funzione Controllo delle versioni comprende l'abilitazione della cancellazione MFA, il proprietario del bucket deve includere l'intestazione `x-amz-mfa` nelle richieste per eliminare definitivamente una versione dell'oggetto o per cambiare lo stato della funzione Controllo delle versioni del bucket. Le richieste che includono `x-amz-mfa` devono utilizzare l'HTTPS.

Il valore dell'intestazione è dato dalla concatenazione del numero di serie del dispositivo di autenticazione, uno spazio e il codice di autenticazione visualizzato sul dispositivo. Se non si include questa intestazione di richiesta, la richiesta ha esito negativo.

Quando si utilizza, AWS CLI includi le stesse informazioni del valore del `mfa` parametro.

Per ulteriori informazioni sui dispositivi di autenticazione, vedere [Multi-factor Autenticazione](#).

Per ulteriori informazioni sull'abilitazione della cancellazione MFA, consultare [Configurazione dell'eliminazione di MFA](#).

Note

L'eliminazione di un oggetto in un bucket con controllo delle versioni che è abilitato all'eliminazione MFA non è disponibile tramite la Console di gestione AWS.

Utilizzo di AWS CLI

Utilizza il comando seguente per eliminare un oggetto in un bucket con controllo delle versioni che è abilitato all'eliminazione MFA. Quando si utilizza il seguente esempio di comando, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key OBJECT-KEY --version-id "VERSION ID" --mfa "MFA_DEVICE_SERIAL_NUMBER MFA_DEVICE_CODE"
```

Utilizzo della REST API

L'esempio seguente mostra come eliminare `my-image.jpg` (con la versione specificata), che risiede in un bucket configurato con l'eliminazione MFA abilitata.

Per ulteriori informazioni, consulta [DeleteObject](#) nella Guida di riferimento delle API di Amazon Simple Storage Service.

```
DELETE /my-image.jpg?versionId=3HL4kqCxf3vjVBH40NrjfkD HTTPS/1.1
Host: bucketName.s3.amazonaws.com
x-amz-mfa: 20899872 301749
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Configurazione delle autorizzazioni degli oggetti con versione

Le autorizzazioni per gli oggetti in Amazon S3 sono impostate a livello di versione. Ogni versione ha il proprio proprietario dell'oggetto. Chi Account AWS crea la versione dell'oggetto è il proprietario. È quindi possibile definire autorizzazioni diverse per versioni differenti dello stesso oggetto. A tale scopo occorre specificare l'ID versione dell'oggetto le cui autorizzazioni si desidera impostare in una richiesta PUT `Object versionId aCL`. Per una descrizione dettagliata e per le istruzioni di utilizzo delle ACL, consultare [Identity and Access Management per Amazon S3](#).

Example- Configurazione delle autorizzazioni di un oggetto con versione

La seguente richiesta imposta l'autorizzazione del beneficiario con ID utente canonico, `FULL_CONTROL` sulla

chiave `b4bf1b36f9716f094c3079dcf5ac9982d4f2847de46204d47448bc557fb5ac2a`, ID di versione `my-image.jpg`, `.3HL4kqtJvjVBH40NrjfkD`

```
PUT /my-image.jpg?acl&versionId=3HL4kqtJvjVBH40NrjfkD HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
Content-Length: 124

<AccessControlPolicy>
```

```
<Owner>
  <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
</Owner>
<AccessControlList>
  <Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
      <ID>a9a7b886d6fd24a52fe8ca5bef65f89a64e0193f23000e241bf9b1c61be666e9</ID>
    </Grantee>
    <Permission>FULL_CONTROL</Permission>
  </Grant>
</AccessControlList>
</AccessControlPolicy>
```

Analogamente, per conoscere le autorizzazioni della versione specifica di un oggetto, è necessario indicarne l'ID versione in una richiesta `GET Object versionId acl`. Includere l'ID versione è necessario perché, per impostazione predefinita, `GET Object acl` restituisce le autorizzazioni della versione corrente dell'oggetto.

Example- Recupero delle autorizzazioni della versione specificata di un oggetto

Nell'esempio seguente Amazon S3 restituisce le autorizzazioni per la chiave, `my-image.jpg`, ID versione, `DVBH40Nr8X8gUMLUo`.

```
GET /my-image.jpg?versionId=DVBH40Nr8X8gUMLUo&acl HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU
```

Per ulteriori informazioni, consulta [GetObjectAcl](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di oggetti di un bucket con funzione Controllo delle versioni sospesa

In Amazon S3 è possibile sospendere la funzione Controllo delle versioni per non accumulare nuove versioni dello stesso oggetto in un bucket. Potrebbe essere necessario farlo perché si desidera solo una singola versione di un oggetto in un bucket. In alternativa, potrebbe esservi la necessità di non voler accumulare addebiti per più versioni.

Quando si sospende la funzione Controllo delle versioni, gli oggetti esistenti nel bucket non si modificano. Ciò che cambia è il modo in cui Amazon S3 gestirà gli oggetti delle richieste future. Negli

argomenti di questa sezione vengono illustrate le varie operazioni degli oggetti in un bucket con la funzione Controllo delle versioni sospesa, tra cui l'aggiunta, il recupero e l'eliminazione di oggetti.

Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#). Per ulteriori informazioni sul recupero delle versioni degli oggetti, consulta la sezione [Recupero delle versioni degli oggetti da un bucket con funzione Controllo delle versioni abilitata](#).

Argomenti

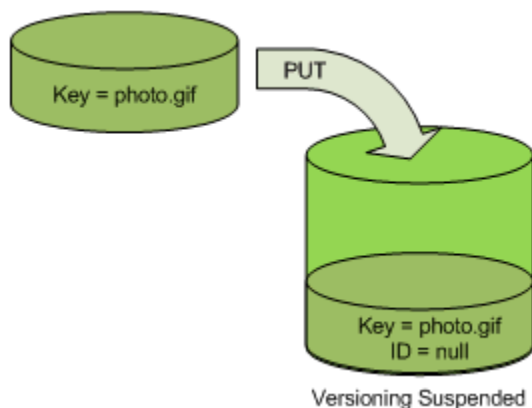
- [Aggiunta di oggetti a bucket con funzione Controllo delle versioni sospesa](#)
- [Recupero di oggetti da bucket con funzione Controllo delle versioni sospesa](#)
- [Eliminazione di oggetti da bucket con funzione Controllo delle versioni sospesa](#)

Aggiunta di oggetti a bucket con funzione Controllo delle versioni sospesa

Puoi aggiungere oggetti a bucket con la funzione Controllo delle versioni sospesa in Amazon S3 per creare l'oggetto con ID versione null o sovrascrivere una qualsiasi versione dell'oggetto con un ID versione corrispondente.

Dopo la sospensione della funzione Controllo delle versioni di un bucket, Amazon S3 aggiungerà automaticamente un ID versione null a ogni oggetto archiviato successivamente (utilizzando PUT, POST o CopyObject) nel bucket.

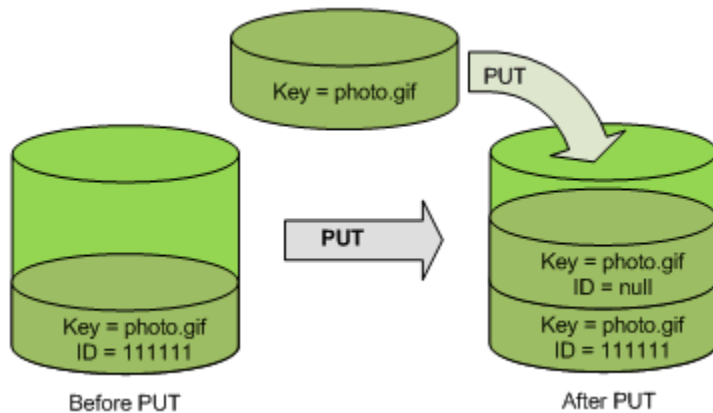
La figura seguente mostra l'aggiunta dell'ID versione null a un oggetto da parte di Amazon S3 quando l'oggetto viene aggiunto a un bucket con funzione Controllo delle versioni abilitata.



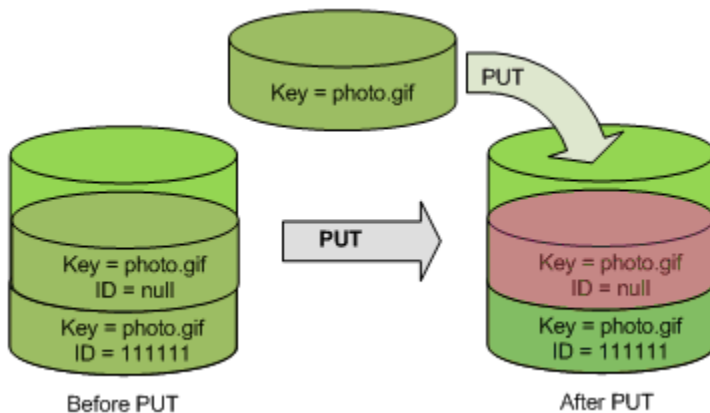
Se nel bucket è già presente una versione null e si aggiunge un altro oggetto con la stessa chiave, l'oggetto così aggiunto sovrascrive la versione null originaria.

Se il bucket contiene oggetti con versione, la versione della funzione PUT diventa quella corrente dell'oggetto. La figura seguente mostra come l'aggiunta di un oggetto a un bucket contenente oggetti con versione non sovrascrive l'oggetto già presente nel bucket.

In questo caso, la versione 111111 risiedeva già nel bucket. Amazon S3 aggiunge un ID versione null all'oggetto da aggiungere e lo archivia nel bucket. La versione 111111 risulta ora sovrascritta.



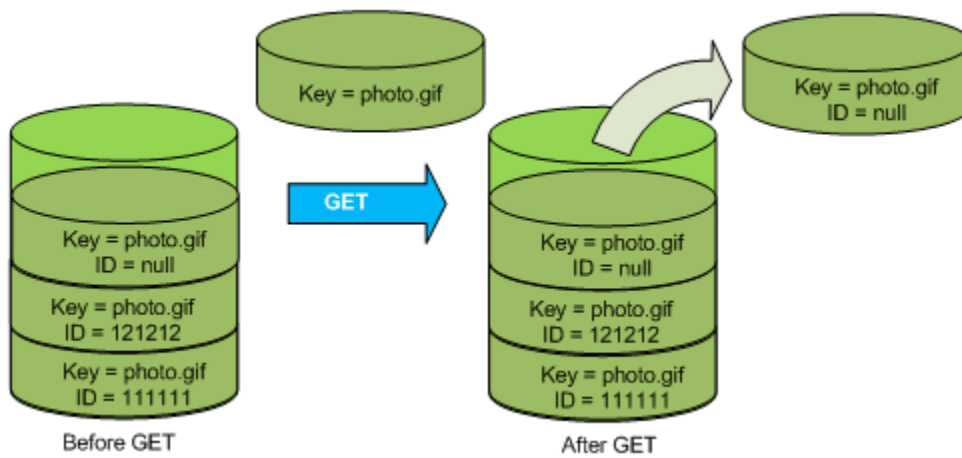
Se nel bucket è già presente una versione null, tale versione viene sovrascritta, come mostrato nell'illustrazione seguente.



Sebbene la chiave e l'ID (null) della versione null siano identici prima e dopo la richiesta PUT, i contenuti della versione null inizialmente memorizzati nel bucket vengono sostituiti da quelli dell'oggetto PUT per l'inserimento nel bucket.

Recupero di oggetti da bucket con funzione Controllo delle versioni sospesa

Le richieste GET Object restituiscono la versione corrente di un oggetto indipendentemente dal fatto che la funzione Controllo delle versioni del bucket sia stata abilitata o meno. La figura seguente mostra come un semplice GET restituisce la versione corrente di un oggetto.



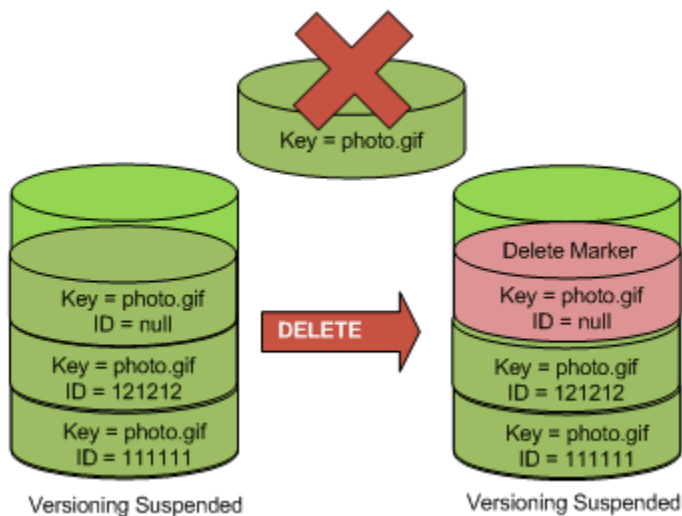
Eliminazione di oggetti da bucket con funzione Controllo delle versioni sospesa

È possibile eliminare oggetti da bucket con la funzione Controllo delle versioni sospesa per rimuovere un oggetto con ID versione null.

Se la funzione Controllo delle versioni è sospesa per un bucket, una richiesta DELETE:

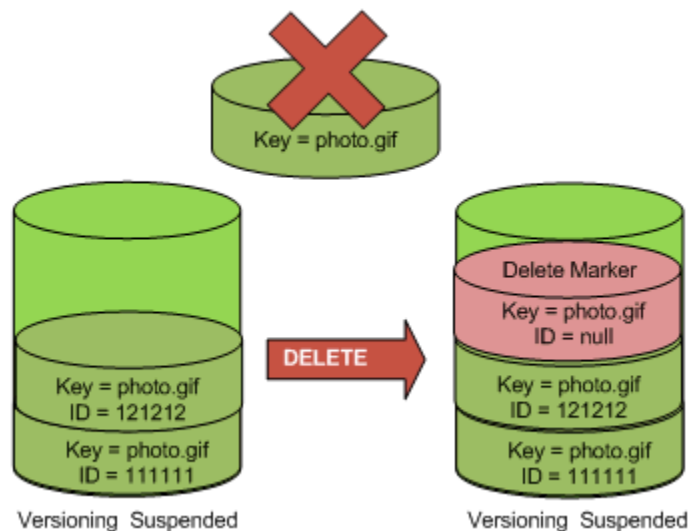
- Può rimuovere solo gli oggetti con ID versione null.
- Non rimuove alcun oggetto se non è presente una versione null dell'oggetto nel bucket.
- Inserisce un contrassegno di eliminazione nel bucket.

Se il controllo delle versioni del bucket è sospeso, l'operazione rimuove l'oggetto con un valore `versionId` null. Se è presente un ID versione, Amazon S3 inserisce un contrassegno di eliminazione che diventa la versione corrente dell'oggetto. La figura seguente mostra come una semplice richiesta DELETE rimuove una versione null e Amazon S3 inserisce un contrassegno di eliminazione al suo posto con ID versione null.



Per eliminare definitivamente un oggetto con `versionId`, è necessario includere il valore `versionId` dell'oggetto nella richiesta. Poiché un contrassegno di eliminazione non include alcun contenuto, il contenuto della versione `null` viene perso quando viene sostituito da un contrassegno di eliminazione.

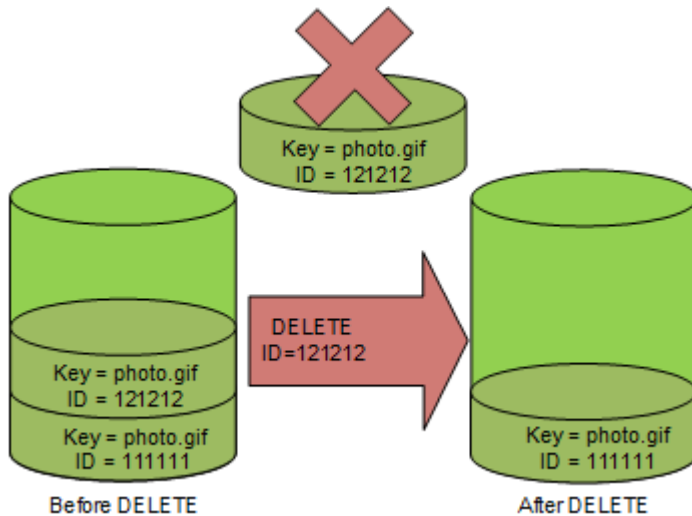
La figura seguente mostra un bucket che non contiene versioni `null`. In questo caso `DELETE` non rimuove nulla. Anziché rimuovere l'oggetto, Amazon S3 inserisce semplicemente un contrassegno di eliminazione.



Anche in un bucket con versione sospesa, il proprietario del bucket può eliminare definitivamente una versione specificata includendo l'ID della versione nella `DELETE` richiesta, a meno che le autorizzazioni per la richiesta non siano state negate esplicitamente. `DELETE` Ad esempio, per

negare l'eliminazione di qualsiasi oggetto con un ID di null versione, è necessario negare esplicitamente le autorizzazioni `and. s3:DeleteObject s3:DeleteObjectVersions`

La figura seguente mostra che l'eliminazione di una versione specificata di un oggetto rimuove tale oggetto in modo permanente. Solo il proprietario del bucket può eliminare la versione specificata di un oggetto.



Risoluzione dei problemi relativi al controllo delle versioni

I seguenti argomenti sono utili per risolvere alcuni problemi comuni relativi alla funzione Controllo delle versioni di Amazon S3.

Argomenti

- [Desidero recuperare oggetti che sono stati eliminati per errore in un bucket in cui la funzione Controllo delle versioni è abilitata](#)
- [Voglio eliminare definitivamente gli oggetti con il controllo delle versioni abilitato](#)
- [Sto riscontrando un peggioramento delle prestazioni dopo aver abilitato il controllo delle versioni del bucket](#)

Desidero recuperare oggetti che sono stati eliminati per errore in un bucket in cui la funzione Controllo delle versioni è abilitata

In generale, quando le versioni degli oggetti vengono eliminate dai bucket S3, Amazon S3 non può più recuperarle. Tuttavia, se hai abilitato la funzione S3 Controllo delle versioni sul tuo bucket S3, una richiesta DELETE che non specifica un ID di versione non può eliminare definitivamente un oggetto.

Viene invece aggiunto un contrassegno di eliminazione come segnaposto. Questo contrassegno di eliminazione diventa la versione corrente dell'oggetto.

Per verificare se gli oggetti eliminati sono rimossi definitivamente o temporaneamente (sostituiti da un contrassegno di eliminazione), procedi come segue:

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) scegliere il nome del bucket contenente l'oggetto.
4. Nell'elenco Oggetti, attiva il controllo Mostra versioni a destra della barra di ricerca, quindi cerca l'oggetto eliminato nella barra di ricerca. Questo controllo è disponibile solo se la funzione Controllo delle versioni è stata precedentemente abilitata nel bucket.

Puoi anche utilizzare [S3 Inventory per cercare gli oggetti eliminati](#).

5. Se non riesci a trovare l'oggetto dopo aver attivato il controllo Mostra versioni o dopo avere creato un report di inventario non riesci a trovare il [contrassegno di eliminazione](#) dell'oggetto, significa che l'eliminazione è permanente e l'oggetto non può più essere recuperato.

Puoi anche verificare lo stato di un oggetto eliminato utilizzando l'operazione HeadObject API di AWS Command Line Interface (AWS CLI). A tale scopo, utilizza il comando `head-object` e sostituisci *user input placeholders* con le tue informazioni.

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html
```

Se esegui il comando `head-object` su un oggetto con il controllo delle versioni abilitato la cui versione corrente è un contrassegno di cancellazione, riceverai un errore 404 Non trovato. Ad esempio:

Si è verificato un errore (404) durante la chiamata all' HeadObject operazione: Not Found

Se esegui il comando `head-object` su un oggetto con il controllo delle versioni abilitato e fornisci l'ID versione dell'oggetto, Amazon S3 recupera i metadati dell'oggetto, a conferma che l'oggetto esiste ancora e che non è stato eliminato definitivamente.

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html --  
version-id versionID
```

```
{
  "AcceptRanges": "bytes",
  "ContentType": "text/html",
  "LastModified": "Thu, 16 Apr 2015 18:19:14 GMT",
  "ContentLength": 77,
  "VersionId": "Zg5HyL7m.eZU9iM7AVlJkrqAiE.0UG4q",
  "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
  "Metadata": {}
}
```

Se l'oggetto viene trovato e la relativa versione più recente è un contrassegno di eliminazione, significa che la versione precedente dell'oggetto esiste ancora. Poiché il contrassegno di eliminazione corrisponde alla versione corrente dell'oggetto, è possibile recuperare l'oggetto eliminando il contrassegno di eliminazione.

Dopo aver rimosso definitivamente il contrassegno di eliminazione, la seconda versione più recente dell'oggetto diventa la versione corrente, rendendolo nuovamente disponibile. Per una rappresentazione visiva di come gli oggetti vengono recuperati, consulta [Rimozione dei contrassegni di eliminazione](#).

Per rimuovere una versione specifica di un oggetto, devi essere il proprietario del bucket. Per eliminare definitivamente un contrassegno di eliminazione occorre includere il suo ID versione nella richiesta `DeleteObject`. Per eliminare il contrassegno di eliminazione, usa il seguente comando e sostituisci *user input placeholders* con le tue informazioni:

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key index.html --
version-id versionID
```

Per ulteriori informazioni sul comando `delete-object`, consulta [delete-object](#) in the Guida di riferimento ai comandi della AWS CLI . Per informazioni sull'eliminazione definitiva dei contrassegni di eliminazione, consulta [Gestione dei contrassegni di eliminazione](#).

Voglio eliminare definitivamente gli oggetti con il controllo delle versioni abilitato

In un bucket con la funzione Controllo delle versioni abilitata, una richiesta DELETE senza un ID versione non può eliminare un oggetto definitivamente. Questo tipo di richiesta inserisce invece un contrassegno di eliminazione.

Per eliminare oggetti con la funzione Controllo delle versioni abilitata in modo permanente, puoi scegliere tra i seguenti metodi:

- Crea una regola del ciclo di vita S3 per eliminare definitivamente le versioni non correnti. Per eliminare in modo definitivo le versioni non correnti, in Elimina in modo definitivo le versioni non correnti degli oggetti, specifica il numero di giorni nel campo Numero di giorni dopo il quale gli oggetti diventano non correnti. Facoltativamente puoi specificare il numero di versioni più recenti da mantenere immettendo un valore nel campo Number of newer versions to retain (Numero di versioni più recenti da mantenere). Per ulteriori informazioni sulla creazione di questa regola, consulta l'argomento relativo all'[impostazione di una configurazione del ciclo di vita S3](#).
- Elimina una versione specificata includendo l'ID versione nella richiesta DELETE. Per ulteriori informazioni, consulta l'argomento relativo alla [procedura di eliminazione definitiva degli oggetti con controllo delle versioni abilitata](#).
- Crea una regola del ciclo di vita per far scadere le versioni correnti. Per definire la scadenza delle versioni correnti degli oggetti, seleziona Scadenza versioni correnti degli oggetti e aggiungi un numero in Giorni dopo la creazione degli oggetti. Per ulteriori informazioni sulla creazione di questa regola del ciclo di vita, consulta l'argomento relativo all'[impostazione di una configurazione del ciclo di vita S3](#).
- Per eliminare definitivamente tutti gli oggetti con il controllo delle versioni abilitato e i relativi contrassegni di eliminazione, crea due regole del ciclo di vita: una per far scadere le versioni correnti ed eliminare definitivamente le versioni non correnti degli oggetti e l'altra per eliminare i contrassegni di eliminazione degli oggetti scaduti.

In un bucket con il controllo delle versioni abilitato, una richiesta DELETE che non specifica un ID versione può rimuovere solo gli oggetti con un ID versione NULL. Se l'oggetto è stato caricato quando il controllo delle versioni era abilitato, una richiesta DELETE che non specifica un ID versione crea un contrassegno di eliminazione per tale oggetto.

Note

Per i Lock-enabled bucket S3 Object, una richiesta di DELETE oggetto con un ID di versione dell'oggetto protetto causa un errore 403 Access Denied. Una richiesta oggetto DELETE senza un ID versione aggiunge un contrassegno di eliminazione come versione più recente dell'oggetto con una risposta 200 OK. Gli oggetti protetti dalla funzionalità Blocco oggetti non possono essere eliminati definitivamente finché i relativi periodi di conservazione e blocchi a fini legali non vengono rimossi. Per ulteriori informazioni, consulta [the section called “Come funziona il blocco oggetti S3”](#).

Sto riscontrando un peggioramento delle prestazioni dopo aver abilitato il controllo delle versioni del bucket

Il peggioramento delle prestazioni può verificarsi nei bucket con il controllo delle versioni abilitato se sono presenti troppi contrassegni di eliminazione o oggetti con versioni e se non vengono seguite le best practice.

Numero eccessivo di contrassegni di eliminazione

Dopo aver abilitato la funzione Controllo delle versioni in un bucket, una richiesta DELETE senza un ID versione effettuata su un oggetto crea un contrassegno di eliminazione con un ID versione univoco. Le configurazioni del ciclo di vita con una regola Scadenza versioni correnti degli oggetti aggiungono un contrassegno di eliminazione con un ID versione univoco a ogni oggetto. Un numero eccessivo di contrassegni di eliminazione può ridurre le prestazioni nel bucket.

Se la funzione Controllo delle versioni viene disabilitata in un bucket, Amazon S3 contrassegna l'ID versione come NULL per i nuovi oggetti creati. Un'operazione di scadenza in un bucket con la funzione Controllo delle versioni disabilitata fa sì che Amazon S3 crei un contrassegno di eliminazione il cui ID versione è NULL. In un bucket con la funzione Controllo delle versioni disabilitata, viene creato un contrassegno di eliminazione NULL per ogni richiesta di eliminazione. Questi contrassegni di eliminazione NULL sono anche chiamati contrassegni di eliminazione degli oggetti scaduti quando tutte le versioni degli oggetti vengono eliminate e rimane solo un unico contrassegno di eliminazione. In presenza di un numero eccessivo di contrassegni di eliminazione NULL, si verifica un peggioramento delle prestazioni nel bucket.

Numero eccessivo di oggetti con il controllo delle versioni abilitato

Se un bucket con il controllo delle versioni abilitato contiene oggetti con milioni di versioni, può verificarsi un incremento del numero di errori di tipo 503 Servizio non disponibile. Se rilevi un aumento significativo del numero di risposte HTTP 503 Servizio non disponibile ricevute per le richieste oggetto PUT o DELETE in un bucket con il controllo delle versioni abilitato, è possibile che esistano uno o più oggetti nel bucket per i quali sono presenti milioni di versioni. In presenza di oggetti con milioni di versioni, Amazon S3 limita automaticamente le richieste a livello di bucket. La limitazione delle richieste consente di proteggere il bucket dal traffico generato da un numero eccessivo di richieste, che potrebbe potenzialmente impedire la gestione di altre richieste eseguite nello stesso bucket.

Per determinare quali oggetti sono dotati di milioni di versioni, utilizza S3 Inventory. S3 Inventory genera un report che fornisce un elenco di file flat degli oggetti in un bucket. Per ulteriori informazioni, consulta [Catalogazione e analisi dei dati con Inventario S3](#).

Per verificare se nel bucket è presente un numero elevato di oggetti con il controllo delle versioni abilitato, utilizza le metriche di S3 Storage Lens per visualizzare i valori pertinenti nei campi Conteggio oggetti versione corrente, Conteggio di oggetti versione non corrente e Conteggio oggetti contrassegno di eliminazione. Per ulteriori informazioni sulle metriche di Storage Lens, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

Il team Amazon S3 consiglia ai clienti di analizzare le applicazioni che sovrascrivono ripetutamente lo stesso oggetto, creando potenzialmente milioni di versioni per tale oggetto, al fine di determinare se il funzionamento dell'applicazione corrisponde a quello previsto. Ad esempio, un'applicazione che sovrascrive lo stesso oggetto ogni minuto per una settimana può creare oltre diecimila versioni. Si consiglia di archiviare meno di centomila versioni per ciascun oggetto. Se hai un caso d'uso che richiede milioni di versioni per uno o più oggetti, contatta il Supporto AWS team per ricevere assistenza nella determinazione di una soluzione migliore.

Best practice

Per evitare problemi di deterioramento delle prestazioni correlati al controllo delle versioni, consigliamo di adottare le seguenti best practice:

- Abilita una regola del ciclo di vita per far scadere le versioni precedenti degli oggetti. Ad esempio, è possibile creare una regola del ciclo di vita per far scadere le versioni non correnti dopo 30 giorni dal passaggio dell'oggetto allo stato non corrente. Puoi anche conservare più versioni non correnti se non desideri eliminarle tutte. Per ulteriori informazioni, consulta l'argomento relativo all'[impostazione di una configurazione del ciclo di vita S3](#).
- Abilita una regola del ciclo di vita per eliminare i contrassegni di eliminazione degli oggetti scaduti a cui non sono associati oggetti dati nel bucket. Per ulteriori informazioni, consulta l'argomento relativo alla [rimozione dei contrassegni di eliminazione degli oggetti scaduti](#).

Per ulteriori best practice per l'ottimizzazione delle prestazioni di Amazon S3, consulta [Modelli di progettazione delle best practice](#).

Blocco di oggetti con Object Lock

Object Lock S3 può impedire che gli oggetti Amazon S3 vengano eliminati o sovrascritti per un determinato periodo di tempo o in modo indefinito. Object Lock utilizza un modello write-once-read-many (WORM) per archiviare gli oggetti. È possibile utilizzare Object Lock per soddisfare i requisiti normativi che richiedono un'archiviazione WORM o per aggiungere un ulteriore livello di protezione contro le modifiche e l'eliminazione degli oggetti.

Note

Object Lock S3 è stato valutato da Cohasset Associates per l'utilizzo in ambienti soggetti alle normative SEC 17a-4, CTCC e FINRA. Per ulteriori informazioni su come Object Lock fa riferimento a queste normative, consulta [Cohasset Associates Compliance Assessment](#).

Il blocco degli oggetti offre due modi per gestire la conservazione degli oggetti: i periodi di conservazione e i blocchi a fini giudiziari. La versione di un oggetto può avere un periodo di conservazione, un blocco a fini legali o entrambi.

- **Periodo di conservazione:** un periodo di conservazione specifica un determinato intervallo di tempo durante il quale la versione di un oggetto rimane bloccata. È possibile impostare un periodo di conservazione univoco per singoli oggetti. Inoltre, è possibile impostare un periodo di conservazione predefinito su un bucket S3. È possibile anche limitare i periodi di conservazione minimi e massimi consentiti utilizzando la chiave di condizione `s3:object-lock-retention-days` nella policy del bucket. Questa chiave di condizione permette di definire il periodo di conservazione consentito. Per ulteriori informazioni, consulta [Impostazione di limiti su periodi di conservazione con una policy di bucket](#).
- **Blocco a fini legali:** un blocco a fini legali offre la stessa protezione di un periodo di conservazione ma non presenta una data di scadenza. pertanto rimane invariato fino a quando non viene rimosso esplicitamente. I blocchi a fini legali sono indipendenti dai periodi di conservazione e vengono applicati alle singole versioni degli oggetti.

Object Lock funziona solo nei bucket con il controllo delle versioni S3 abilitato. Quando si blocca una versione di un oggetto, Amazon S3 archivia le informazioni di blocco nei metadati per quella versione di oggetto. L'inserimento di un periodo di conservazione o di un blocco a fini legali in un oggetto protegge solo la versione specificata nella richiesta. I periodi di conservazione e i blocchi a fini legali non impediscono la creazione di nuove versioni dell'oggetto o l'aggiunta di contrassegni

di eliminazione all'oggetto. Per informazioni sulla funzione Controllo delle versioni S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Se si inserisce un oggetto in un bucket che contiene già un oggetto protetto esistente con lo stesso nome della chiave dell'oggetto, Amazon S3 crea una nuova versione dell'oggetto. La versione protetta esistente dell'oggetto rimane bloccata in base alla rispettiva configurazione di conservazione.

Note

Gli oggetti protetti da Object Lock (entrambe le modalità GOVERNANCE e COMPLIANCE) non consentono modifiche alle annotazioni (creazione, aggiornamento o eliminazione). L'`BypassGovernanceRetention` autorizzazione non si applica alle operazioni di annotazione. Per aggiungere annotazioni a un oggetto bloccato, create una nuova versione dell'oggetto. La nuova versione non è soggetta alle impostazioni di conservazione della versione precedente, a meno che non venga applicata esplicitamente ad essa.

Come funziona il blocco oggetti S3

Argomenti

- [Periodi di conservazione](#)
- [Modalità di conservazione](#)
- [Blocchi a fini giudiziari](#)
- [Come funzionano le eliminazioni con S3 Object Lock](#)
- [Best practice per l'utilizzo di S3 Object Lock](#)
- [Autorizzazioni richieste](#)

Periodi di conservazione

Un periodo di conservazione protegge una versione di un oggetto per un determinato intervallo di tempo. Quando imposti un periodo di conservazione per una versione di un oggetto, Amazon S3 archivia un timestamp nei metadati della versione dell'oggetto per indicare la scadenza del periodo di conservazione. Allo scadere del periodo di conservazione, la versione dell'oggetto può essere sovrascritta o eliminata.

È possibile inserire un periodo di conservazione in modo esplicito sulla versione di un singolo oggetto o sulle proprietà di un bucket in modo che si applichi automaticamente a tutti gli oggetti nel

bucket. Quando applichi un periodo di conservazione a una versione di un oggetto in modo esplicito, specifichi una Data di fine conservazione per tale versione. Amazon S3 archivia questa data nei metadati della versione dell'oggetto.

È anche possibile impostare un periodo di conservazione nelle proprietà di un bucket. Quando si imposta un periodo di conservazione su un bucket, si specifica una durata, in giorni o in anni, per la protezione di qualsiasi versione dell'oggetto inserita nel bucket. Quando si inserisce un oggetto nel bucket, Amazon S3 calcola una Data di fine conservazione per la versione dell'oggetto aggiungendo la durata specificata al timestamp di creazione della versione dell'oggetto. La versione dell'oggetto viene quindi protetta esattamente come se fosse stato impostato un singolo blocco con tale periodo di conservazione sulla versione dell'oggetto.

Note

Quando esegui il PUT di una versione dell'oggetto che dispone di una modalità e un periodo di conservazione individuali espliciti in un bucket, le impostazioni Object Lock individuali della versione dell'oggetto hanno la precedenza su qualsiasi impostazione di conservazione delle proprietà del bucket.

Come tutte le altre impostazioni del blocco degli oggetti, i periodi di conservazione si applicano alle singole versioni degli oggetti. Versioni diverse di un singolo oggetto possono avere modalità e periodi di conservazione diversi.

Ad esempio, supponi di avere un oggetto che è a 15 giorni di un periodo di conservazione di 30 giorni e applichi il comando PUT a un oggetto in Amazon S3 con lo stesso nome e un periodo di conservazione di 60 giorni. In questo caso la richiesta PUT va a buon fine e Amazon S3 crea una nuova versione dell'oggetto con un periodo di conservazione di 60 giorni. Per la versione precedente rimane impostato il periodo di conservazione originale e tale versione può quindi essere eliminata in 15 giorni.

Dopo aver applicato un'impostazione di conservazione a una versione dell'oggetto, è possibile estendere il periodo di conservazione. A tale scopo, invia una nuova richiesta Object Lock per la versione dell'oggetto con una Data di fine conservazione posteriore rispetto a quella attualmente configurata per la versione dell'oggetto. Amazon S3 sostituisce il periodo di conservazione esistente con il nuovo periodo più lungo. Qualsiasi utente con autorizzazioni per impostare un periodo di conservazione per un oggetto può estendere il periodo di conservazione per una

versione di un oggetto. Per impostare un periodo di conservazione, è necessaria l'autorizzazione `s3:PutObjectRetention`.

Quando si imposta un periodo di conservazione su un oggetto o bucket S3, è necessario selezionare una delle due modalità di conservazione: conformità o governance.

Modalità di conservazione

Object Lock S3 fornisce due modalità di conservazione che applicano livelli di protezione diversi agli oggetti:

- Modalità Conformità
- Modalità Governance

In modalità conformità, una versione protetta di un oggetto non può essere sovrascritta o eliminata da alcun utente, incluso l'utente root in Account AWS. Quando un oggetto è bloccato in modalità conformità, la relativa modalità di conservazione non può essere modificata e il periodo di conservazione non può essere abbreviato. La modalità conformità garantisce che una versione di un oggetto non possa essere sovrascritta o eliminata per tutta la durata del periodo di conservazione.

Note

L'unico modo per eliminare un oggetto in modalità di conformità prima della scadenza della data di conservazione è eliminare l'oggetto associato. Account AWS

Nella modalità Governance, gli utenti non possono sovrascrivere o eliminare una versione di un oggetto, né modificare le relative impostazioni di blocco, a meno che non dispongano di autorizzazioni speciali. La modalità governance permette di impedire alla maggior parte degli utenti di eliminare gli oggetti ma, allo stesso tempo, concede ad alcuni utenti l'autorizzazione per modificare le impostazioni di conservazione o per eliminare gli oggetti, se necessario. Puoi usare la modalità governance anche per testare le impostazioni del periodo di conservazione prima di creare un periodo di conservazione in modalità di conformità.

Per sovrascrivere o rimuovere le impostazioni di conservazione in modalità governance, occorre disporre dell'autorizzazione `s3:BypassGovernanceRetention` e includere in modo esplicito `x-amz-bypass-governance-retention:true` come un'intestazione della richiesta in qualsiasi richiesta che richieda la sostituzione della modalità governance.

 Note

Per impostazione predefinita, la console Amazon S3 include l'intestazione `x-amz-bypass-governance-retention:true`. Se si prova a eliminare oggetti protetti dalla modalità governance e che dispongono dell'autorizzazione `s3:BypassGovernanceRetention`, l'operazione andrà a buon fine.

Blocchi a fini giudiziari

Con Object Lock è possibile inserire anche un blocco a fini legali nella versione di un oggetto. Analogamente a un periodo di conservazione, un blocco a fini giudiziari impedisce che una versione di un oggetto venga sovrascritta o eliminata. Tuttavia, un blocco a fini legali non dispone di un periodo di tempo fisso associato e rimane valido fino a quando non viene rimosso. I blocchi a fini giudiziari possono essere applicati e rimossi liberamente da qualsiasi utente con l'autorizzazione `s3:PutObjectLegalHold`.

I blocchi a fini giudiziari sono indipendenti dai periodi di conservazione. L'applicazione di un blocco a fini giudiziari a una versione di un oggetto non influisce sulla modalità di conservazione o sul periodo di conservazione per tale versione dell'oggetto.

Ad esempio, supponi di inserire un blocco a fini legali nella versione di un oggetto mentre la versione dell'oggetto è protetta da un periodo di conservazione. Se il periodo di conservazione scade, l'oggetto non perde la protezione **WORM**. Il blocco a fini legali continua a proteggere l'oggetto fino a quando non viene rimosso in modo esplicito da un utente autorizzato. Analogamente, se rimuovi un blocco a fini giudiziari da una versione di un oggetto per la quale è impostato un periodo di conservazione, la versione dell'oggetto rimane protetta fino alla scadenza del periodo di conservazione.

Come funzionano le eliminazioni con S3 Object Lock

Se il bucket ha S3 Object Lock abilitato e l'oggetto è protetto da un periodo di conservazione o da un blocco legale e si tenta di eliminare un oggetto, Amazon S3 restituisce una delle seguenti risposte, a seconda di come si cerca di eliminare l'oggetto:

- Richiesta **DELETE** permanente: se viene inviata una richiesta **DELETE** permanente (una richiesta che specifica un ID di versione), Amazon S3 restituisce un errore di accesso negato (403 **Forbidden**) quando si tenta di eliminare l'oggetto. Per ulteriori informazioni sulla risoluzione dei problemi relativi agli errori di accesso negato con Object Lock, consulta [the section called "Impostazioni dell'opzione S3 Blocco oggetti"](#).

- Richiesta **DELETE** semplice: se viene inviata una richiesta DELETE semplice (una richiesta che non specifica un ID di versione), Amazon S3 restituisce una risposta 200 OK e inserisce un [indicatore di eliminazione](#) nel bucket, che diventa la versione corrente dell'oggetto con un nuovo ID. Per ulteriori informazioni sulla gestione dei contrassegni di eliminazione con Object Lock, consulta [the section called "Gestione dei contrassegni di eliminazione con Object Lock"](#).

Best practice per l'utilizzo di S3 Object Lock

Prendere in considerazione l'utilizzo della modalità governance se si desidera proteggere gli oggetti dall'eliminazione da parte della maggior parte degli utenti durante un periodo di conservazione predefinito, ma allo stesso tempo si desidera che alcuni utenti con autorizzazioni speciali abbiano la flessibilità necessaria per modificare le impostazioni di conservazione o eliminare gli oggetti.

Prendere in considerazione l'utilizzo della modalità conformità se non si desidera che nessun utente, incluso l'utente root dell' Account AWS, sia in grado di eliminare gli oggetti durante un periodo di conservazione predefinito. È possibile utilizzare questa modalità nel caso in cui sia necessario archiviare dati conformi.

È possibile usare la modalità Blocco a fini legali quando non si è sicuri di quanto tempo si desidera che gli oggetti rimangano immutabili. Ad esempio, se è in corso una verifica esterna dei dati e si desidera mantenere gli oggetti immutabili fino al completamento della verifica. In alternativa, si potrebbe avere un progetto in corso che utilizza un set di dati che si desidera mantenere immutabile fino al completamento del progetto.

Autorizzazioni richieste

Le operazioni del blocco degli oggetti richiedono autorizzazioni specifiche. A seconda dell'operazione esatta che si sta tentando di eseguire, potrebbe essere necessaria una delle seguenti autorizzazioni:

- s3:BypassGovernanceRetention
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectLegalHold
- s3:GetObjectRetention
- s3:PutBucketObjectLockConfiguration
- s3:PutObjectLegalHold
- s3:PutObjectRetention

Per un elenco completo delle autorizzazioni di Amazon S3 con le relative descrizioni, consulta [Operazioni, risorse e chiavi di condizione per Amazon S3](#) nella Guida di riferimento per l'autorizzazione del servizio.

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

Per informazioni sull'utilizzo delle condizioni con le autorizzazioni, consulta [Esempi di policy per i bucket che utilizzano le chiavi di condizione](#).

Considerazioni su Object Lock

Amazon S3 Object Lock può impedire che gli oggetti vengano eliminati o sovrascritti per un determinato periodo di tempo o in modo indefinito.

Puoi utilizzare la console Amazon S3, AWS Command Line Interface (AWS CLI) o l'API REST di Amazon S3 per visualizzare o impostare le informazioni di Object Lock. AWS SDKs Per informazioni generali sulle funzionalità S3 Object Lock, consulta [Blocco di oggetti con Object Lock](#).

Important

- Dopo aver abilitato Object Lock su un bucket, non è possibile disabilitare Object Lock o sospendere il controllo delle versioni per tale bucket.
- I bucket S3 con Object Lock non possono essere utilizzati come bucket di destinazione per i log di accesso al server. Per ulteriori informazioni, consulta [the section called "Registrazione dell'accesso al server"](#).

Argomenti

- [Autorizzazioni per la visualizzazione di informazioni di blocco](#)
- [Bypassare la modalità Governance](#)
- [Utilizzo di Object Lock con la replica S3](#)
- [Utilizzo di Object Lock con la crittografia](#)
- [Utilizzo di Object Lock con Inventario Amazon S3](#)
- [Gestione delle policy del ciclo di vita S3 con Object Lock](#)
- [Gestione dei contrassegni di eliminazione con Object Lock](#)

- [Utilizzo di S3 Storage Lens con Object Lock](#)
- [Caricamento di oggetti in un bucket con Object Lock abilitato](#)
- [Configurare eventi e notifiche](#)
- [Impostazione di limiti su periodi di conservazione con una policy di bucket](#)

Autorizzazioni per la visualizzazione di informazioni di blocco

È possibile visualizzare in modo programmatico lo stato Object Lock della versione di un oggetto Amazon S3 mediante le operazioni [HeadObject](#) o [GetObject](#). Entrambe le operazioni restituiscono la modalità di conservazione, la data di fine conservazione e lo stato del blocco a fini legali per la versione dell'oggetto specificata. Inoltre, è possibile visualizzare lo stato di Object Lock per più oggetti nel bucket S3 utilizzando l'Inventario S3.

Per visualizzare la modalità e il periodo di conservazione della versione di un oggetto, è necessaria l'autorizzazione `s3:GetObjectRetention`. Per visualizzare lo stato di blocco per vincoli di legge di un oggetto, è necessaria l'autorizzazione `s3:GetObjectLegalHold`. Per visualizzare la configurazione di conservazione predefinita di un bucket, occorre disporre dell'autorizzazione `s3:GetBucketObjectLockConfiguration`. Se si esegue una richiesta per una configurazione Object Lock su un bucket che non dispone di S3 Object Lock abilitato, Amazon S3 restituisce un errore.

Bypassare la modalità Governance

Se si dispone dell'autorizzazione `s3:BypassGovernanceRetention`, è possibile eseguire operazioni su versioni degli oggetti bloccate nella modalità governance come se non fossero protette. Queste operazioni includono l'eliminazione di una versione dell'oggetto, la riduzione del periodo di conservazione o la rimozione del periodo di conservazione di Object Lock tramite l'inserimento di una nuova richiesta `PutObjectRetention` con parametri vuoti.

Per bypassare la modalità Governance, è necessario indicare esplicitamente nella richiesta che si desidera bypassare la modalità Governance. A tale scopo, includi `x-amz-bypass-governance-retention:true` nell'intestazione nella richiesta di operazione `PutObjectRetention` API o utilizza il parametro equivalente con le richieste effettuate tramite o. AWS CLI AWS SDKs La console S3 applica automaticamente questa intestazione alle richieste effettuate tramite la console S3 se si dispone dell'autorizzazione `s3:BypassGovernanceRetention`.

 Note

Bypassare la modalità Governance non modifica lo stato dei vincoli di legge della versione di un oggetto. Se nella versione di un oggetto è abilitato un blocco a fini legali, questo rimane in vigore e impedisce richieste di sovrascrittura o eliminazione della versione dell'oggetto.

Utilizzo di Object Lock con la replica S3

È possibile utilizzare Object Lock con la replica S3 per abilitare la copia asincrona e automatica di oggetti bloccati e dei relativi metadati di conservazione tra i bucket S3. Ciò significa che per gli oggetti replicati, Amazon S3 utilizza la configurazione Object Lock del bucket di origine. In altre parole, se Object Lock è abilitato nel bucket di origine, sarà abilitato anche nel bucket di destinazione. Se un oggetto viene caricato direttamente nel bucket di destinazione (all'esterno della Replica S3), utilizza l'Object Lock impostato sul bucket di destinazione. Quando si utilizza la replica, gli oggetti in un bucket di origine vengono replicati in uno o più bucket di destinazione.

Per configurare la replica su un bucket con Object Lock abilitato, puoi utilizzare la console S3, l'API REST di Amazon AWS CLI S3 oppure. AWS SDKs

 Note

Per utilizzare Object Lock con la replica, devi concedere due autorizzazioni aggiuntive sul bucket S3 di origine nel ruolo AWS Identity and Access Management (IAM) che usi per configurare la replica. Le due nuove autorizzazioni aggiuntive sono `s3:GetObjectRetention` e `s3:GetObjectLegalHold`. Se il ruolo dispone di un'istruzione di autorizzazione `s3:Get*`, tale istruzione soddisfa il requisito. Per ulteriori informazioni, consulta [Configurazione delle autorizzazioni per la replica in tempo reale](#). Per informazioni generali sulla replica S3, consulta [Replica di oggetti all'interno e tra le Regioni](#).

Per esempi di configurazione della replica S3, consulta [Esempi di configurazione della replica in tempo reale](#).

Utilizzo di Object Lock con la crittografia

Amazon S3 esegue la crittografia di tutti i nuovi oggetti per impostazione predefinita. È possibile usare Object Lock con gli oggetti crittografati. Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia](#).

Sebbene Object Lock possa aiutare a impedire l'eliminazione o la sovrascrittura degli oggetti Amazon S3, non protegge dalla perdita dell'accesso alle chiavi di crittografia o dall'eliminazione delle chiavi di crittografia. Ad esempio, se si crittografano gli oggetti con la crittografia AWS KMS lato server e la AWS KMS chiave viene eliminata, gli oggetti potrebbero diventare illeggibili.

Utilizzo di Object Lock con Inventario Amazon S3

È possibile configurare Inventario Amazon S3 per creare elenchi degli oggetti in un bucket S3 in base a una pianificazione definita. È possibile configurare Inventario Amazon S3 per includere i seguenti metadati Object Lock per gli oggetti:

- La data di fine conservazione
- La modalità di conservazione
- Lo stato di blocco a fini legali

Per ulteriori informazioni, consulta [Catalogazione e analisi dei dati con Inventario S3](#).

Gestione delle policy del ciclo di vita S3 con Object Lock

Le configurazioni di gestione del ciclo di vita di un oggetto continuano a funzionare normalmente sugli oggetti protetti, compresa l'applicazione del contrassegno di eliminazione. Tuttavia, una versione bloccata di un oggetto non può essere eliminata da una policy di scadenza del ciclo di vita S3. Object Lock viene mantenuto indipendentemente dalla classe di storage in cui risiede l'oggetto e durante le transizioni del ciclo di vita S3 tra le classi di storage.

Per ulteriori informazioni sulla gestione della configurazione del ciclo di vita di un oggetto, consulta [Gestione del ciclo di vita degli oggetti](#).

Gestione dei contrassegni di eliminazione con Object Lock

Anche se non è possibile eliminare una versione protetta di un oggetto, puoi comunque creare un contrassegno di eliminazione per tale oggetto. L'inserimento di un contrassegno di eliminazione su un oggetto non elimina l'oggetto né alcuna sua versione. Tuttavia, fa sì che Amazon S3 si comporti

per molti versi come se l'oggetto fosse stato eliminato. Per ulteriori informazioni, consulta [Utilizzo dei contrassegni di eliminazione](#).

Note

I contrassegni di eliminazione non sono protetti contro i WORM, indipendentemente dal periodo di conservazione o dal blocco per vincoli di legge dell'oggetto a cui si riferiscono.

Utilizzo di S3 Storage Lens con Object Lock

Per visualizzare i parametri relativi ai byte di archiviazione abilitati per il blocco e il conteggio degli oggetti, puoi utilizzare Amazon S3 Storage Lens. S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti.

Per ulteriori informazioni, consulta [Utilizzo di S3 Storage Lens per proteggere i tuoi dati](#).

Per un elenco completo di parametri, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

Caricamento di oggetti in un bucket con Object Lock abilitato

L'intestazione Content-MD5 o x-amz-sdk-checksum-algorithm è necessaria per qualsiasi richiesta di caricamento di un oggetto con un periodo di conservazione configurato con Object Lock. Queste intestazioni servono a verificare l'integrità dell'oggetto durante il caricamento.

Quando si carica un oggetto con la console Amazon S3, S3 aggiunge automaticamente l'intestazione Content-MD5. Facoltativamente, è possibile specificare una funzione di checksum e un valore di checksum aggiuntivi tramite la console come intestazione x-amz-sdk-checksum-algorithm. Se utilizzi l'[PutObject](#) API, devi specificare l'Content-MD5 intestazione, l'intestazione o entrambi per configurare il x-amz-sdk-checksum-algorithm periodo di conservazione di Object Lock.

Per ulteriori informazioni, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

Configurare eventi e notifiche

Puoi utilizzare Amazon S3 Event Notifications per tenere traccia degli accessi e delle modifiche alle configurazioni e ai dati di Object Lock utilizzando AWS CloudTrail. Per informazioni su CloudTrail, consulta [What is? AWS CloudTrail](#) nella Guida AWS CloudTrail per l'utente.

Puoi anche utilizzare Amazon CloudWatch per generare avvisi basati su questi dati. Per informazioni su CloudWatch, consulta [What is Amazon CloudWatch?](#) nella Amazon CloudWatch User Guide.

Impostazione di limiti su periodi di conservazione con una policy di bucket

Puoi impostare periodi di conservazione minimo e massimo per un bucket mediante una policy di bucket. Il periodo massimo di conservazione è 100 anni.

L'esempio seguente mostra una policy di bucket che utilizza la chiave di condizione `s3:object-lock-remaining-retention-days` per impostare un periodo di conservazione massimo di 10 giorni.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "SetRetentionLimits",
  "Statement": [
    {
      "Sid": "SetRetentionPeriod",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:object-lock-remaining-retention-days": "10"
        }
      }
    }
  ]
}
```

Note

Se il bucket è quello di destinazione per una configurazione di replica, puoi impostare i periodi di conservazione minimo e massimo per le repliche di oggetti creati mediante la replica. A questo scopo, occorre consentire l'operazione `s3:ReplicateObject` nella policy di

bucket. Per ulteriori informazioni sulle autorizzazioni di replica, consulta [the section called “Impostazione delle autorizzazioni”](#).

Per ulteriori informazioni sulle policy di bucket, consulta gli argomenti indicati di seguito:

- [Operazioni, risorse e chiavi di condizione per Amazon S3](#) nella Guida di riferimento per l'autorizzazione del servizio

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

- [Operazioni con gli oggetti](#)
- [Esempi di policy per i bucket che utilizzano le chiavi di condizione](#)

Configurazione di S3 Object Lock

Amazon S3 Object Lock consente di archiviare oggetti in Amazon S3 mediante bucket per uso generico utilizzando un modello write-once-read-many (WORM). Puoi utilizzarlo per impedire che un oggetto venga eliminato o sovrascritto per un periodo di tempo fisso o indefinito. Per informazioni generali sulle funzionalità Object Lock, consulta [Blocco di oggetti con Object Lock](#).

Prima di bloccare eventuali oggetti, devi abilitare il controllo delle versioni S3 e Object Lock su un bucket per uso generico. In seguito, puoi impostare un periodo di conservazione, un blocco a fini legali o entrambi.

Per utilizzare Object Lock, devi disporre di determinate autorizzazioni. Per un elenco delle autorizzazioni correlate a varie operazioni Object Lock, consulta [the section called “Autorizzazioni richieste”](#).

Important

- Dopo aver abilitato Object Lock su un bucket, non è possibile disabilitare Object Lock o sospendere il controllo delle versioni per tale bucket.
- I bucket S3 con Object Lock non possono essere utilizzati come bucket di destinazione per i log di accesso al server. Per ulteriori informazioni, consulta [the section called “Registrazione dell'accesso al server”](#).

Argomenti

- [Abilitazione di Object Lock durante la creazione di un nuovo bucket S3 generico](#)
- [Abilitazione di Object Lock su un bucket S3 esistente](#)
- [Impostazione o modifica di un blocco a fini legali su un oggetto S3](#)
- [Impostazione o modifica di un periodo di conservazione su un oggetto S3](#)
- [Impostazione o modifica di un periodo di conservazione predefinito su un bucket S3](#)

Abilitazione di Object Lock durante la creazione di un nuovo bucket S3 generico

Puoi abilitare Object Lock quando crei un nuovo bucket S3 generico utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli SDK o l'API REST di Amazon S3. AWS

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Scegliere Create bucket (Crea bucket).

Viene visualizzata la pagina Create bucket (Crea bucket).

4. In Nome bucket, immettere il nome del bucket.

Note

Una volta creato un bucket, non è possibile modificarne il nome. Per ulteriori informazioni sulla denominazione dei bucket, consulta [Regole di denominazione dei bucket per uso generico](#).

5. Per la regione, scegli Regione AWS dove vuoi che risieda il bucket.
6. In Proprietà dell'oggetto, scegli di disabilitare o abilitare le liste di controllo degli accessi (ACL) e controllare la proprietà degli oggetti caricati nel bucket.
7. In Impostazioni di blocco dell'accesso pubblico per questo bucket scegli le impostazioni di blocco dell'accesso pubblico che vuoi applicare al bucket.
8. In Controllo delle versioni per il bucket, scegli Abilitato.

Object Lock funziona solo con bucket con versioni.

9. (Facoltativo) In Tags (Tag), puoi scegliere di aggiungere tag al bucket. I tag sono coppie chiave-valore utilizzate per classificare lo spazio di archiviazione e allocare i costi.
10. In Impostazioni avanzate, trova Object Lock e scegli Attiva.

Devi confermare che l'attivazione di Object Lock consentirà in modo permanente il blocco degli oggetti in questo bucket.

11. Seleziona Crea bucket.

Utilizzo di AWS CLI

L'esempio `create-bucket` seguente crea un nuovo bucket S3 denominato *amzn-s3-demo-bucket1* con Object Lock abilitato:

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket1 --object-lock-enabled-for-bucket
```

Per ulteriori informazioni ed esempi, consulta [create-bucket](#) nella documentazione di riferimento dei comandi della AWS CLI .

Note

Puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da Console di gestione AWS. Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) nella Guida AWS CloudShell per l'utente.

Utilizzo della REST API

Puoi utilizzare la REST API per creare un nuovo bucket S3 con Object Lock abilitato. Per ulteriori informazioni, consulta [CreateBucket](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

Per esempi su come abilitare Object Lock durante la creazione di un nuovo bucket S3 con gli AWS SDK, consulta Esempi di [codice](#) nell'Amazon S3 API Reference.

Per esempi su come ottenere la configurazione corrente di Object Lock con gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per uno scenario interattivo che illustra le diverse funzionalità di Object Lock utilizzando gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Abilitazione di Object Lock su un bucket S3 esistente

Puoi abilitare Object Lock per un bucket S3 esistente utilizzando la console Amazon S3, gli AWS SDK o l' AWS CLI API REST di Amazon S3.

Utilizzo della console S3

Note

Object Lock funziona solo con bucket con versioni.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket, scegli il nome del bucket per il quale desideri abilitare Object Lock.
4. Scegliere la scheda Properties (Proprietà).
5. In Proprietà, scorri verso il basso fino alla sezione Object Lock e scegli Modifica.
6. In Object Lock, scegli Attiva.

Devi confermare che l'attivazione di Object Lock consentirà in modo permanente il blocco degli oggetti in questo bucket.

7. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Il comando di esempio `put-object-lock-configuration` seguente imposta un periodo di conservazione di Object Lock di 50 giorni su un bucket denominato *amzn-s3-demo-bucket1*:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention": { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

Per ulteriori informazioni ed esempi, consulta [put-object-lock-configuration](#) nella documentazione di riferimento dei comandi della AWS CLI .

Note

Puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) nella Guida AWS CloudShell per l'utente.

Utilizzo della REST API

Puoi utilizzare la REST API Amazon S3 per abilitare Object Lock su un bucket S3 esistente. Per ulteriori informazioni, consulta [PutObjectLockConfiguration](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

Per esempi di come abilitare Object Lock per un bucket S3 esistente con gli AWS SDK, consulta Esempi di [codice](#) nell'Amazon S3 API Reference.

Per esempi su come ottenere la configurazione corrente di Object Lock con gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per uno scenario interattivo che illustra le diverse funzionalità di Object Lock utilizzando gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Impostazione o modifica di un blocco a fini legali su un oggetto S3

Puoi impostare o rimuovere un blocco legale su un oggetto S3 utilizzando la console Amazon S3, AWS CLI gli AWS SDK o l'API REST di Amazon S3.

Important

- Se desideri impostare un blocco a fini legali su un oggetto, Object Lock deve già essere abilitato nel bucket dell'oggetto.

- Quando esegui il PUT di una versione dell'oggetto che dispone di una modalità e un periodo di conservazione individuali espliciti in un bucket, le impostazioni Object Lock individuali della versione dell'oggetto hanno la precedenza su qualsiasi impostazione di conservazione delle proprietà del bucket.

Per ulteriori informazioni, consulta [the section called “Blocchi a fini giudiziari”](#).

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket, scegli il nome del bucket contenente gli oggetti su cui desideri impostare o modificare un blocco a fini legali.
4. Nell'elenco Oggetti, seleziona l'oggetto su cui desideri impostare o modificare un blocco a fini legali.
5. Nella pagina delle proprietà dell'oggetto, individua la sezione Blocco oggetti di carattere legale e scegli Modifica.
6. Scegli Abilita per impostare un blocco a fini legali o Disabilita per rimuoverlo.
7. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

L'esempio `put-object-legal-hold` seguente imposta un blocco a fini legali sull'oggetto *my-image.fs* nel bucket denominato *amzn-s3-demo-bucket1*:

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --  
legal-hold="Status=ON"
```

L'esempio `put-object-legal-hold` seguente rimuove un blocco a fini legali sull'oggetto *my-image.fs* nel bucket denominato *amzn-s3-demo-bucket1*:

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --  
legal-hold="Status=OFF"
```

Per ulteriori informazioni ed esempi, consulta [put-object-legal-hold](#) nella documentazione di riferimento dei comandi della AWS CLI .

Note

Puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) nella Guida AWS CloudShell per l'utente.

Utilizzo della REST API

Puoi utilizzare la REST API per impostare o modificare un blocco a fini legali su un oggetto. Per ulteriori informazioni, consulta [PutObjectLegalHold](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

Per esempi su come impostare un blocco legale su un oggetto con gli AWS SDK, consulta Esempi di [codice](#) nell'Amazon S3 API Reference.

Per esempi su come ottenere l'attuale stato di conservazione legale con gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per uno scenario interattivo che illustra le diverse funzionalità di Object Lock utilizzando gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Impostazione o modifica di un periodo di conservazione su un oggetto S3

Puoi impostare o modificare un periodo di conservazione su un oggetto S3 utilizzando la console Amazon S3, AWS CLI gli AWS SDK o l'API REST di Amazon S3.

Important

- Se desideri impostare un periodo di conservazione su un oggetto, Object Lock deve già essere abilitato nel bucket dell'oggetto.

- Quando esegui il PUT di una versione dell'oggetto che dispone di una modalità e un periodo di conservazione individuali espliciti in un bucket, le impostazioni Object Lock individuali della versione dell'oggetto hanno la precedenza su qualsiasi impostazione di conservazione delle proprietà del bucket.
- L'unico modo per eliminare un oggetto in modalità di conformità prima della scadenza della data di conservazione è eliminare l'oggetto associato. Account AWS

Per ulteriori informazioni, consulta [Periodi di conservazione](#).

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket, scegli il nome del bucket contenente l'oggetto su cui desideri impostare o modificare un periodo di conservazione.
4. Nell'elenco Oggetti, seleziona l'oggetto su cui desideri impostare o modificare un periodo di conservazione.
5. Nella pagina delle proprietà dell'oggetto, individua la sezione Conservazione del blocco oggetti e scegli Modifica.
6. In Conservazione, scegli Abilita per impostare un periodo di conservazione o Disabilita per rimuovere un periodo di conservazione.
7. Se hai scelto Abilita, in Modalità di conservazione, scegli Modalità di governance o Modalità di conformità. Per ulteriori informazioni, consulta [Modalità di conservazione](#).
8. In Data di fine conservazione, scegli la data in cui desideri che termini il periodo di conservazione. Durante questo periodo, il tuo oggetto viene WORM-protected e non può essere sovrascritto o eliminato. Per ulteriori informazioni, consulta [Periodi di conservazione](#).
9. Scegli Salva modifiche.

Utilizzo di AWS CLI

L'esempio `put-object-retention` seguente imposta un periodo di conservazione sull'oggetto *my-image.fs* nel bucket denominato *amzn-s3-demo-bucket1* fino al 1° gennaio 2025:

```
aws s3api put-object-retention --bucket amzn-s3-demo-bucket1 --key my-image.fs --  
retention='{ "Mode": "GOVERNANCE", "RetainUntilDate": "2025-01-01T00:00:00" }'
```

Per ulteriori informazioni ed esempi, consulta [put-object-retention](#) nella documentazione di riferimento dei comandi della AWS CLI .

Note

È possibile eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da Console di gestione AWS. Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) nella Guida AWS CloudShell per l'utente.

Utilizzo della REST API

Puoi utilizzare la REST API per impostare un periodo di conservazione su un oggetto. Per ulteriori informazioni, consulta [PutObjectRetention](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

Per esempi su come impostare un periodo di conservazione su un oggetto con gli AWS SDK, consulta Esempi di [codice](#) nell'Amazon S3 API Reference.

Per esempi su come ottenere il periodo di conservazione di un oggetto con gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per uno scenario interattivo che illustra le diverse funzionalità di Object Lock utilizzando gli AWS SDK, consulta Esempi di [codice](#) nell'API Reference di Amazon S3.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Impostazione o modifica di un periodo di conservazione predefinito su un bucket S3

Puoi impostare o modificare un periodo di conservazione predefinito su un bucket S3 utilizzando la console Amazon S3, AWS CLI, gli AWS SDK o l'API REST di Amazon S3. Specifica una durata, in giorni o in anni, per stabilire quanto a lungo proteggere ogni versione di un oggetto inserita nel bucket.

 Important

- Se desideri impostare un periodo di conservazione su un bucket, Object Lock deve già essere abilitato nel bucket.
- Quando esegui il PUT di una versione dell'oggetto che dispone di una modalità e un periodo di conservazione individuali espliciti in un bucket, le impostazioni Object Lock individuali della versione dell'oggetto hanno la precedenza su qualsiasi impostazione di conservazione delle proprietà del bucket.
- L'unico modo per eliminare un oggetto in modalità di conformità prima della scadenza della data di conservazione è eliminare l'oggetto associato. Account AWS

Per ulteriori informazioni, consulta [Periodi di conservazione](#).

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket, scegli il nome del bucket su cui desideri impostare o modificare un periodo di conservazione.
4. Scegliere la scheda Properties (Proprietà).
5. In Proprietà, scorri verso il basso fino alla sezione Object Lock e scegli Modifica.
6. In Conservazione predefinita, scegli Abilita per impostare un periodo di conservazione predefinito o Disabilita per rimuovere un periodo di conservazione predefinito.
7. Se hai scelto Abilita, in Modalità di conservazione, scegli Modalità di governance o Modalità di conformità. Per ulteriori informazioni, consulta [Modalità di conservazione](#).
8. In Periodo di conservazione predefinito, scegli il numero di giorni o anni di durata del periodo di conservazione. Gli oggetti inseriti in questo bucket verranno bloccati per questo numero di giorni o anni. Per ulteriori informazioni, consulta [Periodi di conservazione](#).
9. Scegli Salva modifiche.

Utilizzo di AWS CLI

Il comando di esempio `put-object-lock-configuration` seguente imposta un periodo di conservazione di Object Lock di 50 giorni su un bucket denominato `amzn-s3-demo-bucket1` utilizzando la modalità di conformità:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention": { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

L'esempio `put-object-lock-configuration` seguente rimuove la configurazione di conservazione predefinita su un bucket:

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-lock-configuration='{ "ObjectLockEnabled": "Enabled"}
```

Per ulteriori informazioni ed esempi, consulta [put-object-lock-configuration](#) nella documentazione di riferimento dei comandi della AWS CLI .

Note

Puoi eseguire AWS CLI comandi dalla console utilizzando AWS CloudShell. AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente da. Console di gestione AWS Per ulteriori informazioni, vedi Che cos'è? [CloudShell](#) nella Guida AWS CloudShell per l'utente.

Utilizzo della REST API

È possibile utilizzare la REST API per impostare un periodo di conservazione predefinito su un bucket S3 esistente. Per ulteriori informazioni, consulta [PutObjectLockConfiguration](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

Per esempi su come impostare un periodo di conservazione predefinito su un bucket S3 esistente con gli AWS SDK, consulta Esempi di [codice](#) nell'Amazon S3 API Reference.

Per uno scenario interattivo che illustra le diverse funzionalità di Object Lock utilizzando gli AWS SDK, consulta Esempi di [codice](#) nell'Amazon S3 API Reference.

Per informazioni generali sull'utilizzo di diversi AWS SDK, consulta [Sviluppo con Amazon S3 utilizzando gli AWS SDK](#) nell'API Reference di Amazon S3.

Backup dei dati di Amazon S3

Amazon S3 è integrato nativamente con AWS Backup un servizio completamente gestito e basato su policy che puoi utilizzare per definire centralmente le policy di backup per proteggere i tuoi dati in Amazon S3. Dopo aver definito le politiche di backup e assegnato le risorse di Amazon S3 alle policy, AWS Backup automatizza la creazione dei backup di Amazon S3 e li archivia in modo sicuro in un deposito di backup crittografato indicato nel piano di backup.

Quando utilizzi Amazon S3, AWS Backup puoi eseguire le seguenti azioni:

- Creare backup continui e backup periodici. I backup continui sono utili per il ripristino point-in-time e i backup periodici sono utili per soddisfare le esigenze di conservazione dei dati a lungo termine.
- Automatizzare la pianificazione e conservazione dei backup configurando centralmente le policy di backup.
- Ripristinare i backup dei dati Amazon S3 di un momento specifico.
- Accedi ai dati di backup direttamente tramite i punti di accesso S3 senza avviare un ripristino, consentendo il ripristino mirato dei file, la convalida dei dati e il controllo di conformità.

Inoltre AWS Backup, puoi utilizzare S3 Versioning e S3 Replication per eseguire il ripristino da eliminazioni accidentali ed eseguire le tue operazioni di ripristino automatico.

Accesso ai dati di backup

AWS Backup consente di leggere i dati di backup di Amazon S3 direttamente tramite i punti di accesso S3 senza avviare un ripristino completo. Crei un punto di accesso di backup per uno specifico punto di ripristino S3 e fornisci un AWS Backup punto di accesso S3 che puoi utilizzare con operazioni di lettura S3 standard come, e. GetObject HeadObject ListObjectsV2

Per ulteriori informazioni, consulta i punti di accesso [di backup](#) nella Developer Guide. AWS Backup

Prerequisiti

È necessario attivare [S3 Versioning](#) sul bucket prima di AWS Backup poterne eseguire il backup.

 Note

Ti consigliamo di [impostare una regola di scadenza del ciclo di vita per i bucket con il controllo delle versioni abilitato](#) che vengono sottoposti a backup. Se non imposti un periodo di scadenza del ciclo di vita, i costi di archiviazione di Amazon S3 potrebbero aumentare perché AWS Backup mantiene tutte le versioni dei dati di Amazon S3.

Nozioni di base

Per iniziare a usare Amazon S3, consulta [Creating Amazon S3 backups](#) nella Developer Guide.
AWS Backup AWS Backup

Restrizioni e limitazioni

Per informazioni sulle limitazioni, consulta [Creating Amazon S3 backups](#) (Creazione di backup di Amazon S3) nella Guida per gli sviluppatori di AWS Backup .

Ottimizzazione dei costi

Amazon S3 offre una gamma di funzionalità e classi di storage per aiutare l'utente a ottimizzare i costi durante l'intero ciclo di vita dei dati. Le classi di storage offrono la flessibilità necessaria per gestire i costi, fornendo diversi livelli di accesso ai dati a costi corrispondenti, senza costi iniziali o impegni sulla quantità di contenuti archiviati. Come per gli altri servizi AWS, si paga in base al consumo e solo per le risorse effettivamente utilizzate.

Le classi di storage di Amazon S3 sono progettate appositamente per fornire lo storage a costi più bassi per diversi modelli di accesso. Ciò include:

- S3 Standard per lo storage generico dei dati a cui si accede di frequente.
- Amazon S3 Express One Zone per dati ad alte prestazioni a cui si accede frequentemente in un'unica zona di disponibilità.
- Piano intelligente S3 per ottimizzare automaticamente i costi per i dati con modelli di accesso sconosciuti o variabili.
- AI S3 Standard (AI S3 Standard) e AI a zona unica S3 (AI a zona unica S3) per dati di lunga durata ma con accessi meno frequenti.
- Recupero istantaneo S3 Glacier per i dati di archivio che richiedono un accesso immediato.
- S3 Glacier Flexible Retrieval è ideale per i dati di archivio che non richiedono un accesso immediato, ma che necessitano di flessibilità per recuperare grandi quantità di dati senza costi aggiuntivi.
- S3 Glacier Deep Archive per l'archiviazione a lungo termine e la conservazione digitale ai costi di storage più bassi del cloud.

È possibile spostare gli oggetti nella classe di storage più conveniente in qualsiasi momento. Inoltre, Amazon S3 offre funzionalità per gestire il ciclo di vita dei dati. Ad esempio, è possibile utilizzare la configurazione del ciclo di vita S3 per automatizzare la transizione degli oggetti a classi di storage più convenienti o per eliminare automaticamente gli oggetti scaduti in base alle regole definite dall'utente.

Funzionalità come l'analisi della classe di storage S3, l'assegnazione di tag per l'allocazione dei costi e i report di fatturazione e utilizzo consentono di analizzare i modelli di costo e di utilizzo.

Argomenti

- [Creazione di report di utilizzo e fatturazione per Amazon S3](#)

- [Comprensione e gestione delle classi di storage Amazon S3](#)
- [Gestione del ciclo di vita degli oggetti](#)

Creazione di report di utilizzo e fatturazione per Amazon S3

Quando si utilizza Amazon S3, non è necessario pagare alcun costo iniziale o impegnarsi per la quantità di contenuti da archiviare. Come tutti gli altri Servizi AWS, paghi man mano che usi e paghi solo per ciò che usi.

AWS fornisce i seguenti report per Amazon S3:

- Report di fatturazione: report multipli che forniscono viste di alto livello di tutte le attività del sistema Servizi AWS che stai utilizzando, incluso Amazon S3. AWS fattura sempre al proprietario del bucket S3 le tariffe di Amazon S3, a meno che il bucket non sia stato creato come bucket Requester Pays. Per ulteriori informazioni sui tipi di Pagamento a carico del richiedente, consulta [Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati](#). Per ulteriori informazioni sui report di fatturazione, consulta [AWS Billing report per Amazon S3](#).
- Report di utilizzo: un riepilogo delle attività relative a uno specifico servizio, raggruppate per ora, giorno o mese. È possibile scegliere quale tipo di utilizzo e operazione includere. È inoltre possibile scegliere la modalità di aggregazione dei dati. Per ulteriori informazioni, consulta [AWS report di utilizzo per Amazon S3](#).

I seguenti argomenti forniscono informazioni sulla creazione di report di utilizzo e fatturazione per Amazon S3.

Argomenti

- [Utilizzo dei tag per l'allocazione dei costi per i bucket S3](#)
- [AWS Billing report per Amazon S3](#)
- [AWS report di utilizzo per Amazon S3](#)
- [Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3](#)
- [Fatturazione per le risposte di errore di Amazon S3](#)

Utilizzo dei tag per l'allocazione dei costi per i bucket S3

Per monitorare i costi di storage o altri criteri per singoli progetti o gruppi di progetti, etichettare i bucket Amazon S3 mediante i tag di allocazione dei costi. Un tag di allocazione dei costi è una coppia chiave/valore associata a un bucket S3. Dopo aver attivato i tag di allocazione dei costi, AWS li utilizza per organizzare i costi delle risorse nel report di allocazione dei costi. I tag per l'allocazione dei costi possono essere utilizzati solo per etichettare i bucket. Per informazioni sui tag utilizzati per etichettare gli oggetti, consulta [Etichettare i tuoi oggetti](#).

Il rapporto sull'allocazione dei costi elenca l'AWS utilizzo del tuo account per categoria di prodotto e utente dell'account collegato. Il report contiene le stesse voci di utilizzo indicate nel report di fatturazione dettagliato (vedere [Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3](#)) e altre colonne relative alle chiavi dei tag.

AWS fornisce due tipi di tag di allocazione dei costi, un tag AWS generato e tag definiti dall'utente. AWS definisce, crea e applica il `createdBy` tag AWS-generated per te dopo un evento Amazon CreateBucket S3. Tu puoi definire, creare e applicare tag definiti dall'utente al bucket S3.

È necessario attivare entrambi i tipi di tag separatamente nella console Gestione di costi e fatturazione prima di poterli visualizzare nei report di fatturazione. Per ulteriori informazioni sui tag AWS-generated, consulta [AWS-Generated Cost Allocation Tags](#).

Per ulteriori informazioni sull'attivazione dei tag, consulta [Utilizzo dei tag per l'allocazione dei costi](#) nella Guida per l'utente di AWS Billing .

Tag per l'allocazione dei costi definiti dall'utente

Un tag per l'allocazione dei costi definito dall'utente presenta i seguenti componenti:

- La chiave di tag: La chiave di tag corrisponde al nome del tag. Ad esempio, nel tag `project/Trinity`, `project` è la chiave. La chiave di tag è una stringa che fa distinzione tra maiuscole e minuscole, contenente da 1 a 128 caratteri Unicode.
- Il valore del tag. Il valore del tag è una stringa obbligatoria. Ad esempio, nel tag `project/Trinity`, `Trinity` è il valore. Il valore del tag è una stringa che fa distinzione tra maiuscole e minuscole, contenente da 0 a 256 caratteri Unicode.

Per informazioni sui caratteri consentiti per i tag definiti dall'utente e altre limitazioni, consulta [Limitazioni per i tag definiti dall'utente](#) nella Guida per l'utente di AWS Billing . Per ulteriori

informazioni sui tag definiti dall'utente, consulta [Tag per l'allocazione dei costi definiti dall'utente](#) nella Guida per l'utente di AWS Billing .

Tag bucket S3

Ogni bucket S3 dispone di un set di tag. Un set di tag contiene tutti i tag assegnati al bucket. Un set di tag può contenere fino a 50 tag o può essere vuoto. Nell'ambito di un set di tag, le chiavi devono essere univoche ma non occorre che i valori di un set di tag siano univoci. Ad esempio, è possibile avere lo stesso valore nei set di tag project/Trinity denominati Cost-center/Trinity.

Nell'ambito di un bucket, se si aggiunge un tag la cui chiave è la stessa di un tag esistente, il nuovo valore sovrascrive il vecchio valore.

AWS non applica alcun significato semantico ai tag. I tag sono interpretati prettamente come stringhe di caratteri.

Per aggiungere, elencare, modificare o eliminare tag, puoi utilizzare la console Amazon S3, AWS Command Line Interface (AWS CLI) o l'API Amazon S3.

Gestione dei tag per i bucket per uso generico

Puoi aggiungere o gestire tag per bucket generici utilizzando la console Amazon S3, AWS l'interfaccia a riga di comando (CLI) o utilizzando S3. AWS SDKs APIs Per ulteriori informazioni, consulta gli argomenti seguenti.

Utilizzo della console Amazon S3

Per creare tag nella console, consulta:

- [Visualizzazione delle proprietà di un bucket per uso generico S3](#).

Utilizzo dell'API

Per gestire i tag utilizzando l'API Amazon S3, consulta le seguenti pagine delle API nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

- [PutBucketTagging](#)
- [GetBucketTagging](#)
- [DeleteBucketTagging](#)

 Note

Dopo aver abilitato ABAC, le DeleteBucketTagging operazioni PutBucketTagging or non funzioneranno più. Utilizza invece il pulsante TagResource e UntagResource APIs per aggiungere o eliminare tag nei bucket. Ti consigliamo di utilizzare TagResource e UntagResource APIs per gestire i tag prima di abilitare ABAC nei tuoi bucket. Per saperne di più su ABAC, consulta. [Abilitazione dell'ABAC in bucket generici](#)

Utilizzo della CLI

Per gestire i tag utilizzando il AWS CLI, consultate le pagine seguenti nel AWS CLI Command Reference.

- [put-bucket-tagging](#)
- [get-bucket-tagging](#)
- [delete-bucket-tagging](#)

Ulteriori informazioni

- [Uso dei tag per l'allocazione dei costi](#) nella Guida per l'utente di AWS Billing .
- [Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3](#)
- [AWS Billing report per Amazon S3](#)

AWS Billing report per Amazon S3

La fattura mensile AWS separa le informazioni sull'utilizzo e i costi per funzione Servizio AWS . Sono disponibili diversi AWS Billing report: il rapporto mensile, il rapporto sull'allocazione dei costi e i report di fatturazione dettagliati. Per informazioni su come visualizzare i report di fatturazione, consulta [Visualizzazione di una fattura](#) nella Guida per l'utente di AWS Billing .

Per monitorare AWS l'utilizzo e fornire una stima degli addebiti associati al tuo account, puoi configurare. AWS Cost and Usage Reports Per ulteriori informazioni, consulta [Cosa sono AWS Cost and Usage Reports?](#) nella Guida all'esportazione AWS dei dati.

È inoltre possibile scaricare un report di utilizzo che fornisce informazioni più dettagliate sull'utilizzo dello storage Amazon S3 rispetto ai report di fatturazione. Per ulteriori informazioni, consulta [AWS report di utilizzo per Amazon S3](#).

Nella tabella seguente sono riportati i costi associati all'utilizzo di Amazon S3.

Costo	Commenti
Storage	<p>L'archiviazione degli oggetti nei bucket S3 è a pagamento. La tariffa applicata dipende dalle dimensioni degli oggetti, dal tempo di conservazione degli oggetti durante il mese e dalla classe di conservazione. Amazon S3 offre le seguenti classi di storage: S3 Standard, S3 Express One Zone, S3, S3 Standard-IA (IA per accessi non frequenti), S3 One Intelligent-Tiering, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval Zone-IA, S3 Glacier Deep Archive o Reduced Redundancy Storage (RRS). Per ulteriori informazioni sulle classi di storage, consulta Comprensione e gestione delle classi di storage Amazon S3.</p> <p>Tieni presente che, se hai abilitato il Controllo delle versioni S3, viene addebitato un costo per ogni versione di un oggetto che viene conservata. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta Come funzionano il Controllo delle versioni S3.</p>
Bucket per uso generale	<p>Non vengono addebitati i primi 2000 bucket generici creati nel proprio account. Tuttavia, è prevista una tariffa per ogni bucket creato oltre i primi 2000. Questa tariffa viene fatturata per bucket/month Per informazioni sui prezzi dei bucket per scopi generici, consulta Prezzi di Amazon S3.</p>

Costo	Commenti
Monitoraggio e automazione	Paghi una tariffa mensile di monitoraggio e automazione per oggetto archiviato nella classe di Intelligent-Tiering storage S3 per monitorare i modelli di accesso e spostare gli oggetti tra i livelli di accesso in S3. Intelligent-Tiering
Richieste	Si pagano le richieste, ad esempio quelle di GET, effettuate sui propri bucket e oggetti S3. Sono incluse le richieste del ciclo di vita. Le tariffe per le richieste dipendono dal tipo di richiesta. Per informazioni sui prezzi delle richieste, consulta Prezzi di Amazon S3 .
Recuperi	Paghi per il recupero di oggetti archiviati nello storage S3, S3 One Standard-IA, S3 Glacier Instant Retrieval Zone-IA, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.
Cancellazioni anticipate	Se elimini un oggetto archiviato nello storage S3, S3 One Standard-IA, S3 Glacier Instant Retrieval Zone-IA, S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive prima che sia passato l'impegno minimo di archiviazione, paghi una tariffa per l'eliminazione anticipata per quell'oggetto.
Gestione dello storage	L'utente paga per le funzioni di gestione dello storage (Inventario Amazon S3, analisi e tagging degli oggetti) abilitate sui bucket del proprio account.

Costo	Commenti
Larghezza di banda	<p>Ti sarà addebitato l'intero costo della larghezza di banda in entrata e in uscita da Amazon S3, eccetto nei seguenti casi:</p> <ul style="list-style-type: none">• Dati trasferiti in entrata da Internet• Dati trasferiti su un'istanza Amazon Elastic Compute Cloud (Amazon EC2), quando l'istanza si trova nello stesso bucket S3 Regione AWS• Dati trasferiti su Amazon CloudFront (CloudFront) <p>L'utente paga inoltre una tariffa per tutti i dati trasferiti utilizzando Amazon S3 Transfer Acceleration.</p>

Per informazioni dettagliate sui costi di utilizzo di Amazon S3 per l'archiviazione, il trasferimento dei dati e i servizi, consulta [Prezzi di Amazon S3](#) e [Domande frequenti su Amazon S3](#).

Per informazioni sulla comprensione dei codici e delle abbreviazioni utilizzati nei report di fatturazione e di utilizzo di Amazon S3, consulta [Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3](#).

Ulteriori informazioni

- [AWS report di utilizzo per Amazon S3](#)
- [Utilizzo dei tag per l'allocazione dei costi per i bucket S3](#)
- [AWS Billing e gestione dei costi](#)
- [Prezzi di Amazon S3](#)

AWS report di utilizzo per Amazon S3

Quando si scarica un report di utilizzo, è possibile scegliere di aggregare i dati sull'utilizzo in base a ora, giorno o mese. Il report sull'utilizzo di Amazon S3 elenca le operazioni per tipo di utilizzo e. Regione AWS Per informazioni più dettagliate sull'utilizzo dell'archiviazione Amazon S3, scarica i report di utilizzo AWS generati in modo dinamico. È possibile scegliere quale tipo di utilizzo, operazione e periodo di tempo includere. Puoi inoltre scegliere la modalità di aggregazione dei dati. Per ulteriori informazioni sui report di utilizzo, vedere [Report di utilizzo AWS](#) nella Guida dell'utente all'esportazione dei dati AWS .

Il report di utilizzo di Amazon S3 include le seguenti informazioni:

- Servizio - Amazon S3
- Operation (Operazione) – Operazione eseguita sul bucket o sull'oggetto. Per una spiegazione dettagliata delle operazioni di Amazon S3, consulta [Operazioni di monitoraggio nei report di utilizzo](#).
- UsageType— Uno dei seguenti valori:
 - Un codice che identifica il tipo di storage
 - Un codice che identifica il tipo di richiesta
 - Un codice che identifica il tipo di recupero
 - Un codice che identifica il tipo di trasferimento dei dati
 - Un codice che identifica le eliminazioni anticipate dallo storage S3, S3 Intelligent-Tiering, S3 One Zone-Infrequent Access (S3 One Zone-IA) Standard-IA, S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive
 - StorageObjectCount – Numero di oggetti archiviati in un determinato bucket

Per una spiegazione dettagliata dei tipi di utilizzo di Amazon S3, consulta [Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3](#).

- Risorsa – Nome della tabella o del bucket associato all'utilizzo indicato.
- StartTime— Ora di inizio del giorno a cui si applica l'utilizzo, in UTC (Coordinated Universal Time).
- EndTime— Ora di fine del giorno a cui si riferisce l'utilizzo, in UTC (Coordinated Universal Time).
- UsageValue— Uno dei seguenti valori di volume. L'unità di misura tipica per i dati è gigabyte (GB). Tuttavia, a seconda del servizio e del report, potrebbero invece essere visualizzati terabyte (TB).
 - Il numero di richieste durante il periodo di tempo specificato
 - La quantità di dati trasferiti

- La quantità di dati memorizzati in una data ora
- La quantità di dati associata ai ripristini dallo storage S3, S3 One Standard-IA Zone-IA, S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive

Tip

Per informazioni dettagliate su ogni richiesta ricevuta da Amazon S3 per gli oggetti, attivare la registrazione degli accessi al server per i bucket. Per ulteriori informazioni, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

È possibile scaricare un report di utilizzo in formato XML o CSV (Comma-Separated Value). Di seguito è riportato un esempio di report di utilizzo in formato CSV aperto in un foglio elettronico.

Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue
AmazonS3	HeadBucket	USW2-C3DataTransfer-Out-Bytes	admin-created3	6/1/2017 0:00	7/1/2017 0:00	15309
AmazonS3	PutObject	USW2-C3DataTransfer-In-Bytes	admin-created3	6/1/2017 0:00	7/1/2017 0:00	19062
AmazonS3	HeadBucket	USW2-Requests-Tier2	admin-created3	6/1/2017 0:00	7/1/2017 0:00	68
AmazonS3	PutObjectForRepl	USW1-Requests-SIA-Tier1	ca-example-bucket	6/1/2017 0:00	7/1/2017 0:00	178294
AmazonS3	PutObjectForRepl	USW1-USW2-AWS-In-Bytes	ca-example-bucket	6/1/2017 0:00	7/1/2017 0:00	387929083
AmazonS3	GetObjectForRepl	USW2-Requests-NoCharge	admin-created3	6/1/2017 0:00	7/1/2017 0:00	108
AmazonS3	GetObjectForRepl	USW2-USW1-AWS-Out-Bytes	my-test-bucket-bash	6/1/2017 0:00	7/1/2017 0:00	387910021

Per ulteriori informazioni, consulta [Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3](#).

Scaricando il AWS Report di utilizzo

È possibile scaricare un report di utilizzo come file XML o CSV.

Per scaricare il report di utilizzo

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra del titolo, scegli il nome utente o l'ID account, quindi scegli Fatturazione e gestione dei costi.
3. Nel riquadro di navigazione, seleziona Pagine legacy e scegli Report sui costi e sull'utilizzo.
4. In Rapporto AWS di utilizzo, scegli Crea un rapporto sull'utilizzo.
5. Nella pagina Scarica report di utilizzo, scegli le seguenti impostazioni:

- Servizi - Scegli Amazon Simple Storage Service.
 - Usage Types (Tipi di utilizzo) – Per una spiegazione dettagliata dei tipi di utilizzo di Amazon S3, consulta [Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3](#).
 - Operation (Operazione) – Per una spiegazione dettagliata delle operazioni di Amazon S3, consulta [Operazioni di monitoraggio nei report di utilizzo](#).
 - Time Period (Periodo di tempo) – Periodo di tempo per cui il report deve fornire informazioni.
 - Report Granularity (Granularità del report) – Consente di specificare se si desidera che il report includa subtotali in base all'ora, al giorno o al mese.
6. Scegli Scarica, scegli il formato di download (Report XML o Report CSV) e segui le istruzioni per aprire o salvare il report.

Ulteriori informazioni

- [Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3](#)
- [AWS Billing report per Amazon S3](#)

Comprendere il tuo AWS report di fatturazione e utilizzo per Amazon S3

Quando utilizzi Amazon S3, includiamo i codici correlati nei report di AWS fatturazione e utilizzo. Esaminare questi codici ti aiuta a comprendere i costi e i modelli di utilizzo di Amazon S3. Il monitoraggio e la gestione delle spese sono essenziali per ottimizzare i costi. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

I report di utilizzo e fatturazione di Amazon S3 usano codici e abbreviazioni. Per i tipi di utilizzo riportati nella tabella seguente, sostituisci *region*, *region1* e *region2* con le abbreviazioni dei [codici di fatturazione di Regione AWS](#) nella Guida per l'utente alle zone di disponibilità e Regioni AWS.

Note

Per la regione Stati Uniti orientali (Virginia settentrionale), il prefisso della regione viene omesso dai codici dei tipi di utilizzo. Ad esempio, verrà visualizzato TimedStorage-ByteHrs al posto di USE1-TimedStorage-ByteHrs

Per i tipi di utilizzo Multi-Region degli Access Points S3 riportati nella tabella seguente, sostituisci *regiongroup1* e *regiongroup2* con le abbreviazioni presenti in questo elenco:

- AP: Asia Pacifico
- AU: Australia
- EU: Europa
- IN: India
- NA: Nord America
- SA: Sud America

I gruppi di Regioni sono raggruppamenti geografici di più Regioni AWS. Per ulteriori informazioni, consulta [Regioni e zone di disponibilità](#). Per informazioni sui prezzi per Regione AWS, consulta [Prezzi di Amazon S3](#).

La prima colonna della tabella che segue elenca i tipi di utilizzo presenti nei report di utilizzo e fatturazione. L'unità di misura tipica per i dati è gigabyte (GB). Tuttavia, a seconda del servizio e del report, potrebbero invece essere visualizzati terabyte (TB).

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region1-region2</i> -AWS-In-A Bytes	GB	Orario	La quantità di dati accelerati trasferiti a <i>region1</i> da <i>region2</i>
<i>region1-region2</i> -AWS-In-A Bytes-T1	GB	Orario	La quantità di dati accelerati T1 trasferiti <i>region1</i> da <i>region2</i> , dove T1 si riferisce CloudFront alle richieste ai punti di presenza (POPs) negli Stati Uniti d'America, in Europa e in Giappone
<i>region1-region2</i> -AWS-In-A Bytes-T2	GB	Orario	La quantità di dati accelerati T2 trasferiti <i>region1</i> da <i>region2</i> ,

Tipo di utilizzo	unità	Granularità	Descrizione
			dove T2 si riferisce alle CloudFront richieste in tutte le altre location periferiche POPs AWS
<i>region1-region2</i> -AWS-In-Bytes	GB	Orario	La quantità di dati trasferiti a <i>region1</i> da <i>region2</i>
<i>region1-region2</i> -AWS-Out-Bytes	GB	Orario	La quantità di dati accelerati trasferiti da <i>region1</i> a <i>region2</i>
<i>region1-region2</i> -AWS-Out-Bytes-T1	GB	Orario	La quantità di dati accelerati T1 trasferiti da <i>region1</i> a <i>region2</i> , dove T1 si riferisce CloudFront alle richieste ai POP negli Stati Uniti d'America, in Europa e in Giappone
<i>region1-region2</i> -AWS-Out-Bytes-T2	GB	Orario	La quantità di dati accelerati T2 trasferiti da <i>region1</i> a <i>region2</i> , dove T2 si riferisce alle CloudFront richieste ai POP in tutte le altre sedi periferiche AWS
<i>region1-region2</i> -AWS-Out-Bytes	GB	Orario	La quantità di dati trasferiti da <i>region1</i> a <i>region2</i>
<i>region</i> -BatchOperations-Jobs	Conteggio	Orario	Il numero di processi di S3 Batch Operations eseguiti

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -BatchOperations-Objects	Conteggio	Orario	Il numero di operazioni sugli oggetti eseguite da S3 Batch Operations
<i>region</i> -Bulk-Retrieval-Bytes	GB	Orario	La quantità di dati recuperati con richieste S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive di tipo Bulk
<i>region</i> -BytesDeleted-GDA	GB	Mensile	La quantità di dati eliminati da un'operazione DeleteObject dallo storage S3 Glacier Deep Archive
<i>region</i> -BytesDeleted-GIR	GB	Mensile	La quantità di dati eliminati da un'operazione DeleteObject dallo storage Recupero istantaneo S3 Glacier.
<i>region</i> -BytesDeleted-GLACIER	GB	Mensile	La quantità di dati eliminati da un'operazione DeleteObject dallo storage Recupero flessibile S3 Glacier
<i>region</i> -BytesDeleted-INT	GB	Mensile	La quantità di dati eliminati da un>DeleteObject operazione dallo storage S3 Intelligent-Tiering

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -BytesDeleted-RRS	GB	Mensile	La quantità di dati eliminati da un'operazione DeleteObject dallo storage Reduced Redundancy Storage (RRS)
<i>region</i> -BytesDeleted-SIA	GB	Mensile	La quantità di dati eliminati da un>DeleteObject operazione dallo storage S3 Standard-IA
<i>region</i> -BytesDeleted-STANDARD	GB	Mensile	La quantità di dati eliminati da un'operazione DeleteObject dallo storage S3 Standard
<i>region</i> -BytesDeleted-ZIA	GB	Mensile	La quantità di dati eliminati da un>DeleteObject operazione dallo storage di S3 One Zone-IA
<i>region</i> -C3DataTransfer-In-Bytes	GB	Orario	La quantità di dati trasferiti in Amazon S3 da Amazon EC2 all'interno dello stesso Regione AWS
<i>region</i> -C3DataTransfer-Out-Bytes	GB	Orario	La quantità di dati trasferiti da Amazon S3 ad Amazon EC2 nell'ambito della stessa Regione AWS

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -CloudFront-In-Bytes	GB	Orario	La quantità di dati trasferiti in Regione AWS da e verso una distribuzione CloudFront
<i>region</i> -CloudFront-Out-Bytes	GB	Orario	La quantità di dati trasferiti da una Regione AWS a una CloudFront distribuzione
<i>region</i> -DataTransfer-In-Bytes	GB	Orario	Quantità di dati trasferiti in Amazon S3 da Internet
<i>region</i> -DataTransfer-Out-Bytes	GB	Orario	Quantità di dati trasferiti da Amazon S3 a Internet ¹
<i>region</i> -DataTransfer-Regional-Bytes	GB	Orario	La quantità di dati trasferiti da Amazon S3 alle AWS risorse all'interno dello stesso Regione AWS
<i>region</i> -EarlyDelete-ByteHrs	GB-Hours	Orario	Utilizzo dell'archiviazione ripartita proporzionalmente per gli oggetti eliminati dall'archivio S3 Glacier Flexible Retrieval prima del termine minimo di 90 giorni ²
<i>region</i> -EarlyDelete-GDA	GB-Hours	Orario	Utilizzo dello storage ripartito proporzionalmente per gli oggetti eliminati dallo storage S3 Glacier Deep Archive prima del termine minimo di 180 giorni ²

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -EarlyDelete-GIR	GB-Hours	Orario	Utilizzo dell'archiviazione ripartita proporzionalmente per gli oggetti eliminati o trasferiti dalla classe S3 Glacier Instant Retrieval prima del termine minimo di 90 giorni.
<i>region</i> -EarlyDelete-GIR-SmObjects	GB-Hours	Orario	Utilizzo dell'archiviazione ripartita proporzionalmente per gli oggetti di piccole dimensioni (inferiori a 128 KB) eliminati da S3 Glacier Instant Retrieval prima del termine minimo di 90 giorni.
<i>region</i> -EarlyDelete-SIA	GB-Hours	Orario	Utilizzo proporzionale dello storage per gli oggetti eliminati da S3 Standard-IA prima della scadenza dell'impegno minimo di 30 giorni 3
<i>region</i> -EarlyDelete-SIA-SmObjects	GB-Hours	Orario	Utilizzo proporzionale dello storage per oggetti di piccole dimensioni (inferiori a 128 KB) eliminati da S3 prima della scadenza dell'impegno minimo di 30 giorni 3 Standard-IA

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -EarlyDelete-ZIA	GB-Hours	Orario	Utilizzo proporzionale dello storage per oggetti eliminati da S3 One Zone-IA prima della scadenza dell'impegno minimo di 30 giorni 3
<i>region</i> -EarlyDelete-ZIA-S mObjects	GB-Hours	Orario	Utilizzo proporzionale dello storage per oggetti di piccole dimensioni (inferiori a 128 KB) eliminati da S3 One Zone-IA prima della scadenza dell'impegno minimo di 30 giorni 3
<i>region</i> -Expedited-Retrieval-Bytes	GB	Orario	La quantità di dati recuperati con le richieste S3 Glacier Flexible Retrieval di tipo Expedited
Global-Bucket-Hrs-FreeTier	Bucket	Mensile	Il numero di bucket di uso generale nell'account entro il livello gratuito di 2000 bucket
Global-Bucket-Hrs	Bucket	Mensile	Il numero di bucket per scopi generici presenti nell'account oltre il livello gratuito di 2000 bucket
<i>region</i> -Inventory-Objects Listed	Oggetti	Orario	Numero di oggetti elencati per un gruppo di oggetti (gli oggetti sono raggruppati in base al bucket o al prefisso) con un elenco di inventario

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Metadata-Updates	Aggiornamenti	Orario	Tariffa per aggiornamento per gli aggiornamenti elaborati da S3 Metadata
<i>region</i> -Metadata-Annotation-Processed-Bytes	GB	Orario	Dati elaborati dalla tabella di annotazione S3 Metadata
<i>region</i> -Monitoring-Automation-INT	Oggetti	Orario	Il numero di oggetti unici monitorati e suddivisi automaticamente su più livelli nella classe di storage S3 Intelligent-Tiering
<i>region</i> -MRAP-Out-Bytes	GB	Orario	La quantità di dati trasferiti tramite un endpoint S3 Multi-Region Access Points dai bucket di una regione (prezzo di routing dei dati MRAP).
<i>region</i> -MRAP-In-Bytes	GB	Orario	La quantità di dati trasferiti tramite un endpoint S3 Multi-Region Access Points dai bucket di una regione (prezzo di routing dei dati MRAP).

Tipo di utilizzo		unità	Granularità	Descrizione
<i>regiongroup1-regiongroup2-</i> MRAP-Out-Bytes	-	GB	Orario	La quantità di dati trasferiti tramite un endpoint S3 Multi-Region Access Points da un bucket in a un client si trova <i>regiongroup1</i> all'esterno della rete. <i>regiongroup2</i> AWS
<i>regiongroup1-regiongroup2-</i> MRAP-In-Bytes	-	GB	Orario	La quantità di dati trasferiti tramite un endpoint S3 Multi-Region Access Points a un bucket in <i>regiongroup1</i> da un client situato all'esterno della rete. <i>regiongroup2</i> AWS
<i>region</i> -OverwriteBytes-Copy-GDA		GB	Mensile	La quantità di dati sovrascritti da un'operazione CopyObject dallo storage S3 Glacier Deep Archive
<i>region</i> -OverwriteBytes-Copy-GIR		GB	Mensile	La quantità di dati sovrascritti da un'operazione CopyObject dallo storage Recupero istantaneo S3 Glacier.
<i>region</i> -OverwriteBytes-Copy-GLACIER		GB	Mensile	La quantità di dati sovrascritti da un'operazione CopyObject dallo storage Recupero flessibile S3 Glacier

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -OverwriteBytes-Copy-INT	GB	Mensile	La quantità di dati sovrascritti da un'CopyObject operazione dallo storage S3 Intelligent-Tiering
<i>region</i> -OverwriteBytes-Copy-RRS	GB	Mensile	La quantità di dati sovrascritti da un'operazione CopyObject dallo storage Reduced Redundancy Storage (RRS)
<i>region</i> -OverwriteBytes-Copy-SIA	GB	Mensile	La quantità di dati sovrascritti da un'CopyObject operazione dallo storage S3 Standard-IA
<i>region</i> -OverwriteBytes-Copy-STANDARD	GB	Mensile	La quantità di dati sovrascritti da un'operazione CopyObject dallo storage S3 Standard
<i>region</i> -OverwriteBytes-Copy-ZIA	GB	Mensile	La quantità di dati sovrascritti da un'CopyObject operazione dallo storage S3 One Zone-IA
<i>region</i> -OverwriteBytes-Put-GDA	GB	Mensile	La quantità di dati sovrascritti da un'operazione PutObject dallo storage S3 Glacier Deep Archive

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -OverwriteBytes-Put-GIR	GB	Mensile	La quantità di dati sovrascritti da un'operazione PutObject dallo storage Recupero istantaneo S3 Glacier.
<i>region</i> -OverwriteBytes-Put-GLACIER	GB	Mensile	La quantità di dati sovrascritti da un'operazione PutObject dallo storage Recupero flessibile S3 Glacier
<i>region</i> -OverwriteBytes-Put-INT	GB	Mensile	La quantità di dati sovrascritti da un'PutObject operazione dallo storage S3 Intelligent-Tiering
<i>region</i> -OverwriteBytes-Put-RRS	GB	Mensile	La quantità di dati sovrascritti da un'operazione PutObject dallo storage Reduced Redundancy Storage (RRS)
<i>region</i> -OverwriteBytes-Put-SIA	GB	Mensile	La quantità di dati sovrascritti da un'PutObject operazione dallo storage S3 Standard-IA
<i>region</i> -OverwriteBytes-Put-STANDARD	GB	Mensile	La quantità di dati sovrascritti da un'operazione PutObject dallo storage S3 Standard

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -OverwriteBytes-Put-ZIA	GB	Mensile	La quantità di dati sovrascritti da un'PutObject operazione dallo storage S3 One Zone-IA
<i>region1-region2</i> -S3RTC-In-Bytes	GB	Mensile	La quantità di dati trasferiti per il controllo del tempo di replica di S3 (S3 RTC) da <i>region2</i> a <i>region1</i> mediante le operazioni PutObjectReplTime , GetObjectReplTime , InitiateMultipartUploadReplTime , UploadPartReplTime , CompleteMultipartUploadReplTime e WriteACLReplTime
<i>region1-region2</i> -S3RTC-Out-Bytes	GB	Mensile	La quantità di dati trasferiti per il controllo del tempo di replica di S3 (S3 RTC) da <i>region1</i> a <i>region2</i> mediante le operazioni PutObjectReplTime , GetObjectReplTime , InitiateMultipartUploadReplTime , UploadPartReplTime , CompleteMultipartUploadReplTime e WriteACLReplTime

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Annotation-TimedStorage-ByteHrs	GB-Month	Giornaliero	Archiviazione per le annotazioni, fatturata alla tariffa standard di Amazon S3
<i>region</i> -Requests-Annotation-Tier1	Conteggio	Orario	Il numero diPUT, COPYPOST, e LIST richieste di annotazioni (,). PutObject Annotation ListObjectAnnotations Fatturato per 1.000 richieste.
<i>region</i> -Requests-Annotation-Tier2	Conteggio	Orario	Il numero di GET richieste di annotazioni ()GetObject Annotation . Fatturato per 1.000 richieste.
<i>region</i> -Requests-GDA-Tier1	Conteggio	Orario	Il numero di richieste PUT, COPY, POST, CreateMultipartUpload , UploadPart , o CompleteMultipartUpload su oggetti S3 Glacier Deep Archive ⁶
<i>region</i> -Requests-GDA-Tier2	Conteggio	Orario	Il numero di richieste GET e HEAD sugli oggetti di S3 Glacier Deep Archive

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Requests-GDA-Tier3	Conteggio	Orario	Numero di richieste di ripristino S3 Glacier Deep Archive di tipo standard
<i>region</i> -Requests-GDA-Tier5	Conteggio	Orario	Numero di richieste di ripristino S3 Glacier Deep Archive di tipo Bulk
<i>region</i> -Requests-GIR-Tier1	Conteggio	Orario	Il numero di richieste PUT, COPY o POST su oggetti Recupero istantaneo S3 Glacier.
<i>region</i> -Requests-GIR-Tier2	Conteggio	Orario	Il numero GET e tutte le altre Retrieval-Tier1 richieste non S3 Glacier Instant sugli oggetti S3 Glacier Instant Retrieval.
<i>region</i> -Requests-GLACIER-Tier1	Conteggio	Orario	Il numero di richieste PUT, COPY, POST, CreateMultipartUpload, UploadPart, o CompleteMultipartUpload su oggetti Recupero flessibile S3 Glacier ⁶
<i>region</i> -Requests-GLACIER-Tier2	Conteggio	Orario	Il numero di GET e di tutte le altre richieste non elencate sugli oggetti Recupero flessibile S3 Glacier

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Requests-INT-Tier1	Conteggio	Orario	Il numero di o richieste sugli oggetti S3 PUT COPY POST Intelligent-Tiering
<i>region</i> -Requests-INT-Tier2	Conteggio	Orario	Il numero GET e tutte le altre richieste non di livello 1 per oggetti S3 Intelligent-Tiering
<i>region</i> -Requests-SIA-Tier1	Conteggio	Orario	Il numero di o POST richieste PUT sugli COPY oggetti S3 Standard-IA
<i>region</i> -Requests-SIA-Tier2	Conteggio	Orario	Il numero GET e tutte le altre richieste non S3 Glacier Instant sugli oggetti S3 Retrieval-Tier1 Standard-IA
<i>region</i> -Requests-Tier1	Conteggio	Orario	Il numero di richieste PUT, COPY, o POST per S3 Standard, RRS e tag, più le richieste LIST per tutti i bucket e gli oggetti
<i>region</i> -Requests-Tier2	Conteggio	Orario	Il numero di GET e di tutte le altre richieste non-Tier1
<i>region</i> -Requests-Tier3	Conteggio	Orario	Numero totale di richieste del ciclo di vita verso S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive e richieste di ripristino standard di S3 Glacier Flexible Retrieval

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Requests-Tier4	Conteggio	Orario	Il numero di transizioni del ciclo di vita verso lo storage S3 Glacier Instant Retrieval, S3, S3 o S3 One Intelligent-Tiering Standard-IA Zone-IA
<i>region</i> -Requests-Tier5	Conteggio	Orario	Numero di richieste di ripristino S3 Glacier Flexible Retrieval di tipo Bulk
<i>region</i> -Requests-Tier6	Conteggio	Orario	Numero di richieste di ripristino S3 Glacier Flexible Retrieval di tipo Expedited
<i>region</i> -Requests-Tier8	Conteggio	Orario	Il numero di richieste S3 Access Grants
<i>region</i> -Requests-XZ-Tier1	Conteggio	Orario	Il numero di richieste PUT o COPY su oggetti S3 Express One Zone
<i>region</i> -Requests-XZ-Tier2	Conteggio	Orario	Il numero e tutte le altre richieste non S3 Express One sugli oggetti GET S3 Express One Zone Zone-Tier1
<i>region</i> -Requests-ZIA-Tier1	Conteggio	Orario	Il numero di PUT o POST richieste sugli oggetti S3 One COPY Zone-IA

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Requests-ZIA-Tier2	Conteggio	Orario	Il numero GET e tutte le altre Zone-IA-Tier1 richieste non S3 One sugli oggetti S3 One Zone-IA
<i>region</i> -Retrieval-GIR	GB	Orario	La quantità di dati recuperati dall'archivio S3 Glacier Instant Retrieval.
<i>region</i> -Retrieval-SIA	GB	Orario	La quantità di dati recuperati dallo storage S3 Standard-IA
<i>region</i> -Retrieval-XZ	GB	Orario	La porzione di dati che supera i 512 KB in una determinata richiesta di recupero (PUT o COPY) con lo storage S3 Express One Zone
<i>region</i> -Retrieval-ZIA	GB	Orario	La quantità di dati recuperati dallo storage S3 One Zone-IA
<i>region</i> -S3DSSE-In-Bytes	GB	Mensile	La quantità di dati a doppia crittografia da parte di Amazon S3
<i>region</i> -S3DSSE-Out-Bytes	GB	Mensile	La quantità di dati a doppia crittografia decriptati da Amazon S3

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -S3G-DataTransfer-In-Bytes	GB	Orario	La quantità di dati trasferiti ad Amazon S3 per il ripristino degli oggetti dall'archivio S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive
<i>region</i> -S3G-DataTransfer-Out-Bytes	GB	Orario	La quantità di dati trasferiti da Amazon S3 per la transizione degli oggetti all'archivio S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive
<i>region</i> -Select-Returned-Bytes	GB	Orario	La quantità di dati restituiti con richieste Seleziona dallo storage S3 Standard
<i>region</i> -Select-Returned-GIR-Bytes	GB	Orario	La quantità di dati restituiti dall'archivio S3 Glacier Instant Retrieval con richieste Select.
<i>region</i> -Select-Returned-INT-Bytes	GB	Orario	La quantità di dati restituiti con le richieste Select dallo storage S3 Intelligent-Tiering
<i>region</i> -Select-Returned-SIA-Bytes	GB	Orario	La quantità di dati restituiti con le richieste Select dallo storage S3 Standard-IA

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Select-Returned-ZIA-Bytes	GB	Orario	La quantità di dati restituiti con le richieste Select dallo storage S3 One Zone-IA
<i>region</i> -Select-Scanned-Bytes	GB	Orario	La quantità di dati scansionati con richieste Seleziona dallo storage S3 Standard
<i>region</i> -Select-Scanned-GIR-Bytes	GB	Orario	La quantità di dati scansionati dall'archivio S3 Glacier Instant Retrieval con richieste Select.
<i>region</i> -Select-Scanned-INT-Bytes	GB	Orario	La quantità di dati scansionati con le richieste Select dallo storage S3 Intelligent-Tiering
<i>region</i> -Select-Scanned-SIA-Bytes	GB	Orario	La quantità di dati scansionati con le richieste Select dallo storage S3 Standard-IA
<i>region</i> -Select-Scanned-ZIA-Bytes	GB	Orario	La quantità di dati scansionati con le richieste Select dallo storage S3 One Zone-IA

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Standard-Retrieval-Bytes	GB	Orario	La quantità di dati recuperati con richieste standard S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive
<i>region</i> -StorageAnalytics-ObjCount	Oggetti	Orario	Il numero di oggetti univoci monitorati in ciascuna configurazione di Storage Class Analysis.
<i>region</i> -StorageLens-ObjCount	Oggetti	Giornaliero	Il numero di oggetti univoci in ogni pannello di controllo di S3 Storage Lens monitorati da parametri e raccomandazioni avanzati di S3 Storage Lens.
<i>region</i> -StorageLensFreeTier-ObjCount	Oggetti	Giornaliero	Il numero di oggetti univoci in ogni pannello di controllo di S3 Storage Lens monitorati da parametri di utilizzo di S3 Storage Lens.
StorageObjectCount	Conteggio	Giornaliero	Numero di oggetti archiviati in un determinato bucket

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Tables-CompactedObjects	Oggetti	Orario	Numero di oggetti compattati nei bucket di Tabelle Amazon S3 utilizzando la strategia di compattazione binpack in un processo di compattazione di Tabelle Amazon S3.
<i>region</i> -Tables-SortCompactedObjects-	Oggetti	Orario	Numero di oggetti compattati nei bucket di Tabelle Amazon S3 utilizzando sort o le strategie di compattazione z-order in un processo di compattazione di Tabelle Amazon S3.
<i>region</i> -Tables-MonitoredObjects	Oggetti	Orario	Numero di oggetti nei bucket di Tabelle Amazon S3
<i>region</i> -Tables-ProcessedBytes	GB	Orario	Quantità di dati elaborati per la compattazione nei bucket di Tabelle Amazon S3
<i>region</i> -Tables-Requests-Tier1	Conteggio	Orario	Numero di richieste PUT sui bucket di Tabelle Amazon S3

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -Tables-Requests-Tier2	Conteggio	Orario	Numero di richieste GET e di tutte le altre richieste di tipo non-Tier1 sui bucket di Tabelle Amazon S3
<i>region</i> -Tables-TimedStorage-ByteHrs	GB-Month	Giornaliero	Il numero di tali dati GB-months è stato archiviato in bucket da tabella Amazon S3.
<i>region</i> -TagStorage-TagHrs	Tag-Hours	Giornaliero	Tag complessivi su tutti gli oggetti del bucket indicati su base oraria
<i>region</i> -TimedStorage-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nello storage S3 Standard
<i>region</i> -TimedStorage-GDA-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nello storage S3 Glacier Deep Archive.
<i>region</i> -TimedStorage-GDA-Staging	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nello storage di staging S3 Glacier Deep Archive.
<i>region</i> -TimedStorage-GIR-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nello storage S3 Glacier Instant Retrieval.

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -TimedStorage-GIR-SmObjects	GB-Month	Giornaliero	Il numero di GB-months quei piccoli oggetti (inferiori a 128 KB) è stato archiviato nello storage S3 Glacier Instant Retrieval.
<i>region</i> -TimedStorage-GlacierByteHrs	GB-Month	Giornaliero	Il numero di quei dati è stato archiviato nello GB-months storage S3 Glacier Flexible Retrieval
<i>region</i> -TimedStorage-GlacierStaging	GB-Month	Giornaliero	Il numero di quei dati è stato archiviato nello GB-months storage di staging S3 Glacier Flexible Retrieval
<i>region</i> -TimedStorage-INT-FA-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months tali dati è stato archiviato nel livello Frequent Access dello storage S3 Intelligent-Tiering
<i>region</i> -TimedStorage-INT-IA-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months tali dati è stato archiviato nel livello Infrequent Access dello storage S3 Intelligent-Tiering
<i>region</i> -TimedStorage-INT-AA-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato nel livello Archive Access dello storage S3 Intelligent-Tiering

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -TimedStorage-INT-AIA-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nel livello Archive Instant Access dello storage S3 Intelligent-Tiering
<i>region</i> -TimedStorage-INT-DAA-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nel livello Deep Archive Access dello storage S3 Intelligent-Tiering
<i>region</i> -TimedStorage-RRS-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months tali dati è stato archiviato o nello storage RRRS (Reduced Redundancy Storage)
<i>region</i> -TimedStorage-SIA-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nello storage S3 Standard-IA
<i>region</i> -TimedStorage-SIA-SmObjects	GB-Month	Giornaliero	Il numero di GB-months quei piccoli oggetti (inferiori a 128 KB) è stato archiviato nello storage S3 4 Standard-IA
<i>region</i> -TimedStorage-XZ-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nello storage S3 Express One Zone

Tipo di utilizzo	unità	Granularità	Descrizione
<i>region</i> -TimedStorage-ZIA-ByteHrs	GB-Month	Giornaliero	Il numero di GB-months quei dati è stato archiviato o nello storage S3 One Zone-IA
<i>region</i> -TimedStorage-ZIA-SmObjects	GB-Month	Giornaliero	Il numero di GB-months quei piccoli oggetti (inferiori a 128 KB) è stato archiviato nello storage S3 One Zone-IA
<i>region</i> -Upload-XZ	GB	Orario	La porzione di dati che supera i 512 KB in una determinata richiesta di upload (PUT o COPY) con S3 Express One Zone

Note

1. I tipi di Global-Bucket-Hrs-FreeTier utilizzo Global-Bucket-Hrs e si applicano ai bucket per uso generico in ambito commerciale Regioni AWS e. AWS GovCloud (US)
2. Se termini un trasferimento prima del completamento, la quantità di dati trasferiti può superare la quantità di dati ricevuti dall'applicazione. Questa discrepanza può verificarsi perché una richiesta di terminazione del trasferimento non può essere eseguita istantaneamente e una certa quantità di dati potrebbe essere in transito, in attesa dell'esecuzione della richiesta di terminazione. Questi dati in transito vengono fatturati come dati trasferiti "in uscita".
3. Per gli oggetti archiviati nelle classi di archiviazione S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive che vengono eliminati, sovrascritti o trasferiti prima del periodo minimo di conservazione (90 giorni per S3 Glacier Instant Retrieval e S3 Glacier Flexible Retrieval, 180 giorni per S3 Glacier Deep Archive), è previsto un addebito proporzionale per gigabyte per i giorni rimanenti. Questi addebiti vengono riportati in fattura rispettivamente come tipi di utilizzo EarlyDelete-GIR, EarlyDelete-ByteHrs, e EarlyDelete-GDA.

4. Per gli oggetti che si trovano nello Zone-IA storage S3 Standard-IA o S3 One, quando vengono eliminati, sovrascritti o trasferiti a una classe di archiviazione diversa prima di 30 giorni, è previsto un addebito ripartito proporzionalmente per gigabyte per i giorni rimanenti.
5. Per gli oggetti di piccole dimensioni (inferiori a 128 KB) che si trovano nello Zone-IA storage S3 Standard-IA o S3 One, quando vengono eliminati, sovrascritti o trasferiti a una classe di archiviazione diversa prima di 30 giorni, viene applicata una tariffa proporzionale per gigabyte per i giorni rimanenti.
6. Non esiste una dimensione minima fatturabile degli oggetti per gli oggetti nella classe di archiviazione S3 Intelligent-Tiering. Gli oggetti di dimensioni inferiori a 128 KB non sono monitorati né idonei per il tiering automatico. Gli oggetti più piccoli vengono sempre archiviati nel livello S3 Intelligent-Tiering Frequent Access.
7. Quando si avvia una richiesta `CreateMultipartUpload`, `UploadPart` o `UploadPartCopy` alle classi di storage Recupero flessibile S3 Glacier o S3 Glacier Deep Archive, le richieste vengono fatturate alle tariffe S3 Standard fino al completamento del caricamento multiparte. Una volta completato il caricamento, la singola `CompleteMultipartUpload` richiesta viene fatturata alla PUT tariffa dello storage S3 Glacier di destinazione. In-progress le parti di caricamento in più parti per PUT a sulla classe di storage S3 Glacier Flexible Retrieval vengono fatturate come S3 Glacier Flexible Retrieval Staging Storage alle tariffe di archiviazione S3 Standard fino al completamento del caricamento. Allo stesso modo, le parti di caricamento multiparte in corso per PUT nella classe di storage S3 Glacier Deep Archive vengono fatturate come S3 Glacier Deep Archive Staging Storage alle tariffe di archiviazione S3 Standard fino al completamento del caricamento.
8. S3 Express One Zone applica un costo forfettario per richiesta per dimensioni fino a 512 KB. Per le richieste PUT e GET viene applicato un costo aggiuntivo per GB per la parte di richiesta superiore a 512 KB.
9. Per informazioni sulle funzionalità supportate per la classe di archiviazione S3 Express One Zone, consulta [Funzioni di Amazon S3 non supportate dai bucket della directory](#).
- 10 I tipi di utilizzo con unità fatturate in GB sono calcolati in byte nei report di utilizzo.
- 11 A GB-Month si ricava prendendo il numero totale di GB-hours, aggregandolo nel corso di un mese e dividendolo per il numero di ore di quel mese. Per saperne di più, consulta [Domande frequenti: come verrà addebitato e fatturato l'utilizzo di Amazon S3?](#)

Note

In generale, ai proprietari di bucket S3 vengono addebitati i costi associati alle richieste con risposte HTTP 200 OK andate a buon fine e risposte di errore del client HTTP 4XX. Ai proprietari di bucket non vengono addebitati i costi per le risposte di errore del server HTTP 5XX, come ad esempio gli errori HTTP 503 Slow Down. Per ulteriori informazioni sui codici di errore S3 sotto i codici di stato HTTP 3XX e 4XX che non vengono fatturati, consulta [Fatturazione per le risposte di errore di Amazon S3](#). Per ulteriori informazioni sui costi addebitati in caso di configurazione del bucket come bucket con pagamento a carico del richiedente, consulta [Come funzionano i pagamenti a carico del richiedente](#).

Operazioni di monitoraggio nei report di utilizzo

Le operazioni descrivono l'azione intrapresa sull' AWS oggetto o sul bucket in base al tipo di utilizzo specificato. Le operazioni sono indicate con codici autoesplicativi, ad esempio PutObject o ListBucket. Fare riferimento a tali codici per vedere quali operazioni nel bucket hanno generato un tipo di utilizzo specifico. Quando crei un report di utilizzo, puoi scegliere di specificare All Operations (Tutte le operazioni) o un'operazione specifica, ad esempio GetObject.

Ulteriori informazioni

- [AWS report di utilizzo per Amazon S3](#)
- [AWS Billing report per Amazon S3](#)
- [Prezzi di Amazon S3](#)
- [Domande frequenti su Amazon S3](#)

Fatturazione per le risposte di errore di Amazon S3

In generale, ai proprietari di bucket S3 vengono addebitati i costi associati alle richieste con risposte HTTP 200 OK andate a buon fine e risposte di errore del client HTTP 4XX. Ai proprietari di bucket non vengono addebitati i costi per le risposte di errore del server HTTP 5XX, come ad esempio gli errori HTTP 503 Slow Down. Per ulteriori informazioni sui costi addebitati in caso di configurazione del bucket come bucket con pagamento a carico del richiedente, consulta [Come funzionano i pagamenti a carico del richiedente](#).

La tabella seguente elenca i codici di errore specifici inclusi tra i codici di stato HTTP 3XX e 4XX per cui non vengono addebitati costi. Per i bucket configurati con l'hosting di siti web, i costi applicabili associati alle richieste e ad altri elementi vengono comunque applicati quando S3 restituisce un [documento di errore personalizzato](#) o per i reindirizzamenti personalizzati.

 Note

Per AccessDenied (HTTP 403 Forbidden), S3 non addebita alcun costo al proprietario del bucket quando la richiesta viene avviata al di fuori dell'account AWS individuale del proprietario del bucket o dell'organizzazione AWS del proprietario del bucket.

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
301 Moved Permanently (301 Spostato definitivamente)	PermanentRedirect	Il bucket a cui si sta tentando di accedere deve essere indirizzato tramite l'endpoint specificato. Inviare tutte le richieste future a questo endpoint.	
	PermanentRedirectControlError	L'operazione API a cui si sta tentando di accedere deve essere indirizzata tramite l'endpoint specificato. Inviare tutte le richieste future a questo endpoint.	
307 Reindirizzamento temporaneo	TemporaryRedirect	L'utente viene reindirizzato al bucket mentre il server del sistema dei nomi di dominio (DNS) viene aggiornato.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
400 Richiesta non valida	AuthorizationHeaderMalformed	L'intestazione di autorizzazione fornita non è valida.	
	AuthorizationQueryParametersError	I parametri della query di autorizzazione forniti non sono validi.	
	ConnectionClosedByRequester	Restituito al chiamante originale quando si verifica un errore durante la lettura del corpo di WriteGetObjectResponse.	
	DeviceNotActiveError	Il dispositivo non è attualmente attivo.	
	EndpointNotFound	Indirizzare le richieste all'endpoint corretto.	
	ExpiredToken	Il token fornito è scaduto.	
	IllegalLocationConstraintException	Si sta tentando di accedere a un bucket da una Regione diversa da quella in cui esiste il bucket. Per evitare questo errore, utilizzare l'opzione --region. Ad esempio: <code>aws s3 cp awsexample.txt s3://amzn-s3-demo-bucket / --region ap-east-1</code> .	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	InvalidArgument	<p>Questo errore può verificarsi per i seguenti motivi:</p> <ul style="list-style-type: none">• L'argomento specificato non è valido.• Nella richiesta manca un'intestazione obbligatoria.• L'argomento specificato è incompleto o nel formato errato.• L'argomento specificato deve avere una lunghezza maggiore o uguale a 3.	
	InvalidBucketOwner AWSAccountID	Il valore del parametro previsto per il proprietario del bucket deve essere l'ID di un Account AWS.	
	InvalidDigest	Il valore content-MD5 o checksum specificato non è valido.	
	InvalidEncryptionA lgorithmError	La richiesta di crittografia specificata non è valida. Il valore valido è AES256.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	InvalidHostHeader	Le intestazioni dell'host fornite nella richiesta utilizzano uno stile di indirizzamento errato.	
	InvalidHttpMethod	La richiesta è stata effettuata utilizzando un metodo HTTP imprevisto.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	InvalidRequest	<p>Questo errore può verificarsi per i seguenti motivi:</p> <ul style="list-style-type: none">• La richiesta utilizza la versione della firma errata. Utilizzare AWS4-HMAC-SHA256 (Signature Version 4).• Un punto di accesso può essere creato solo per un bucket esistente.• Il punto di accesso non si trova in uno stato in cui può essere eliminato.• Un punto di accesso può essere elencato solo per un bucket esistente.• Il token successivo non è valido.• È necessario specificare almeno un'operazione in una regola del ciclo di vita.•	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
		<p>È necessario specificare almeno una regola del ciclo di vita.</p> <ul style="list-style-type: none">• Il numero di regole del ciclo di vita non deve superare il limite consentito di 1.000 regole.• L'intervallo per il parametro <code>MaxResults</code> non è valido.• Le richieste SOAP devono essere effettuate tramite una connessione HTTPS.• Amazon S3 Transfer Acceleration non è supportato per i bucket con nomi non conformi a DNS.• Amazon S3 Transfer Acceleration non è supportato per i bucket con punti (.) nei nomi.• L'endpoint Amazon S3 Transfer Acceleration supporta solo richieste in stile virtuale.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
		<ul style="list-style-type: none">• Amazon S3 Transfer Acceleration non è configurato in questo bucket.• Amazon S3 Transfer Acceleration è disabilitato in questo bucket.• Amazon S3 Transfer Acceleration non è supportato in questo bucket. Per assistenza, contattare il Supporto.• Amazon S3 Transfer Acceleration non può essere abilitato in questo bucket. Per assistenza, contattare il Supporto.• Valori in conflitto forniti nelle intestazioni HTTP e nei parametri di query.• Valori in conflitto forniti nelle intestazioni HTTP e nei campi del modulo POST.• Richiesta CopyObject effettuata su oggetti di	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
		dimensioni superiori a 5 GB.	
	InvalidSessionException	Restituito se la sessione non esiste più perché è andata in timeout o scaduta.	
	InvalidSignature	La firma della richiesta calcolata dal server non corrisponde alla firma fornita dall'utente. Verificare la chiave di accesso segreta di AWS e il metodo di firma. Per ulteriori informazioni, consulta Signing and authenticating REST requests .	
	InvalidSOAPRequest	Il corpo della richiesta SOAP non è valido.	
	InvalidStorageClass	La classe di storage specificata non è valida.	
	InvalidTag	La richiesta contiene un tag inserito non valido. Ad esempio, la richiesta potrebbe contenere chiavi duplicate, chiavi o valori troppo lunghi oppure tag di sistema.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	InvalidToken	Il token fornito ha un formato errato o comunque non è valido.	
	InvalidURI	L'URI specificato non può essere analizzato.	
	KeyTooLongError	La chiave è troppo lunga.	
	KMS.DisabledException	La richiesta è stata rifiutata perché la chiave KMS specificata non è abilitata.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	KMS.InvalidKeyUsageException	<p>La richiesta è stata rifiutata per uno dei seguenti motivi:</p> <ul style="list-style-type: none">• Il valore KeyUsage della chiave KMS è incompatibile con l'operazione API.• L'algoritmo di crittografia o di firma specificato per l'operazione è incompatibile con il tipo di materiale della chiave KMS (KeySpec). <p>Per crittografare, decrittografare, ricrittografare e generare le chiavi di dati, KeyUsage deve essere ENCRYPT_DECRYPT. Per firmare e verificare i messaggi, KeyUsage deve essere SIGN_VERIFY. Per generare e verificare i codici di autenticazione dei messaggi (MAC), KeyUsage deve essere GENERATE_VERIFY_MAC. Per ricavare i segreti dell'accordo della chiave, KeyUsage deve essere</p>	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
		<p>KEY_AGREEMENT.</p> <p>Per trovare il valore KeyUsage di una chiave KMS, utilizzare l'operazione DescribeKey.</p> <p>Per trovare gli algoritmi di crittografia o di firma supportati per una particolare chiave KMS, utilizzare l'operazione DescribeKey.</p>	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	KMS.KMSInvalidStateException	<p>La richiesta è stata rifiutata perché lo stato della risorsa specificata non è valido per questa richiesta. Questa eccezione indica una delle seguenti situazioni:</p> <ul style="list-style-type: none">• Lo stato della chiave KMS non è compatibile con l'operazione. <p>Per trovare lo stato della chiave, utilizzare l'operazione <code>DescribeKey</code>. Per saperne di più su quali sono gli stati delle chiavi compatibili con ciascuna operazione KMS, consulta Key states of AWS KMS keys nella Guida per gli sviluppatori del AWS Key Management Service.</p> <ul style="list-style-type: none">• Per le operazioni di crittografia sulle chiavi KMS negli archivi di chiavi personalizzati, questa eccezione rappresenta un errore generale con molte possibili cause. Per identificare la causa,	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
		vedere il messaggio di errore che accompagna l'eccezione.	
	KMS.NotFoundException	La richiesta è stata rifiutata perché non è possibile trovare l'entità o la risorsa specificata.	
	LambdaInvalidResponse	Restituito al chiamante originale quando WriteGetObjectResponse risponde con ValidationError a AWS Lambda. Per ulteriori dettagli, vedere il messaggio ValidationError. Non tutti i casi di ValidationError generano un errore LambdaInvalidResponse.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	LambdaInvocationFailed	Invocazione della funzione Lambda non riuscita. I chiamanti potrebbero ricevere il seguente errore quando Lambda per oggetti S3 non è in grado di invocare correttamente la funzione Lambda configurata. Il messaggio di errore potrebbe contenere dettagli su un eventuale errore restituito dal servizio AWS Lambda quando si invoca la funzione (ad esempio, codice di stato, codice di errore, messaggio di errore e ID richiesta).	
	MalformedACLError	L'ACL fornito non è in un formato valido o non è stato convalidato in base al nostro schema pubblicato.	
	MalformedPOSTRequest	Il corpo della richiesta POST non è multipart/form-data in un formato valido.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	MalformedXML	Il documento XML fornito non è in un formato valido o non è stato convalidato in base al nostro schema pubblicato.	
	MaxPostPreDataLengthExceededError	I campi della richiesta POST che precedono il file di caricamento sono troppo grandi.	
	MetadataTooLarge	Le intestazioni dei metadati superano la dimensione massima consentita per i metadati.	
	MissingAttachment	Era previsto un allegato SOAP, ma non è stato trovato.	
	MissingRequestBodyError	È stato inviato un documento XML vuoto come richiesta.	
	MissingSecurityHeader	Nella richiesta manca un'intestazione obbligatoria.	
	NoLoggingStatusForKey	Non esiste una risorsa secondaria dello stato di registrazione per una chiave.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	NotDeviceOwnerError	Il dispositivo che ha generato il token non è di proprietà dell'utente autenticato.	
	ResponseInterrupted	Restituito al chiamante originale quando si verifica un errore durante la lettura del corpo di WriteGetObjectResponse.	
	RequestHeaderSectionTooLarge	L'intestazione della richiesta e i parametri della query utilizzati per effettuare la richiesta superano le dimensioni massime consentite.	
	TokenCodeInvalidError	Il numero di serie e/o il codice token forniti non sono validi.	
	UnexpectedContent	Questa richiesta contiene contenuti non supportati.	
	UnsupportedArgument	La richiesta contiene un argomento non supportato.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	UnsupportedSignature	La richiesta fornita è firmata con una versione del token STS non supportata o la versione della firma non è supportata.	
	UserKeyMustBeSpecified	La richiesta POST del bucket deve contenere il nome di campo specificato. Se è specificato, controllare l'ordine dei campi.	
	IncorrectEndpoint	Il bucket specificato esiste in un'altra Regione. Indirizzare le richieste all'endpoint corretto.	
	ValidationError	Gli errori di convalida possono essere restituiti dall'operazione API WriteGetObjectResponse e possono verificarsi per numerose ragioni. Per ulteriori dettagli, vedere il messaggio di errore.	
403 Non consentito	RequestTimeTooSkewed	La differenza tra l'ora della richiesta e l'ora del server è troppo grande.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	SignatureDoesNotMatch	La firma della richiesta calcolata dal server non corrisponde alla firma fornita dall'utente. Verificare la chiave di accesso segreta di AWS e il metodo di firma. Per ulteriori informazioni, vedere Autenticazione REST e Autenticazione SOAP .	
	NotSignedUp	L'account non è registrato per il servizio Amazon S3. È necessario registrarsi prima di poter utilizzare Amazon S3. È possibile registrarsi al seguente URL: https://aws.amazon.com/s3	
	InvalidSecurity	Le credenziali di sicurezza fornite non sono valide.	
	InvalidPayer	Tutti gli accessi a questo oggetto sono stati disabilitati. Per ulteriore assistenza, vedere Contattaci .	
	InvalidAccessKeyId	L'ID chiave di accesso AWS fornito non esiste nei nostri record.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	AccountProblem	Si è verificato un problema con l'Account AWS che impedisce il corretto completamento dell'operazione. Per ulteriore assistenza, vedere Contattaci .	
	UnauthorizedAccessError	Applicabile solo nelle Regioni della Cina. Restituito quando viene effettuata una richiesta a un bucket che non dispone di una licenza ICP. Per ulteriori informazioni, consulta ICP Recordal .	
	UnexpectedIPError	Applicabile solo nelle Regioni della Cina. La richiesta è stata rifiutata perché l'IP era imprevisto.	
	MissingAuthenticationToken	La richiesta non è firmata.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	LambdaPermissionError	Il chiamante non è autorizzato a invocare la funzione Lambda. Il chiamante deve disporre dell'autorizzazione per invocare la funzione Lambda. Controllare le policy collegate al chiamante e assicurarsi che disponga dell'autorizzazione per utilizzare <code>lambda:Invoke</code> per la funzione configurata. Il messaggio di errore potrebbe contenere dettagli su un eventuale errore restituito dal servizio Lambda quando si invoca la funzione (ad esempio, codice di stato, codice di errore, messaggio di errore e ID richiesta).	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
404 Not Found (404 Non trovato)	LambdaNotFound	La funzione AWS Lambda non è stata trovata. La funzione Lambda, la versione o l'alias configurati non sono stati trovati durante il tentativo di invocarli . Assicurarsi che la configurazione del punto di accesso Lambda per oggetti S3 punti all'ARN della funzione Lambda corretto. Il messaggio di errore potrebbe contenere dettagli su un eventuale errore restituito dal servizio AWS Lambda quando si invoca la funzione (ad esempio, codice di stato, codice di errore, messaggio di errore e ID richiesta).	
	NoSuchAsyncRequest	La richiesta specificata non è stata trovata.	
	NoSuchObjectLockConfiguration	L'oggetto specificato non ha una configurazione ObjectLock.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	NoSuchUpload	Il caricamento in più parti specificato non esiste. L'ID di caricamento potrebbe non essere valido oppure il caricamento in più parti potrebbe essere stato interrotto o completato.	
	NoSuchWebsiteConfiguration	Il bucket specificato non ha una configurazione del sito web.	
	NoTransformationDefined	Nessuna trasformazione trovata per questo punto di accesso per le espressioni Lambda dell'oggetto.	
	ObjectLockConfigurationNotFoundError	La configurazione Object Lock non esiste per questo bucket.	
405 Metodo non consentito	MethodNotAllowed	Il metodo specificato non è consentito su questa risorsa.	
409 Conflitto	BucketAlreadyExists	Il nome del bucket richiesto non è disponibile. Lo spazio dei nomi del bucket è condiviso da tutti gli utenti del sistema. Specificare un nome diverso e riprovare.	

Codice di stato HTTP	Codice di errore	Descrizione del codice di errore	
	InvalidBucketState	La richiesta non è valida per lo stato corrente del bucket.	
	OperationAborted	Su questa risorsa è attualmente in corso un'operazione condizionale in conflitto. Riprovare.	
411 Lunghezza richiesta	MissingContentLength	È necessario fornire l'intestazione HTTP Content-Length.	
412 Precondizione non riuscita	RequestIsNotMultipartContent	Una richiesta POST del bucket deve essere del tipo enclosure-type multipart/form-data.	
416 Impossibile attenersi all'intervallo richiesto	InvalidRange	L'intervallo richiesto non è valido per la richiesta. Provare un altro intervallo.	

Comprensione e gestione delle classi di storage Amazon S3

A ogni oggetto di Amazon S3 è associata una classe di storage. Per impostazione predefinita, gli oggetti in S3 sono archiviati nella classe di storage S3 Standard; tuttavia Amazon S3 offre una gamma di altre classi di storage per gli oggetti che vengono archiviati dall'utente. Puoi scegliere una classe di storage a seconda dello scenario del caso d'uso e dei requisiti relativi all'accesso e alle prestazioni. La scelta di una classe di storage progettata per il proprio caso d'uso consente di ottimizzare i costi di archiviazione, le prestazioni e la disponibilità degli oggetti. Tutte queste classi di storage offrono un livello elevato di durabilità.

Nelle sezioni seguenti vengono fornite informazioni dettagliate sulle varie classi di storage e su come impostare la classe di storage più adatta ai tuoi oggetti.

Argomenti

- [Classi di storage per oggetti a cui si accede di frequente](#)
- [Classe di storage per ottimizzare automaticamente i dati con modelli di accesso variabili o sconosciuti](#)
- [Classi di storage per oggetti a cui si accede raramente](#)
- [Classi di storage per oggetti con accesso non frequente](#)
- [Classe di storage per Amazon S3 su Outposts](#)
- [Confronto delle classi di storage di Amazon S3](#)
- [Impostazione della classe di storage di un oggetto](#)
- [Analisi di Amazon S3 – Analisi della classe di storage](#)
- [Gestione dei costi di storage con il Piano intelligente Amazon S3](#)
- [Informazioni sulle classi di storage S3 Glacier per l'archiviazione di dati a lungo termine](#)
- [Utilizzo di oggetti archiviati](#)

Classi di storage per oggetti a cui si accede di frequente

Per i casi d'uso sensibili alle prestazioni (quelli che richiedono un tempo di accesso in millisecondi) e per i dati a cui si accede di frequente, Amazon S3 fornisce le seguenti classi di storage:

- **S3 Standard (STANDARD):** classe di archiviazione predefinita. Se al momento del caricamento di un oggetto non specifichi una classe di storage, Amazon S3 assegna la classe di storage S3 Standard. Per aiutarti a ottimizzare i costi tra S3 Standard e S3 Standard-IA puoi utilizzare. [Analisi di Amazon S3 – Analisi della classe di storage](#)
- **S3 Express One Zone (EXPRESS_ONEZONE):** Amazon S3 Express One Zone è una classe di archiviazione Amazon S3 a zona singola ad alte prestazioni, creata appositamente per fornire un accesso ai dati coerente nell'ordine di millisecondi per le applicazioni sensibili alla latenza. S3 Express One Zone è la classe di storage di oggetti cloud con la latenza minima attualmente disponibile, con velocità di accesso ai dati fino a 10 volte maggiori e con costi di richiesta inferiori del 50% rispetto a S3 Standard. Con S3 Express One Zone, i dati vengono archiviati in modo ridondante su più dispositivi all'interno di una singola zona di disponibilità. Per ulteriori informazioni, consulta [S3 Express One Zone](#).

- Archiviazione a ridondanza ridotta (REDUCED_REDUNDANCY): la classe di archiviazione a ridondanza ridotta (RRS, Reduced Redundancy Storage) è concepita per dati riproducibili non critici che possono essere archiviati con una ridondanza inferiore rispetto alla classe di archiviazione S3 Standard.

 Important

È consigliabile non utilizzare questa classe di archiviazione. La classe di archiviazione S3 Standard è più conveniente in termini di costi.

Riguardo la durabilità, gli oggetti RRS hanno una perdita di oggetti annua media stimata dello 0,01%. Se perdi un oggetto RRS, Amazon S3 restituisce un errore 405 per le richieste eseguite a tale oggetto.

Classe di storage per ottimizzare automaticamente i dati con modelli di accesso variabili o sconosciuti

S3 Intelligent-Tiering (INTELLIGENT_TIERING) è una classe di storage Amazon S3 progettata per ottimizzare i costi di storage spostando automaticamente i dati al livello di accesso più conveniente, senza impatto sulle prestazioni o sovraccarico operativo. S3 Intelligent-Tiering è l'unica classe di storage cloud che offre risparmi automatici sui costi spostando i dati su un livello di oggetto granulare tra i livelli di accesso quando i modelli di accesso cambiano. S3 Intelligent-Tiering è la classe di storage ideale quando si desidera ottimizzare i costi di archiviazione per dati con modelli di accesso sconosciuti o mutevoli. Non sono previsti costi di recupero per S3. Intelligent-Tiering

Con una piccola tariffa mensile per il monitoraggio e l'automazione degli oggetti, S3 Intelligent-Tiering monitora i modelli di accesso e sposta automaticamente gli oggetti a cui non è stato effettuato l'accesso a livelli di accesso a costi inferiori. S3 Intelligent-Tiering offre risparmi automatici sui costi di storage in tre livelli di accesso a bassa latenza e throughput elevato. Per i dati a cui è possibile accedere in modo asincrono, è possibile scegliere di attivare le funzionalità di archiviazione automatica all'interno della classe di storage S3. Intelligent-Tiering S3 Intelligent-Tiering è progettato per una disponibilità del 99,9% e una durata del 99,9%.

S3 archivia Intelligent-Tiering automaticamente gli oggetti in tre livelli di accesso:

- Accesso frequente: gli oggetti caricati o trasferiti su S3 Intelligent-Tiering vengono automaticamente archiviati nel livello di accesso frequente.

- **Accesso infrequente:** S3 Intelligent-Tiering sposta gli oggetti a cui non è stato effettuato l'accesso per 30 giorni consecutivi nel livello Infrequent Access.
- **Archive Instant Access:** con S3 Intelligent-Tiering, tutti gli oggetti esistenti a cui non si accede per 90 giorni consecutivi vengono automaticamente spostati nel livello Archive Instant Access.

Oltre a questi tre livelli, S3 Intelligent-Tiering offre due livelli di accesso all'archivio opzionali:

- **Accesso all'archivio:** S3 Intelligent-Tiering offre la possibilità di attivare il livello di accesso all'archivio per i dati a cui è possibile accedere in modo asincrono. Dopo l'attivazione, il livello Archive Access archivia automaticamente gli oggetti a cui non è stato eseguito l'accesso per un minimo di 90 giorni consecutivi.
- **Deep Archive Access** — S3 Intelligent-Tiering offre la possibilità di attivare il livello Deep Archive Access per i dati a cui è possibile accedere in modo asincrono. Dopo l'attivazione, il livello Deep Archive Access archivia automaticamente gli oggetti a cui non è stato eseguito l'accesso per un minimo di 180 giorni consecutivi.

Note

- Attivare il livello Archive Access per 90 giorni solo se si desidera ignorare il livello Archive Instant Access. Il livello Archive Access (Accesso archiviazione) offre costi di archiviazione leggermente inferiori con tempi di recupero nell'arco di minuti o ore. Il livello Archive Instant Access (Archiviazione con accesso istantaneo) offre un accesso in millisecondi e prestazioni a elevata velocità di trasmissione effettiva.
- Attiva i livelli Accesso di archiviazione e Accesso di archiviazione profonda solo se l'applicazione può accedere agli oggetti in modo asincrono. Se l'oggetto recuperato è archiviato nei livelli Archive Access (Accesso archiviazione) o Deep Archive Access (Accesso archiviazione profondo), prima devi ripristinarlo utilizzando `RestoreObject`.

Puoi [spostare i dati appena creati su S3 Intelligent-Tiering](#), impostandoli come classe di archiviazione predefinita. Puoi anche scegliere di attivare uno o entrambi i livelli di accesso all'archivio utilizzando l'operazione [PutBucketIntelligentTieringConfiguration](#) API AWS CLI, la console o Amazon S3. Per ulteriori informazioni sull'utilizzo di S3 Intelligent-Tiering e sull'attivazione dei livelli di accesso all'archivio, consulta [Usare S3 Intelligent-Tiering](#).

Per accedere agli oggetti nei livelli Accesso archivio o Accesso archivio approfondito, devi prima ripristinarli. Per ulteriori informazioni, consulta [Ripristino di oggetti dai livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access](#).

Note

Se le dimensioni di un oggetto sono inferiori a 128 KB, questo non è monitorato e il tiering automatico non è consentito. Gli oggetti più piccoli vengono sempre archiviati nel livello Accesso frequente. Per ulteriori informazioni su Intelligent-Tiering S3, vedere. [Livelli di accesso S3 Intelligent-Tiering](#)

Classi di storage per oggetti a cui si accede raramente

Le classi di Zone-IA storage S3 Standard-IA e S3 One sono progettate per dati di lunga durata e a cui si accede raramente. IA è l'acronimo di Infrequent Access (accesso non frequente). Zone-IA Gli oggetti S3 Standard-IA e S3 One sono disponibili per l'accesso in millisecondi (in modo simile alla classe di storage S3 Standard). Amazon S3 addebita un costo per il recupero di questi oggetti, di conseguenza sono più appropriati per i dati a cui si accede raramente. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Ad esempio, puoi scegliere le classi di storage S3 Standard-IA e S3 One per effettuare le seguenti operazioni: Zone-IA

- Per lo storage di backup.
- Per i dati più vecchi a cui si accede raramente ma che richiedono l'accesso in millisecondi. Ad esempio, quando carichi dati, puoi scegliere la classe di storage S3 Standard e utilizzare la configurazione del ciclo di vita per dire ad Amazon S3 di trasferire gli oggetti alla classe S3 o S3 One. Standard-IA Zone-IA

Per ulteriori informazioni sulla gestione del ciclo di vita, consulta [Gestione del ciclo di vita degli oggetti](#).

Note

Le classi di Zone-IA storage S3 Standard-IA e S3 One sono adatte per oggetti di dimensioni superiori a 128 KB che prevedi di archiviare per almeno 30 giorni. Se un oggetto è inferiore a 128 KB, Amazon S3 addebita il costo relativo a 128 KB. Se elimini un oggetto prima della

fine del periodo minimo di storage di 30 giorni, viene addebitato un costo corrispondente a 30 giorni. Gli oggetti eliminati, sovrascritti o trasferiti a una classe di archiviazione diversa prima di 30 giorni sono soggetti al normale costo di utilizzo dell'archiviazione e all'addebito ripartito proporzionalmente per il resto del periodo minimo di 30 giorni. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Di seguito sono riportate le differenze tra queste classi di storage:

- S3 Standard-IA (STANDARD_IA) — Amazon S3 archivia i dati degli oggetti in modo ridondante in più zone di disponibilità separate geograficamente (in modo simile alla classe di storage S3 Standard). Standard-IA Gli oggetti S3 sono resistenti alla perdita di una zona di disponibilità. Questa classe di storage offre una maggiore disponibilità e resilienza rispetto alla classe S3 One. Zone-IA Per aiutarti a ottimizzare i costi tra S3 Standard e Standard-IA S3, puoi utilizzare [Analisi di Amazon S3 – Analisi della classe di storage](#)
- S3 One Zone-IA (ONEZONE_IA): Amazon S3 archivia i dati degli oggetti in una sola zona di disponibilità, il che li rende meno costosi di S3. Standard-IA Tuttavia, i dati non sono resilienti alla perdita fisica della zona di disponibilità dovuta a disastri naturali, come terremoti e alluvioni. La classe di Zone-IA storage S3 One è resistente quanto S3 Standard-IA, ma è meno disponibile e meno resiliente. Per un confronto della durabilità e della disponibilità delle classi di storage, consulta [Confronto delle classi di storage di Amazon S3](#) alla fine della sezione. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#). Per i casi d'uso relativi alla residenza e all'isolamento dei dati, puoi creare bucket di directory nelle zone AWS locali e utilizzare le classi di archiviazione S3 Express One Zone (EXPRESS_ONEZONE) e S3 One (). Zone-IA ONEZONE_IA Per ulteriori informazioni sui bucket di directory in Zone locali, consulta [Carichi di lavoro di residenza dei dati](#).

Consigliamo quanto segue:

- S3 Standard-IA (STANDARD_IA): utilizzalo per la tua copia principale o unica dei dati che non possono essere ricreati.
- S3 One Zone-IA (ONEZONE_IA): da utilizzare se è possibile ricreare i dati in caso di errore nella zona di disponibilità, per le repliche degli oggetti durante la configurazione di S3 Replication (CRR). Cross-Region Inoltre, per la residenza e l'isolamento dei dati, è possibile creare bucket di directory nelle zone AWS locali e utilizzare la classe di storage S3 One. Zone-IA

Classi di storage per oggetti con accesso non frequente

Le classi di archiviazione S3 Glacier Instant Retrieval (GLACIER_IR), S3 Glacier Flexible Retrieval (GLACIER) e S3 Glacier Deep Archive (DEEP_ARCHIVE) sono progettate per l'archiviazione di dati a lungo termine e a basso costo. Queste classi di storage richiedono durate di archiviazione e costi di recupero minimi, il che le rende più efficaci per i dati a cui si accede raramente. Per ulteriori informazioni sulle classi di storage S3 Glacier, consulta [Informazioni sulle classi di storage S3 Glacier per l'archiviazione di dati a lungo termine](#).

In Amazon S3 sono disponibili le classi di storage S3 Glacier seguenti:

- S3 Glacier Instant Retrieval (GLACIER_IR): da utilizzare per i dati a lungo termine a cui si accede raramente e che richiede un recupero nell'ordine di millisecondi. I dati in questa classe di storage sono disponibili per l'accesso in tempo reale.
- S3 Glacier Flexible Retrieval (GLACIER): da utilizzare per le archiviazioni con porzioni di dati da recuperare nell'ordine di pochi minuti. I dati in questa classe di storage sono archiviati e non sono disponibili per l'accesso in tempo reale.
- S3 Glacier Deep Archive (DEEP_ARCHIVE): da utilizzare per l'archiviazione di dati a cui è necessario accedere raramente. I dati in questa classe di storage sono archiviati e non sono disponibili per l'accesso in tempo reale.

Recupero di oggetti archiviati

È possibile impostare la classe di archiviazione di un oggetto su S3 Glacier Flexible Retrieval (GLACIER) o S3 Glacier Deep Archive (DEEP_ARCHIVE) allo stesso modo di qualsiasi altra classe di archiviazione, come descritto nella sezione [Impostazione della classe di storage di un oggetto](#). Tuttavia, gli oggetti nelle classi di storage Recupero flessibile S3 Glacier e S3 Glacier Deep Archive sono archiviati e non sono disponibili per l'accesso in tempo reale. Per ulteriori informazioni, consulta [Informazioni sullo storage di archiviazione in S3 Glacier Flex Retrieval e S3 Glacier Deep Archive](#).

Note

Quando si utilizzano le classi di storage S3 Glacier, gli oggetti rimangono in Amazon S3. Non è possibile accedervi direttamente tramite il servizio Amazon Glacier separato. Per informazioni sul servizio Amazon Glacier, consulta la [Guida per gli sviluppatori di Amazon Glacier](#).

Classe di storage per Amazon S3 su Outposts

Con Amazon S3 on Outposts, puoi creare bucket S3 sulle tue AWS Outposts risorse e archiviare e recuperare oggetti in locale per applicazioni che richiedono accesso locale ai dati, elaborazione locale dei dati e residenza dei dati. Puoi utilizzare le stesse operazioni e funzionalità API di Amazon S3 AWS Outposts , tra cui policy di accesso, crittografia e tagging. Puoi usare S3 su Outposts tramite Console di gestione AWS, AWS CLI, AWS SDK o API REST.

S3 su Outposts offre una nuova classe di storage, S3 Outposts (OUTPOSTS). La classe di archiviazione S3 Outposts è disponibile solo per gli oggetti archiviati in bucket su Outposts. Se provi a utilizzare questa classe di archiviazione con un bucket S3 in un, si verifica un Regione AWS errore. `InvalidStorageClass` Inoltre, se provi a utilizzare altre classi di storage S3 con oggetti archiviati in bucket S3 su Outposts, si avrà la stessa risposta di errore.

Gli oggetti archiviati nella classe di storage S3 Outposts (OUTPOSTS) vengono sempre crittografati utilizzando la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (). SSE-S3 Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(\) SSE-S3](#).

Puoi anche scegliere esplicitamente di crittografare gli oggetti archiviati nella classe di storage S3 Outposts utilizzando la crittografia lato server con chiavi di crittografia fornite dal cliente (). SSE-C Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi fornite dal cliente \(\) SSE-C](#).

Note

S3 on Outposts non supporta la crittografia lato server con chiavi () (). AWS Key Management Service AWS KMS SSE-KMS

Per ulteriori informazioni su S3 su Outposts, consulta [Che cos'è Amazon S3 su Outposts?](#) nella Guida per l'utente di Amazon S3 su Outposts.

Confronto delle classi di storage di Amazon S3

Nella tabella seguente vengono confrontate le classi di storage con disponibilità, durata, durata minima di storage e altre considerazioni.

Storage Class	Designed for	Durability (designed for)	Availability (designed for)	Availability Zones	Min storage duration	Min billable object size	Other Considerations
STANDARD	Frequently accessed data	99.999999999%	99.99%	>= 3	None	None	None
STANDARD_IA	Long-lived, infrequently accessed data	99.999999999%	99.9%	>= 3	30 days	128 KB	Per GB retrieval fees apply.
INTELLIGENT_TIERING	Long-lived data with changing or unknown access patterns	99.999999999%	99.9%	>= 3	30 days	None	Monitoring and automation fees per object apply. No retrieval fees.
ONEZONE_IA	Long-lived, infrequently accessed, non-critical data	99.999999999%	99.5%	1	30 days	128 KB	Per GB retrieval fees apply. Not resilient to the loss of the Availability Zone.
GLACIER	Long-term data archiving with retrieval times ranging from minutes to hours	99.999999999%	99.99% (after you restore objects)	>= 3	90 days	None	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects .
DEEP_ARCHIVE	Archiving rarely accessed data with a default retrieval time of 12 hours	99.999999999%	99.99% (after you restore objects)	>= 3	180 days	None	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects .
RRS (Not recommended)	Frequently accessed, non-critical data	99.99%	99.99%	>= 3	None	None	None

* Recupero flessibile S3 Glacier richiede 40 KB di metadati aggiuntivi per ogni oggetto archiviato. Ciò include 32 KB di metadati addebitati alla tariffa Recupero flessibile S3 Glacier (richiesta per identificare e recuperare i dati) e altri 8 KB di dati addebitati alla tariffa S3 Standard. La tariffa S3 Standard è necessaria per mantenere il nome e i metadati definiti dall'utente per gli oggetti archiviati in Recupero flessibile S3 Glacier. Per ulteriori informazioni sulle classi di storage, consultare [Classi di storage di Amazon S3](#).

** S3 Glacier Deep Archive richiede 40 KB di metadati aggiuntivi per ogni oggetto archiviato. Ciò include 32 KB di metadati addebitati alla tariffa Deep Archive Amazon S3 Glacier (richiesta per identificare e recuperare i dati) e altri 8 KB di dati addebitati alla tariffa S3 Standard. La tariffa S3 Standard è necessaria per mantenere il nome e i metadati definiti dall'utente per gli oggetti archiviati in Deep Archive Amazon S3 Glacier. Per ulteriori informazioni sulle classi di storage, consultare [Classi di storage di Amazon S3](#).

Tieni presente che tutte le classi di storage ad eccezione di S3 One Zone-IA (ONEZONE_IA) e S3 Express One Zone (EXPRESS_ONEZONE) sono progettate per resistere alla perdita fisica di una zona di disponibilità a causa di disastri. Oltre ai requisiti relativi alle prestazioni, devi considerare anche i costi. Per il prezzo delle classi di storage, consulta [Prezzi di Amazon S3](#).

Impostazione della classe di storage di un oggetto

È possibile specificare una classe di archiviazione per un oggetto quando lo si carica. In caso contrario, Amazon S3 utilizza la classe di archiviazione Amazon S3 Standard predefinita per gli oggetti in bucket per uso generico. Puoi anche cambiare la classe di storage di un oggetto già

archiviato in un bucket generico Amazon S3 con qualsiasi altra classe di storage utilizzando la console Amazon S3, AWS gli SDK o (). AWS Command Line Interface AWS CLI Tutti questi approcci utilizzano le operazioni API di Amazon S3 per inviare richieste ad Amazon S3.

Note

Non è possibile modificare la classe di archiviazione degli oggetti archiviati nei bucket di directory.

È possibile indicare ad Amazon S3 di modificare automaticamente la classe di storage degli oggetti aggiungendo la configurazione del ciclo di vita S3 a un bucket. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#).

Quando si imposta la configurazione della replica S3, è possibile impostare la classe di storage per gli oggetti replicati su qualsiasi altra classe di storage. Tuttavia, non è possibile copiare oggetti archiviati nelle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Per ulteriori informazioni, consulta [Elementi del file di configurazione della replica](#).

Quando si imposta la classe di storage a livello di codice, si fornisce il valore della classe di storage. Di seguito è riportato un elenco di nomi di console per le classi di storage con i valori API corrispondenti:

- Archiviazione a ridondanza ridotta – REDUCED_REDUNDANCY
- S3 Express One Zone – EXPRESS_ONEZONE
- S3 Glacier Deep Archive – DEEP_ARCHIVE
- Recupero flessibile S3 Glacier – GLACIER
- Recupero istantaneo S3 Glacier – GLACIER_IR
- S3 — Intelligent-Tiering INTELLIGENT_TIERING
- S3 Uno — Zone-IA ONEZONE_IA
- S3 Standard – STANDARD
- S3 Standard-IA — STANDARD_IA

Impostazione della classe di storage di un nuovo oggetto

Per impostare la classe di storage quando si carica un oggetto, è possibile utilizzare i metodi riportati di seguito.

Utilizzo della console S3

Per impostare la classe di storage quando si carica un nuovo oggetto nella console:

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo: <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket in cui caricare le cartelle o i file.
4. Scegli Carica.
5. Nella finestra Carica scegli Proprietà.
6. In Classe di storage, scegli una classe di storage per i file che stai caricando.
7. (Facoltativo) Configura eventuali proprietà aggiuntive per i file che stai caricando. Per ulteriori informazioni, consulta [Caricamento degli oggetti](#)
8. Nella finestra Carica completa una delle seguenti operazioni:
 - Trascina i file e le cartelle nella finestra Carica.
 - Scegli Aggiungi file o Aggiungi cartella, seleziona i file o le cartelle da caricare e scegli Apri.
9. Scegli Carica.

Utilizzo della REST API

È possibile specificare la classe di storage di un oggetto quando lo si crea utilizzando le operazioni API PutObject, POST Object Object e CreateMultipartUpload, aggiungendo l'intestazione della richiesta x-amz-storage-class. Se non aggiungi questa intestazione, Amazon S3 utilizza la classe di storage predefinita S3 Standard (STANDARD).

Questa richiesta di esempio utilizza il [PutObject](#) comando per impostare la classe di archiviazione su un nuovo oggetto su S3: Intelligent-Tiering

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
```

```
x-amz-storage-class: INTELLIGENT_TIERING
```

Utilizzo di AWS CLI

Questo esempio utilizza il `put-object` comando per *my_images.tar.bz2* caricare il file *amzn-s3-demo-bucket1* nella classe *GLACIER* di archiviazione:

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key dir-1/my_images.tar.bz2 --  
storage-class GLACIER --body my_images.tar.bz2
```

Se la dimensione dell'oggetto è superiore a 5 GB, utilizza il seguente comando per impostare la classe di storage:

```
aws s3 cp large_test_file s3://amzn-s3-demo-bucket1 --storage-class GLACIER
```

Modifica della classe di storage di un oggetto esistente

Per impostare la classe di storage quando si carica un oggetto, è possibile utilizzare i metodi riportati di seguito.

Utilizzo della console S3

È possibile modificare la classe di storage di un oggetto utilizzando la console Amazon S3 se le dimensioni dell'oggetto sono inferiori a 5 GB. Se è più grande, si consiglia di aggiungere la configurazione del ciclo di vita di S3 per modificare la classe di storage dell'oggetto.

Per cambiare la classe di storage di un oggetto nella console:

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket che contiene gli oggetti da ripristinare.
4. Seleziona la casella di controllo a sinistra dei nomi degli oggetti da modificare.

5. Nel menu Azioni, scegli Modifica la classe di storage dall'elenco di opzioni visualizzato.
6. Seleziona una delle classi di storage disponibili per l'oggetto.
7. In Impostazioni di copia aggiuntive, scegli se eseguire Copia impostazioni dell'origine, Non specificare le impostazioni o Specifica le impostazioni. Copia impostazioni dell'origine è l'opzione predefinita. Se desideri copiare solo l'oggetto senza gli attributi delle impostazioni dell'origine, scegli Non specificare le impostazioni. Scegli Specifica le impostazioni per specificare le impostazioni per la classe di storage, le ACL, i tag degli oggetti, i metadati, la crittografia lato server e i checksum aggiuntivi.
8. Scegli Save changes (Salva modifiche). Amazon S3 salva le modifiche.

Utilizzo della REST API

Per cambiare la classe di storage di un oggetto esistente, utilizza i metodi riportati di seguito.

Per modificare la classe di archiviazione di un oggetto esistente, è necessario creare una copia dell'oggetto nella stessa posizione con una nuova classe di archiviazione utilizzando l'[CopyObject](#) operazione. La seguente richiesta di esempio copia un oggetto su se stesso con la classe di archiviazione modificata in S3: Intelligent-Tiering

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
x-amz-copy-source: /amzn-s3-demo-bucket1/my-image.jpg
x-amz-metadata-directive: COPY
x-amz-storage-class: INTELLIGENT_TIERING
```

Utilizzo di AWS CLI

Questo esempio utilizza il comando `cp` per modificare la classe di archiviazione di un oggetto esistente dalla classe di archiviazione corrente alla classe di archiviazione *DEEP_ARCHIVE* :

```
aws s3 cp object_S3_URI object_S3_URI --storage-class DEEP_ARCHIVE
```

Limitazione delle autorizzazioni delle policy di accesso a una classe di storage specifica

Quando concedi le autorizzazioni alle policy di accesso per le operazioni Amazon S3, è possibile utilizzare la chiave di condizione `s3:x-amz-storage-class` per limitare la classe di storage da utilizzare durante l'archiviazione degli oggetti caricati. Ad esempio, quando concedi l'autorizzazione `s3:PutObject`, puoi limitare il caricamento di oggetti a una classe di archiviazione specifica. Per un esempio di policy, consulta [Esempio: limitazione del caricamento di oggetti a oggetti con una classe di storage specifica](#).

Per ulteriori informazioni sull'utilizzo delle condizioni nelle policy e per l'elenco completo delle chiavi di condizione Amazon S3, consulta i seguenti argomenti:

- [Operazioni, risorse e chiavi di condizione per Amazon S3](#) nella Guida di riferimento per l'autorizzazione del servizio

Per ulteriori informazioni sulle autorizzazioni alle operazioni API S3 per tipi di risorse S3, consulta [Autorizzazioni necessarie per le operazioni API di Amazon S3](#).

- [Esempi di policy per i bucket che utilizzano le chiavi di condizione](#)

Analisi di Amazon S3 – Analisi della classe di storage

Lo strumento per l'analisi della classe di storage Amazon S3 Analytics consente di analizzare gli schemi di accesso allo storage per stabilire quando eseguire la transizione dei dati corretti alla classe di storage appropriata. Questa nuova funzionalità di analisi di Amazon S3 osserva gli schemi di accesso ai dati per determinare quando è opportuno spostare i dati meno utilizzati dallo storage STANDARD alla classe di storage STANDARD_IA (ad accesso infrequente). Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

Dopo l'osservazione degli schemi di accesso poco frequenti a un set di dati filtrati in un certo periodo di tempo da parte dell'analisi della classe di archiviazione, i risultati dell'analisi possono essere utilizzati per migliorare le configurazioni del ciclo di vita. È possibile configurare l'analisi della classe di archiviazione per analizzare tutti gli oggetti in un bucket, oppure si possono configurare filtri per raggruppare gli oggetti per l'analisi in base a un prefisso condiviso (ossia, oggetti i cui nomi iniziano con una stringa comune), ai tag dell'oggetto o a entrambe le opzioni. Con ogni probabilità, l'applicazione di filtri in base ai gruppi di oggetti si rivelerà la soluzione più vantaggiosa per l'analisi della classe di archiviazione.

 Important

L'analisi della classe di archiviazione fornisce solo suggerimenti per le classi da standard a standard (accesso infrequente).

La funzionalità di analisi della classe di archiviazione consente di attivare più filtri per bucket (fino a 1.000) e di ricevere un'analisi separata per ogni filtro. Le configurazioni a più filtri permettono di analizzare gruppi specifici di oggetti al fine di migliorare le configurazioni del ciclo di vita che trasferiscono gli oggetti alla classe STANDARD_IA.

L'analisi della classe di storage fornisce nella console Amazon S3 le visualizzazioni relative l'utilizzo dello storage aggiornate quotidianamente. Puoi anche esportare questi dati di utilizzo giornaliero in un bucket S3 e visualizzarli in un'applicazione per fogli di calcolo o con strumenti di business intelligence, come Quick.

Ci sono costi associati all'analisi della classe di archiviazione. Per informazioni sui prezzi, consulta Gestione e approfondimenti in [Prezzi di Amazon S3](#).

Argomenti

- [Come impostare l'analisi della classe di storage](#)
- [Come utilizzare l'analisi della classe di storage](#)
- [Come esportare i dati relativi all'analisi della classe di storage](#)
- [Configurazione dell'analisi della classe di storage](#)

Come impostare l'analisi della classe di storage

È possibile impostare l'analisi della classe di storage configurando i dati degli oggetti da analizzare. A seconda della configurazione, l'analisi della classe di storage può:

- Analizzare l'intero contenuto di un bucket.

Verrà generata un'analisi per tutti gli oggetti del bucket.

- Analizzare gli oggetti raggruppati in base al prefisso e ai tag.

Si possono configurare filtri che raggruppano gli oggetti per l'analisi in base a un prefisso, ai tag dell'oggetto o a una combinazione di entrambe le opzioni. Viene generata un'analisi separata

per ogni filtro configurato. È possibile definire più configurazioni di filtri per ciascun bucket (fino a 1.000).

- Esportare i dati dell'analisi.

Quando si configura l'analisi della classe di storage per un bucket o un filtro, si può scegliere di far esportare ogni giorno i relativi dati in un file. L'analisi del giorno corrente viene aggiunta al file per formare un registro storico dell'analisi per il filtro configurato. Il file viene aggiornato quotidianamente nella destinazione selezionata. Al momento della selezione dei dati da esportare, si specifica un bucket di destinazione e un prefisso di destinazione (facoltativo) dove scrivere il file.

Puoi utilizzare la console Amazon S3, l'API REST o gli AWS SDK or per configurare l'analisi delle AWS CLI classi di storage.

- Per informazioni su come configurare l'analisi delle classi di storage nella console Amazon S3, consulta [Configurazione dell'analisi della classe di storage](#).
- Per utilizzare l'API Amazon S3, utilizza l'API [PutBucketAnalyticsConfiguration](#) REST, o l'equivalente, disponibile negli AWS CLI SDK or. AWS

Come utilizzare l'analisi della classe di storage

L'analisi della classe di storage consente di osservare gli schemi di accesso ai dati nel tempo e raccogliere così informazioni utili per migliorare la gestione del ciclo di vita dello storage STANDARD_IA. Dopo aver configurato un filtro, entro 24 o 48 ore nella console Amazon S3 inizierà a essere disponibile l'analisi dei dati basata sul filtro. Tuttavia, prima di fornire un risultato, la funzionalità continuerà a osservare gli schemi di accesso a un insieme di dati filtrati per almeno 30 giorni, al fine di raccogliere le informazioni necessarie. Dopo i primi risultati, l'analisi resta in esecuzione e aggiorna il risultato via via che gli schemi di accesso cambiano.

Quando configuri un filtro per la prima volta, alla console Amazon S3 potrebbe occorrere qualche istante per analizzare i tuoi dati.

L'analisi della classe di archiviazione continua a osservare gli schemi di accesso a un insieme di dati di oggetti filtrati per almeno 30 giorni, al fine di raccogliere informazioni sufficienti. Una volta raccolte informazioni a sufficienza, nella console Amazon S3 verrà visualizzato un messaggio di analisi completata.

Durante l'analisi degli oggetti ad accesso infrequente, l'analisi della classe di storage prende in considerazione un insieme filtrato di oggetti raggruppati in base al tempo trascorso dal loro

caricamento su Amazon S3. e determina se l'accesso al gruppo di età è infrequente valutando i fattori seguenti per l'insieme di dati filtrati:

- Oggetti nella classe di storage STANDARD più grandi di 128 KB.
- Volume medio di storage totale per gruppo di età
- Numero medio di byte trasferiti in uscita (non la frequenza) per gruppo di età.
- I dati dell'esportazione analitica includono solo le richieste con dati pertinenti per l'analisi della classe di storage. Per questo motivo il numero di richieste, nonché il totale dei byte per caricamenti e richieste, potrebbe variare rispetto a quanto riportato nei parametri dello storage o tracciato dai sistemi interni dell'utente
- Benché non siano conteggiate nell'analisi, le richieste GET e PUT non andate a buon fine sono incluse nei parametri dello storage.

Volume di storage recuperato

I grafici della console Amazon S3 mostrano il volume di storage dei dati filtrati che è stato recuperato nel periodo di osservazione.

Percentuale di storage recuperata

I grafici della console Amazon S3 mostrano anche la percentuale di storage dei dati filtrati che è stata recuperata nel periodo di osservazione.

Come indicato più in alto in questo argomento, durante l'analisi degli oggetti ad accesso infrequente, l'analisi della classe di storage prende in considerazione un insieme filtrato di oggetti raggruppati in base al tempo trascorso dal loro caricamento su Amazon S3. L'analisi della classe di storage utilizza questi gruppi predefiniti di età degli oggetti:

- Oggetti Amazon S3 con meno di 15 giorni
- Oggetti Amazon S3 con 15-29 giorni
- Oggetti Amazon S3 con 30-44 giorni
- Oggetti Amazon S3 con 45-59 giorni
- Oggetti Amazon S3 con 60-74 giorni
- Oggetti Amazon S3 con 75-89 giorni
- Oggetti Amazon S3 con 90-119 giorni
- Oggetti Amazon S3 con 120-149 giorni

- Oggetti Amazon S3 con 150-179 giorni
- Oggetti Amazon S3 con 180-364 giorni
- Oggetti Amazon S3 con 365-729 giorni
- Oggetti Amazon S3 con almeno 730 giorni

In genere servono circa 30 giorni di osservazione degli schemi di accesso per raccogliere informazioni sufficienti a generare un risultato dell'analisi. Potrebbero anche essere necessari più di 30 giorni, a seconda dei singoli schemi di accesso ai dati. Tuttavia, dopo aver configurato un filtro, entro 24 o 48 ore nella console Amazon S3 inizierà a essere disponibile l'analisi dei dati basata sul filtro. Nella console Amazon S3 è possibile visualizzare l'analisi giornaliera dell'accesso agli oggetti suddivisa per gruppo di età degli oggetti.

Volume di storage ad accesso infrequente

La console Amazon S3 mostra i modelli di accesso raggruppati in base ai gruppi di età degli oggetti predefiniti. Il testo visualizzato Frequently accessed (Accesso frequente) o Infrequently accessed (Accesso poco frequente) è inteso come un aiuto visivo per aiutarti nel processo di creazione del ciclo di vita.

Come esportare i dati relativi all'analisi della classe di storage

Si può scegliere di far esportare i report dell'analisi della classe di storage in un file flat in formato CSV. I report sono aggiornati quotidianamente e si basano sui filtri configurati per i gruppi di età degli oggetti. Utilizzando la console Amazon S3, al momento di creare un filtro si può scegliere l'opzione di esportazione del report. Al momento della selezione dei dati da esportare, si specifica un bucket di destinazione e un prefisso di destinazione (facoltativo) dove scrivere il file. I dati possono essere esportati in un bucket di destinazione in un account diverso, ma il bucket di destinazione deve trovarsi nella stessa regione del bucket configurato per l'analisi.

È necessario creare una bucket policy sul bucket di destinazione per concedere le autorizzazioni ad Amazon S3 per verificare a chi Account AWS appartiene il bucket e scrivere oggetti nel bucket nella posizione definita. Per un esempio di policy, consulta [Concedere autorizzazioni per S3 Inventory e S3 Analytics](#).

Una volta configurati, i report dell'analisi della classe di storage esportati iniziano a essere disponibili dopo 24 ore. Successivamente Amazon S3 continua a monitorare e generare esportazioni quotidiane.

Puoi aprire il file CSV in un'applicazione per fogli di calcolo o importare il file in altre applicazioni come Amazon Quick. <https://docs.aws.amazon.com/quicksight/latest/user/welcome.html> Per informazioni sull'utilizzo di oggetti Amazon S3 con Amazon Quick, consulta la [Amazon Quick User Guide](#).

Nel file esportato, i dati sono ordinati per data nell'ambito del gruppo di età degli oggetti, come nell'esempio seguente. Se la classe di storage è STANDARD, la riga contiene anche i dati per le colonne `ObjectAgeForSIATransition` e `RecommendedObjectAgeForSIATransition`.

Date	ConfigId	Filter	StorageClass	ObjectAge	ObjectCount	DataUploaded_MB	Storage_MB	DataRetrieved_MB	GetRequestCount	CumulativeAccessRatio	ObjectAgeForSIATransition	RecommendedObjectAgeForSIATransition
8/17/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/2/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/22/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
8/25/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/6/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/30/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/28/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/21/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/5/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		

Alla fine del report, il gruppo di età degli oggetti restituito è ALL (Tutti). Le righe ALL contengono i totali cumulativi, inclusi gli oggetti inferiori a 128 KB, per tutti i gruppi di età per quel dato giorno.

8/24/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0 000-014		
9/3/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.02426125 015-029		
8/28/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.03545875 015-029		
8/17/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0 000-014		
8/25/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0 000-014		
9/6/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.0209529 015-029		
9/4/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.02304819 015-029		
8/22/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0 000-014		
8/21/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0 000-014		
8/30/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.03073092 015-029		
8/20/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0 000-014		

La sezione successiva descrive le colonne utilizzate nel report.

Layout del file esportato

La tabella seguente descrive il layout del file di esportazione dall'analisi della classe di storage Amazon S3.

Configurazione dell'analisi della classe di storage

Lo strumento per l'analisi della classe di storage Amazon S3 consente di analizzare gli schemi di accesso allo storage per stabilire quando eseguire la transizione dei dati verso l'opportuna classe di storage. Osservando gli schemi di accesso ai dati, l'analisi della classe di storage aiuta a determinare quando è opportuno spostare i dati meno utilizzati dallo storage STANDARD alla classe di storage STANDARD_IA (ad accesso infrequente). Per maggiori informazioni su STANDARD_IA, consulta le [domande frequenti su Amazon S3](#) e [Comprensione e gestione delle classi di storage Amazon S3](#).

È possibile impostare l'analisi della classe di storage configurando i dati degli oggetti da analizzare. A seconda della configurazione, l'analisi della classe di storage può:

- Analizzare l'intero contenuto di un bucket.

Verrà generata un'analisi per tutti gli oggetti del bucket.

- Analizzare gli oggetti raggruppati in base al prefisso e ai tag.

Si possono configurare filtri che raggruppano gli oggetti per l'analisi in base a un prefisso, ai tag dell'oggetto o a una combinazione di entrambe le opzioni. Viene generata un'analisi separata per ogni filtro configurato. È possibile definire più configurazioni di filtri per ciascun bucket (fino a 1.000).

- Esportare i dati dell'analisi.

Quando si configura l'analisi della classe di storage per un bucket o un filtro, si può scegliere di far esportare ogni giorno i relativi dati in un file. L'analisi del giorno corrente viene aggiunta al file per formare un registro storico dell'analisi per il filtro configurato. Il file viene aggiornato quotidianamente nella destinazione selezionata. Al momento della selezione dei dati da esportare, si specifica un bucket di destinazione e un prefisso di destinazione (facoltativo) dove scrivere il file.

Puoi utilizzare la console Amazon S3, l'API REST o gli AWS SDK AWS CLI o per configurare l'analisi delle classi di storage.

Important

L'analisi della classe di archiviazione non fornisce suggerimenti sulla transizione alle classi di archiviazione ONEZONE_IA o S3 Glacier Flexible Retrieval.

Se desideri configurare l'analisi delle classi di storage per esportare i risultati come file .csv e il bucket di destinazione utilizza la crittografia del bucket predefinita con a AWS KMS key, devi aggiornare la policy AWS KMS chiave per concedere ad Amazon S3 l'autorizzazione a crittografare il file .csv. Per istruzioni, consulta [Concessione ad Amazon S3 dell'autorizzazione per l'utilizzo della chiave gestita dal cliente per la crittografia](#).

Per ulteriori informazioni sull'analisi, consulta [Analisi di Amazon S3 – Analisi della classe di storage](#).

Utilizzo della console S3

Per configurare l'analisi della classe di storage

1. Accedi e apri la console Amazon S3 all'indirizzo. Console di gestione AWS <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico o Bucket di directory.
3. Nell'elenco dei bucket seleziona il nome del bucket per cui desideri configurare l'analisi della classe di archiviazione.
4. Seleziona la scheda Parametri.
5. In Storage Class Analysis (Analisi classe storage), scegliere Create analytics configuration (Crea configurazione di analisi).
6. Digitare un nome per il filtro. Per analizzare l'intero bucket, lasciare vuoto il campo Prefix (Prefisso).
7. Nel campo Prefix (Prefisso), digitare il testo per il prefisso per gli oggetti che si desidera analizzare.
8. Per aggiungere un tag, scegli Add tag (Aggiungi tag). Digitare una Key (Chiave) e un Value (Valore) per il tag. È possibile immettere un prefisso e più tag.
9. Se si desidera, scegliere Enable (Abilita) in Export CSV (Esporta CSV) per esportare i report dell'analisi in un file flat in formato .csv. Scegliere un bucket di destinazione per archiviare il file. È anche possibile scegliere un prefisso per il bucket di destinazione. Il bucket di destinazione deve trovarsi nello Regione AWS stesso bucket per il quale stai configurando l'analisi. Il bucket di destinazione può trovarsi in un diverso Account AWS.

Se il bucket di destinazione per il file .csv utilizza la crittografia del bucket predefinita con una chiave KMS, devi aggiornare la policy delle chiavi per concedere ad Amazon S3 l'AWS KMS autorizzazione a crittografare il file .csv. Per istruzioni, consulta [Concessione ad Amazon S3 dell'autorizzazione per l'utilizzo della chiave gestita dal cliente per la crittografia](#).

10. Scegliere Create configuration (Crea configurazione).

Amazon S3 crea una policy nel bucket di destinazione che concede ad Amazon S3 l'autorizzazione di scrittura. Questo consentirà di scrivere i dati dell'esportazione nel bucket.

Se si verifica un errore quando si tenta di creare la policy di bucket, vengono fornite le istruzioni per correggerlo. Ad esempio, se hai scelto un bucket di destinazione in un altro Account AWS e non disponi delle autorizzazioni di lettura e scrittura per la policy di bucket, verrà visualizzato il messaggio

riportato di seguito. Il proprietario del bucket di destinazione deve aggiungere a quest'ultimo la policy di bucket. Se la policy non viene aggiunta al bucket di destinazione, i dati non verranno esportati in quanto Amazon S3 non dispone dell'autorizzazione di scrittura su tale bucket. Se il bucket di origine è di proprietà di un account diverso da quello dell'utente attuale, l'ID account corretto del bucket di origine verrà sostituito nella policy.

Per informazioni sui dati esportati e sul funzionamento del filtro, consulta [Analisi di Amazon S3 – Analisi della classe di storage](#).

Utilizzo della REST API

Per configurare Storage Class Analysis utilizzando l'API REST, utilizza.

[PutBucketAnalyticsConfiguration](#) Puoi anche utilizzare l'operazione equivalente con AWS CLI o AWS SDK.

È possibile utilizzare le seguenti API REST per lavorare con l'analisi della classe di storage:

- [Configurazione di DELETE Bucket Analytics](#)
- [Configurazione di GET Bucket Analytics](#)
- [List Bucket Analytics Configuration](#)

Gestione dei costi di storage con il Piano intelligente Amazon S3

La classe di archiviazione S3 Intelligent-Tiering è progettata per ottimizzare i costi di archiviazione spostando automaticamente i dati al livello di accesso più conveniente quando i modelli di accesso subiscono cambiamenti, senza impatto sulle prestazioni o sovraccarico operativo. Per un monitoraggio degli oggetti mensile e una tariffa di automazione bassi, S3 Intelligent-Tiering monitora i modelli di accesso e sposta automaticamente gli oggetti ai quali non è stato eseguito l'accesso a livelli di accesso a costo più basso.

S3 Intelligent-Tiering offre risparmi automatici sui costi di archiviazione in tre livelli di accesso a bassa latenza ed elevata velocità effettiva. Per i dati a cui è possibile accedere in modo asincrono, puoi scegliere di attivare le funzionalità di archiviazione automatica all'interno della classe di archiviazione S3 Intelligent-Tiering. Non sono previste spese di recupero in S3 Intelligent-Tiering. Se si accede in seguito a un oggetto nel livello Accesso Infrequente o Accesso Istantaneo all'Archivio, l'oggetto verrà automaticamente spostato nel livello Accesso Frequente. Lo spostamento di oggetti tra i livelli di accesso all'interno della classe di archiviazione S3 Intelligent-Tiering non comporta l'applicazione di costi di livello.

S3 Intelligent-Tiering è la classe di archiviazione consigliata per i dati con modelli di accesso sconosciuti, in mutamento o imprevedibili, indipendentemente dalla dimensione dell'oggetto o dal periodo di conservazione, come data lake, analisi dei dati e nuove applicazioni.

La classe di archiviazione S3 Intelligent-Tiering supporta tutte le funzionalità di Amazon S3, tra cui:

- S3 Inventory, per verificare il livello di accesso degli oggetti
- Replica S3, per la replica di dati in qualsiasi Regione AWS
- S3 Storage Lens, per visualizzare i parametri di utilizzo e attività dell'archiviazione
- Crittografia lato server, per la protezione dei dati degli oggetti
- S3 Object Lock, per prevenire l'eliminazione accidentale
- AWS PrivateLink, per accedere ad Amazon S3 tramite un endpoint privato in un cloud privato virtuale (VPC)

Per informazioni sull'utilizzo di S3 Intelligent-Tiering, consulta le sezioni seguenti:

Argomenti

- [Come funziona S3 Intelligent-Tiering](#)
- [Usare S3 Intelligent-Tiering](#)
- [Gestione di S3 Intelligent-Tiering](#)

Come funziona S3 Intelligent-Tiering

La classe di archiviazione Amazon S3 Intelligent-Tiering memorizza automaticamente gli oggetti in tre livelli di accesso. Un livello è ottimizzato per l'accesso frequente, un livello a basso costo è ottimizzato per l'accesso infrequente e un altro livello a costi minimi è ottimizzato per i dati a cui si accede raramente. Per una ridotta tariffa mensile per l'automazione e il monitoraggio degli oggetti, S3 Intelligent-Tiering monitora i modelli di accesso e sposta automaticamente gli oggetti a cui non è stato eseguito l'accesso per 30 giorni consecutivi al livello Accesso infrequente. Dopo 90 giorni senza che sia stato eseguito l'accesso, gli oggetti vengono spostati nel livello Archive Instant Access senza impatto sulle prestazioni o sovraccarico operativo.

Per ottenere il minor costo di archiviazione sui dati a cui è possibile accedere in pochi minuti o ore, attiva funzionalità di archiviazione per avere due livelli aggiuntivi. È possibile spostare gli oggetti al livello Archive Access (Accesso archiviazione), al livello Deep Archive Access (Accesso archiviazione profonda) o a entrambi. Con il livello Archive Access (Accesso archiviazione), la

classe di archiviazione S3 Intelligent-Tiering (Piano intelligente S3) sposta gli oggetti a cui non è stato eseguito l'accesso per un minimo di 90 giorni consecutivi al livello Archive Access (Accesso archiviazione). Con il livello Deep Archive Access (Accesso archiviazione profonda), la classe di archiviazione S3 Intelligent-Tiering (Piano intelligente S3) sposta gli oggetti al livello Deep Archive Access (Accesso archiviazione profonda) dopo un minimo di 180 giorni consecutivi senza accesso. Per entrambi i livelli, puoi configurare il numero di giorni senza accesso in base alle tue esigenze.

Le seguenti azioni costituiscono un accesso che impedisce la suddivisione degli oggetti al livello Archive Access o al livello Deep Archive Access:

- Scarica o copia un oggetto archiviato tramite la console di Amazon S3.
- Richiamare [CopyObject](#), [UploadPartCopy](#) o replicare oggetti con S3 Batch Replication. In questi casi, gli oggetti di origine delle operazioni di copia o replica sono suddivisi su più livelli.
- Invocare [GetObject](#), [PutObject](#), [RestoreObject](#), [CompleteMultipartUpload](#) o [SelectObjectContent](#).

Ad esempio, se si accede agli oggetti tramite `SelectObjectContent` prima del numero di giorni di inattività specificato (ad esempio 180 giorni), tale azione ripristina il timer. I tuoi oggetti non passeranno al livello Archive Access o al livello Deep Archive Access fino al raggiungimento del numero di giorni specificato dopo l'ultima richiesta `SelectObjectContent`.

Se si accede in seguito a un oggetto nel livello Accesso Infrequente o Archive Instant Access, l'oggetto verrà automaticamente spostato nel livello Accesso Frequente.

Le seguenti azioni costituiscono l'accesso che automaticamente sposta gli oggetti dal livello Infrequent Access al livello Archive Instant Access e poi di nuovo al livello Frequent Access:

- Scarica o copia un oggetto tramite la console di Amazon S3.
- Invocare [CopyObject](#), [UploadPartCopy](#) o replicare oggetti con Batch Replication. In questi casi, gli oggetti di origine delle operazioni di copia o replica sono suddivisi su più livelli.
- Invocare [GetObject](#), [PutObject](#), [RestoreObject](#) o [CompleteMultipartUpload](#).

Le altre azioni non costituiscono un accesso che automaticamente muove gli oggetti dal livello Infrequent Access o Archive Instant Access di nuovo al livello Frequent Access. Di seguito è riportato un esempio, non un elenco definitivo, di tali azioni:

- Invocando [HeadObject](#), [GetObjectTagging](#), [PutObjectTagging](#), [ListObjects](#), [ListObjectsV2](#), [ListObjectVersions](#), e [UpdateObjectEncryption](#).

- L'invocazione di [SelectObjectContent](#) non costituisce un accesso che classifica gli oggetti fino a un livello di accesso frequente. Inoltre, non impedisce la suddivisione degli oggetti dal livello Frequent Access al livello Infrequent Access e quindi al livello Archive Instant Access.

È possibile utilizzare S3 Intelligent-Tiering come classe di archiviazione predefinita per i dati appena creati specificando INTELLIGENT-TIERING nell'[intestazione della richiesta x-amz-storage-class](#) quando si richiamano le operazioni PutObject, CopyObject o CreateMultipartUpload. S3 Intelligent-Tiering è progettato per una disponibilità del 99,9% e una durata del 99,999999999%.

Note

Se le dimensioni di un oggetto sono inferiori a 128 KB, questo non è monitorato e il tiering automatico non sarà consentito. Gli oggetti più piccoli vengono sempre archiviati nel livello Accesso frequente.

Livelli di accesso S3 Intelligent-Tiering

Di seguito vengono illustrati i diversi livelli di accesso automatici e facoltativi. Quando gli oggetti vengono spostati tra i livelli di accesso, la classe di archiviazione rimane la stessa (S3 Intelligent-Tiering).

Livello Accesso frequente (automatico)

Questo è il livello di accesso predefinito in cui qualsiasi oggetto creato o trasferito in S3 Intelligent-Tiering inizia il suo ciclo di vita. Un oggetto rimane in questo livello finché viene eseguito l'accesso ad esso. Il livello Frequent Access offre bassa latenza ed elevata velocità di trasmissione effettiva.

Livello Accesso infrequente (automatico)

Se non si accede a un oggetto per 30 giorni consecutivi, l'oggetto passa al livello Accesso infrequente. Il livello Infrequent Access offre bassa latenza ed elevate prestazioni di velocità di trasmissione effettiva.

Livello Archive Instant Access (automatico)

Se non si accede a un oggetto per 90 giorni consecutivi, l'oggetto passa al livello Archive Instant Access. Il livello Archive Instant Access offre bassa latenza ed elevate prestazioni di velocità di trasmissione effettiva.

Livello Accesso di archiviazione (facoltativo)

S3 Intelligent-Tiering offre la possibilità di attivare il livello Archive Access per i dati a cui è possibile accedere in modo asincrono. Dopo l'attivazione, il livello Archive Access archivia automaticamente gli oggetti a cui non è stato eseguito l'accesso per un minimo di 90 giorni consecutivi. Puoi estendere il momento dell'ultimo accesso per l'archiviazione a un massimo di 730 giorni. Il livello Archive Access ha le stesse prestazioni della classe di archiviazione [S3 Glacier Flexible Retrieval](#).

I tempi di recupero standard per questo livello di accesso possono variare dalle 3 alle 5 ore. Se avvii la richiesta di ripristino utilizzando le Operazioni in batch S3, il ripristino inizia in pochi minuti. Per ulteriori informazioni sulle opzioni e gli orari di recupero, consulta [the section called “Ripristino di oggetti dai livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access”](#).

Note

Attivare il livello Archive Access per 90 giorni solo se si desidera ignorare il livello Archive Instant Access. Il livello Archive Access offre costi di storage leggermente inferiori, con tempi di minute-to-hour recupero. Il livello Archive Instant Access (Archiviazione con accesso istantaneo) offre un accesso in millisecondi e prestazioni a elevata velocità di trasmissione effettiva.

Livello Accesso di archiviazione profonda (opzionale)

S3 Intelligent-Tiering offre la possibilità di attivare il livello Deep Archive Access per i dati a cui è possibile accedere in modo asincrono. Dopo l'attivazione, il livello Deep Archive Access archivia automaticamente gli oggetti a cui non è stato eseguito l'accesso per un minimo di 180 giorni consecutivi. Puoi estendere il momento dell'ultimo accesso per l'archiviazione a un massimo di 730 giorni. Il livello Accesso di archiviazione profonda ha le stesse prestazioni della classe di archiviazione [S3 Glacier Deep Archive](#).

Il recupero standard degli oggetti in questo livello di accesso avviene entro 12 ore. Se avvii la richiesta di ripristino utilizzando le Operazioni in batch S3, il ripristino inizia nell'arco di 9 ore. Per ulteriori informazioni sulle opzioni e gli orari di recupero, consulta [the section called “Ripristino di oggetti dai livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access”](#).

 Note

Attiva i livelli Accesso di archiviazione e Accesso di archiviazione profonda solo se l'applicazione può accedere agli oggetti in modo asincrono. Se l'oggetto recuperato è archiviato nei livelli Archive Access o Deep Archive Access, prima devi ripristinarlo utilizzando `RestoreObject`.

È possibile ripristinare gli oggetti archiviati con un massimo di 1.000 transazioni al secondo (TPS) di richieste di ripristino degli oggetti per account per AWS regione da S3 Intelligent-Tiering Archive Access e S3 Intelligent-Tiering Deep Archive Access.

Usare S3 Intelligent-Tiering

È possibile utilizzare la classe di Intelligent-Tiering storage S3 per ottimizzare automaticamente i costi di archiviazione. S3 Intelligent-Tiering offre risparmi automatici sui costi spostando i dati a livello di oggetto granulare tra i livelli di accesso quando i modelli di accesso cambiano. Per i dati a cui è possibile accedere in modo asincrono, puoi scegliere di abilitare l'archiviazione automatica all'interno della classe di Intelligent-Tiering storage S3 utilizzando l'API, o Amazon S3. Console di gestione AWS AWS CLI

Spostamento dei dati su S3 Intelligent-Tiering

Esistono due modi per spostare i dati in Intelligent-Tiering S3. È possibile caricare oggetti direttamente in S3 Intelligent-Tiering dalla console o a livello di codice utilizzando un'operazione. PUT Per ulteriori informazioni, consulta [Impostazione della classe di storage di un oggetto](#). Puoi anche configurare le configurazioni del ciclo di vita di S3 per trasferire gli oggetti da S3 Standard o S3 Access a S3. Standard-Infrequent Intelligent-Tiering

Caricamento dei dati su S3 utilizzando Direct PUT Intelligent-Tiering

Quando si carica un oggetto nella classe di Intelligent-Tiering archiviazione S3 utilizzando l'operazione [API PUT](#), si specifica S3 Intelligent-Tiering nell'intestazione della richiesta. [x-amz-storage-class](#)

La seguente richiesta archivia l'immagine, `my-image.jpg`, nel bucket `myBucket`. La richiesta utilizza l'`x-amz-storage-class` intestazione per richiedere che l'oggetto venga archiviato utilizzando la classe di archiviazione S3. Intelligent-Tiering

Example

```
PUT /my-image.jpg HTTP/1.1
Host: myBucket.s3.<Region>.amazonaws.com (http://amazonaws.com/)
Date: Wed, 1 Sep 2021 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

Transizione dei dati a S3 Intelligent-Tiering da S3 Standard o S3 Access utilizzando S3 Lifecycle Standard-Infrequent

Puoi aggiungere regole a una configurazione del ciclo di vita S3 per indicare ad Amazon S3 di trasferire gli oggetti da una classe di archiviazione a un'altra. Per informazioni sulle transizioni supportate e sui vincoli correlati, consulta [Trasferimento degli oggetti utilizzando il ciclo di vita S3](#).

Puoi specificare le configurazioni del ciclo di vita S3 a livello di bucket o di prefisso. In questa regola di configurazione del ciclo di vita S3, il filtro specifica un prefisso della chiave (documents/). Pertanto la regola si applica agli oggetti con il prefisso del nome della chiave documents/, ad esempio documents/doc1.txt e documents/doc2.txt. La regola specifica un'Transitionazione che indirizza Amazon S3 a trasferire gli oggetti alla classe di storage S3 0 giorni dopo la creazione. Intelligent-Tiering In questo caso, gli oggetti sono idonei per la transizione a S3 alla mezzanotte UTC successiva Intelligent-Tiering alla creazione.

Example

```
<LifecycleConfiguration>
  <Rule>
    <ID>ExampleRule</ID>
    <Filter>
      <Prefix>documents/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>INTELLIGENT_TIERING</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Un bucket che supporta la funzione Controllo delle versioni mantiene una versione dell'oggetto corrente e zero o più versioni dell'oggetto non correnti. È possibile definire regole del ciclo di vita separate per le versioni dell'oggetto correnti e non correnti.

Per ulteriori informazioni, consulta [Elementi della configurazione del ciclo di vita](#).

Abilitazione dei livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access

Per ottenere il costo di storage più basso sui dati a cui è possibile accedere in pochi minuti o ore, puoi attivare uno o entrambi i livelli di accesso all'archivio creando una configurazione a livello di bucket, prefisso o tag di oggetto utilizzando l'API Console di gestione AWS AWS CLI, o Amazon S3.

Utilizzo della console S3

Per abilitare l'archiviazione automatica di S3 Intelligent-Tiering

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket scegli il nome del bucket desiderato.
3. Scegli Properties (Proprietà).
4. Vai alla sezione delle configurazioni dell' Intelligent-Tiering archivio S3 e scegli Crea configurazione.
5. Nella sezione Impostazioni di configurazione dell'archivio, specifica un nome di configurazione descrittivo per la tua configurazione di S3 Archive. Intelligent-Tiering
6. In Choose a configuration scope (Scegli un ambito di configurazione), scegli l'ambito di configurazione da utilizzare. Facoltativamente, puoi limitare l'ambito di configurazione agli oggetti specificati all'interno di un bucket utilizzando un prefisso condiviso, un tag oggetto o una combinazione dei due.
 - a. Per limitare l'ambito della configurazione, seleziona Limit the scope of this configuration using one or more filters (Limita l'ambito di questa configurazione utilizzando uno o più filtri).
 - b. Per limitare l'ambito della configurazione utilizzando un singolo prefisso, inserisci il prefisso in Prefisso.
 - c. Per limitare l'ambito della configurazione utilizzando i tag oggetto, seleziona Add tag (Aggiungi tag) e inserisci un valore per la chiave.
7. In Status (Stato), seleziona Enable (Abilita).
8. Nella sezione Archive settings (Impostazioni archivio), seleziona uno o entrambi i livelli Accesso di archiviazione per abilitarli.

9. Scegli Crea.

Utilizzo di AWS CLI

È possibile utilizzare AWS CLI i seguenti comandi per gestire le configurazioni S3: Intelligent-Tiering

- [delete-bucket-intelligent-tiering-configuration](#)
- [get-bucket-intelligent-tiering-configuration](#)
- [list-bucket-intelligent-tiering-configurations](#)
- [put-bucket-intelligent-tiering-configuration](#)

Per istruzioni sulla configurazione di AWS CLI, consulta [Developing with Amazon S3 using the AWS CLI](#) nell'Amazon S3 API Reference.

Quando si utilizza il AWS CLI, non è possibile specificare la configurazione come file XML. È necessario specificare invece il JSON. Di seguito è riportato un esempio di Intelligent-Tiering configurazione XML S3 e JSON equivalente che è possibile specificare in un AWS CLI comando.

L'esempio seguente inserisce una Intelligent-Tiering configurazione S3 nel bucket specificato.

Example [put-bucket-intelligent-tiering-configuration](#)

JSON

```
{
  "Id": "string",
  "Filter": {
    "Prefix": "string",
    "Tag": {
      "Key": "string",
      "Value": "string"
    },
  },
  "And": {
    "Prefix": "string",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  },
  ...
}
```

```

    ]
  }
},
"Status": "Enabled"|"Disabled",
"Tierings": [
  {
    "Days": integer,
    "AccessTier": "ARCHIVE_ACCESS"|"DEEP_ARCHIVE_ACCESS"
  }
  ...
]
}

```

XML

```

PUT /?intelligent-tiering&id=Id HTTP/1.1
Host: Bucket.s3.amazonaws.com
<?xml version="1.0" encoding="UTF-8"?>
<IntelligentTieringConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Id>string</Id>
  <Filter>
    <And>
      <Prefix>string</Prefix>
      <Tag>
        <Key>string</Key>
        <Value>string</Value>
      </Tag>
      ...
    </And>
    <Prefix>string</Prefix>
    <Tag>
      <Key>string</Key>
      <Value>string</Value>
    </Tag>
  </Filter>
  <Status>string</Status>
  <Tiering>
    <AccessTier>string</AccessTier>
    <Days>integer</Days>
  </Tiering>
  ...
</IntelligentTieringConfiguration>

```

Utilizzo dell'operazione API PUT

È possibile utilizzare l'[PutBucketIntelligentTieringConfiguration](#) operazione per un bucket specificato e fino a 1.000 configurazioni S3 per bucket. Intelligent-Tiering Puoi definire quali oggetti all'interno di un bucket sono idonei per i livelli di accesso di archiviazione utilizzando un prefisso condiviso o un tag oggetto. Usare un prefisso condiviso o un tag oggetto permette l'allineamento a determinate applicazioni aziendali, flussi di lavoro, o organizzazioni interne. Hai inoltre la flessibilità necessaria per attivare il livello Accesso di archiviazione, il livello Accesso di archiviazione profonda o entrambi.

Gestione di S3 Intelligent-Tiering

La classe di Intelligent-Tiering storage S3 offre risparmi automatici sui costi di storage in tre livelli di accesso a bassa latenza e alta produttività. Inoltre offre funzionalità di archiviazione opzionali che permettono di ottenere costi di archiviazione più bassi nel cloud per i dati accessibili nel giro di minuti o ore.

Identificazione in quali oggetti del livello di accesso S3 sono archiviati Intelligent-Tiering

Per ottenere un elenco dei tuoi oggetti e dei metadati corrispondenti, incluso il livello di Intelligent-Tiering accesso S3, puoi utilizzare [Amazon S3 Inventory](#). Inventario S3 fornisce CSV, ORC o file di output Parquet che elencano gli oggetti e i metadati corrispondenti. Puoi ricevere questi report di inventario su base giornaliera o settimanale per un bucket Amazon S3 o un prefisso condiviso. (Prefisso condiviso si riferisce agli oggetti con nomi che iniziano con una stringa comune.)

Visualizzazione dello stato di archiviazione di un oggetto all'interno di S3 Intelligent-Tiering

Per ricevere una notifica quando un oggetto all'interno della classe di Intelligent-Tiering storage S3 viene spostato al livello Archive Access o al livello Deep Archive Access, puoi configurare S3 Event Notifications. Per ulteriori informazioni, consulta [Abilitare le notifiche eventi](#).

Amazon S3 può pubblicare notifiche di eventi in un argomento Amazon Simple Notification Service (Amazon SNS), una coda Amazon Simple Queue Service (Amazon SQS) o una funzione AWS Lambda . Per ulteriori informazioni, consulta [Notifiche di eventi Amazon S3](#).

Quello che segue è un esempio di un messaggio inviato da Amazon S3 per pubblicare un evento s3: IntelligentTiering. Per ulteriori informazioni, consulta [the section called “Struttura del messaggio di evento”](#).

```
{
```

```

"Records":[
  {
    "eventVersion":"2.3",
    "eventSource":"aws:s3",
    "awsRegion":"us-west-2",
    "eventTime":"1970-01-01T00:00:00.000Z",
    "eventName":"IntelligentTiering",
    "userIdentity":{
      "principalId":"s3.amazonaws.com"
    },
    "requestParameters":{
      "sourceIPAddress":"s3.amazonaws.com"
    },
    "responseElements":{
      "x-amz-request-id":"C3D13FE58DE4C810",
      "x-amz-id-2":"FMMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvAN0jpD"
    },
    "s3":{
      "s3SchemaVersion":"1.0",
      "configurationId":"testConfigRule",
      "bucket":{
        "name":"amzn-s3-demo-bucket",
        "ownerIdentity":{
          "principalId":"A3NL1K0ZZKExample"
        },
        "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
      },
      "object":{
        "key":"HappyFace.jpg",
        "size":1024,
        "eTag":"d41d8cd98f00b204e9800998ecf8427e",
      }
    },
    "intelligentTieringEventData":{
      "destinationAccessTier": "ARCHIVE_ACCESS"
    }
  }
]
}

```

Puoi utilizzare anche una [richiesta di oggetto HEAD](#) per visualizzare lo stato di archiviazione di un oggetto. Se un oggetto è archiviato nella classe di Intelligent-Tiering storage S3 e si trova in uno

dei livelli di archivio, la risposta dell'HEAD oggetto mostra il livello di archivio corrente. Per mostrare il livello di archiviazione, la richiesta utilizza l'intestazione [x-amz-archive-status](#).

La seguente richiesta di oggetto HEAD restituisce i metadati di un oggetto (in questo caso, *my-image.jpg*).

Example

```
HEAD /my-image.jpg HTTP/1.1
Host: bucket.s3.region.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:02236Q3V0RonhpaBX5sCYVf1bNRuU=
```

Le richieste di oggetto HEAD possono essere utilizzate anche per monitorare lo stato di una richiesta `restore-object`. Se il ripristino dell'archivio è in corso, la richiesta di oggetto HEAD include l'intestazione [x-amz-restore](#).

La seguente risposta all'HEAD oggetto di esempio mostra un oggetto archiviato utilizzando S3 Intelligent-Tiering con una richiesta di ripristino in corso.

Example

```
HTTP/1.1 200 OK
x-amz-id-2: FSVaTMjrmBp3Izs1NnwBZeu7M19iI8UbxMbi0A8AirHANJBo+hEftBuiESACOMJp
x-amz-request-id: E5CEFCB143EB505A
Date: Fri, 13 Nov 2020 00:28:38 GMT
Last-Modified: Mon, 15 Oct 2012 21:58:07 GMT
ETag: "1accb31fcf202eba0c0f41fa2f09b4d7"
x-amz-storage-class: 'INTELLIGENT_TIERING'
x-amz-archive-status: 'ARCHIVE_ACCESS'
x-amz-restore: 'ongoing-request="true"'
x-amz-restore-request-date: 'Fri, 13 Nov 2020 00:20:00 GMT'
Accept-Ranges: bytes
Content-Type: binary/octet-stream
Content-Length: 300
Server: AmazonS3
```

Ripristino di oggetti dai livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access

Per accedere agli oggetti nei livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access, è necessario avviare una richiesta [di](#) ripristino e quindi attendere che l'oggetto venga spostato nel

livello Frequent Access. Per ulteriori informazioni sull'archiviazione degli oggetti, consulta [the section called “Utilizzo di oggetti archiviati”](#).

Quando esegui il ripristino dai livelli Accesso di archiviazione o di archiviazione profonda, l'oggetto passa nuovamente al livello Accesso frequente. In seguito, se non accedi all'oggetto per 30 giorni consecutivi, l'oggetto verrà spostato automaticamente nel livello Accesso infrequente. Dopodiché, dopo un minimo di 90 giorni consecutivi senza accesso, l'oggetto passa al livello Accesso archivio. Dopo un minimo di 180 giorni consecutivi senza accesso, l'oggetto passa al livello Accesso archivio approfondito. Per ulteriori informazioni, consulta [the section called “Come funziona S3 Intelligent-Tiering”](#).

Puoi ripristinare un oggetto archiviato utilizzando la console Amazon S3, S3 Batch Operations, l'API REST di Amazon S3, gli SDK o (). AWS AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta [the section called “Utilizzo di oggetti archiviati”](#).

Informazioni sulle classi di storage S3 Glacier per l'archiviazione di dati a lungo termine

È possibile utilizzare le classi di storage S3 Glacier di Amazon S3 per fornire soluzioni convenienti per l'archiviazione di dati a lungo termine a cui non si accede spesso. Le classi di storage S3 Glacier sono:

- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive

Scegli una di queste classi di storage in base alla frequenza con cui accedi ai dati e alla velocità con cui è necessario recuperarli. Ognuna di queste classi di storage offre la stessa durabilità e resilienza della classe di storage S3 Standard, ma a costi di storage inferiori. [Per ulteriori informazioni sulle classi di storage S3 Glacier, consulta storage-classes/glacier/. https://aws.amazon.com/s3/](#)

Argomenti

- [Confronto delle classi di storage S3 Glacier](#)
- [S3 Glacier Instant Retrieval](#)
- [S3 Glacier Flexible Retrieval](#)
- [S3 Glacier Deep Archive](#)
- [Informazioni sullo storage di archiviazione in S3 Glacier Flex Retrieval e S3 Glacier Deep Archive](#)

- [In che modo queste classi di archiviazione differiscono dal servizio Amazon Glacier](#)

Confronto delle classi di storage S3 Glacier

Ogni classe di storage S3 Glacier ha una durata di storage minima per tutti gli oggetti. Se l'utente elimina, sovrascrive o trasferisce l'oggetto a un'altra classe di storage prima del termine minimo, gli verrà addebitato il costo della durata residua.

Alcune classi di storage S3 Glacier sono di tipo archiviazione, il che significa che gli oggetti archiviati in tali classi vengono archiviati e non sono disponibili per l'accesso in tempo reale. Per ulteriori informazioni, consulta [Informazioni sullo storage di archiviazione in S3 Glacier Flex Retrieval e S3 Glacier Deep Archive](#).

Le classi di storage progettate per modelli di accesso meno frequenti con tempi di recupero più lunghi offrono costi di storage inferiori. Per informazioni sui prezzi, consulta <https://aws.amazon.com/s3/pricing/>.

La tabella seguente riassume i punti chiave da considerare quando si sceglie una classe di storage S3 Glacier:

S3 Glacier Instant Retrieval

Consigliamo di utilizzare Recupero istantaneo S3 Glacier per dati a lungo termine a cui si accede una volta al trimestre e che richiedono tempi di recupero di millisecondi. Questa classe di storage è ideale per casi d'uso sensibili alle prestazioni come l'hosting di immagini, le applicazioni di condivisione di file e l'archiviazione di cartelle cliniche per l'accesso durante gli appuntamenti.

La classe di storage Recupero istantaneo S3 Glacier offre accesso in tempo reale agli oggetti con le stesse prestazioni di latenza e throughput della classe di storage AI S3 Standard. Rispetto ad AI S3 Standard, Recupero istantaneo S3 Glacier ha costi di storage inferiori ma costi di accesso ai dati superiori.

La dimensione minima degli oggetti per i dati archiviati nella classe di storage Recupero istantaneo S3 Glacier è di 128 KB. Questa classe di storage ha inoltre un periodo di archiviazione minimo di 90 giorni.

S3 Glacier Flexible Retrieval

Consigliamo di utilizzare Recupero flessibile S3 Glacier per archiviare i dati a cui si accede una o due volte all'anno e che non richiedono un accesso immediato. Recupero flessibile S3 Glacier offre

tempi di recupero flessibili in modo da poter bilanciare i costi con tempi di accesso che vanno da pochi minuti ad alcune ore e recuperi Bulk gratuiti. Questa classe di storage è ideale per il backup e il disaster recovery.

Gli oggetti archiviati in Recupero flessibile S3 Glacier sono archiviati e non sono disponibili per l'accesso in tempo reale. Per ulteriori informazioni, consulta [Informazioni sullo storage di archiviazione in S3 Glacier Flex Retrieval e S3 Glacier Deep Archive](#). Per accedere a questi oggetti, è necessario innanzitutto avviare una richiesta di ripristino che crea una copia temporanea dell'oggetto a cui è possibile accedere al termine della richiesta. Per informazioni, consulta [Utilizzo di oggetti archiviati](#). Quando si ripristina un oggetto, è possibile scegliere un livello di recupero adatto al proprio caso d'uso, con costi inferiori per tempi di ripristino più lunghi.

Per Recupero flessibile S3 Glacier sono disponibili i seguenti livelli di recupero:

- Recupero expedited: in genere l'oggetto viene ripristinato in 1-5 minuti. I recuperi expedited sono soggetti alla domanda, pertanto per garantire tempi di ripristino affidabili e prevedibili, è consigliabile acquistare capacità di recupero con provisioning. Per ulteriori informazioni, consulta [Capacità con provisioning](#).
- Recupero Standard: in genere l'oggetto viene ripristinato in 3-5 ore o in un tempo compreso tra 1 minuto e 5 ore quando si utilizza Operazioni in batch S3. Per ulteriori informazioni, consulta [Ripristino di oggetti con operazioni in batch](#).
- Recupero Bulk: in genere l'oggetto viene ripristinato entro 5-12 ore. I recuperi Bulk sono gratuiti.

Per qualsiasi opzione di recupero, gli oggetti di dimensioni superiori a 5 TB vengono in genere completati entro 48 ore con una velocità di recupero fino a 300 megabyte al secondo (MBps). Per ulteriori informazioni, consulta [Informazioni sulle opzioni di recupero dall'archivio](#).

La durata minima dello storage per gli oggetti nella classe di storage Recupero flessibile S3 Glacier è di 90 giorni.

Recupero flessibile S3 Glacier richiede 40 KB di metadati aggiuntivi per ogni oggetto archiviato. Ciò include 32 KB di metadati necessari per identificare e recuperare i dati, addebitati alla tariffa predefinita per Recupero flessibile S3 Glacier. Sono necessari altri 8 KB di dati per mantenere il nome e i metadati definiti dall'utente per gli oggetti archiviati addebitati alla tariffa S3 Standard.

S3 Glacier Deep Archive

Si consiglia di utilizzare S3 Glacier Deep Archive per i dati di archivio a cui si accede meno di una volta all'anno. Questa classe di storage è progettata per conservare i set di dati per più anni per

soddisfare i requisiti di conformità e può essere utilizzata anche per il backup o il disaster recovery o per tutti i dati a cui si accede raramente e il cui recupero può richiedere fino a 72 ore. Deep Archive Amazon S3 Glacier è l'opzione di archiviazione più conveniente di AWS.

Gli oggetti archiviati in S3 Glacier Deep Archive sono archiviati e non sono disponibili per l'accesso in tempo reale. Per ulteriori informazioni, consulta [Informazioni sullo storage di archiviazione in S3 Glacier Flex Retrieval e S3 Glacier Deep Archive](#). Per accedere a questi oggetti, è necessario innanzitutto avviare una richiesta di ripristino che crea una copia temporanea dell'oggetto a cui è possibile accedere al termine della richiesta. Per informazioni, consulta [Utilizzo di oggetti archiviati](#). Quando si ripristina un oggetto, è possibile scegliere un livello di recupero adatto al proprio caso d'uso, con costi inferiori per tempi di ripristino più lunghi.

Per S3 Glacier Deep Archive sono disponibili i seguenti livelli di recupero:

- Recupero Standard: in genere l'oggetto viene ripristinato entro 12 ore o entro 9-12 ore se si utilizza Operazioni in batch S3. Per ulteriori informazioni, consulta [Ripristino di oggetti con operazioni in batch](#).
- Recupero Bulk: in genere ripristina l'oggetto entro 48 ore a una frazione del costo del livello di recupero Standard.

La durata minima dello storage per gli oggetti nella classe di storage S3 Glacier Deep Archive è di 180 giorni.

S3 Glacier Deep Archive richiede 40 KB di metadati aggiuntivi per ogni oggetto. Ciò include 32 KB di metadati necessari per identificare e recuperare i dati, addebitati alla tariffa predefinita per S3 Glacier Deep Archive. Sono necessari altri 8 KB di dati per mantenere il nome e i metadati definiti dall'utente per gli oggetti archiviati addebitati alla tariffa S3 Standard.

Informazioni sullo storage di archiviazione in S3 Glacier Flex Retrieval e S3 Glacier Deep Archive

S3 Glacier Flex Retrieval e S3 Glacier Deep Archive sono classi di storage di archiviazione. Ciò significa che quando si archivia un oggetto in queste classi di storage, tale oggetto viene archiviato e non è possibile accedervi direttamente. Per accedere a un oggetto archiviato, si invia una richiesta di ripristino dell'oggetto e si attende che il servizio ripristini l'oggetto. La richiesta di ripristino ripristina una copia temporanea dell'oggetto, che viene eliminata alla scadenza della durata specificata nella richiesta. Per ulteriori informazioni, consulta [Utilizzo di oggetti archiviati](#).

La transizione di oggetti nella classe di storage S3 Glacier Deep Archive è unidirezionale.

Se vuoi cambiare la classe di storage di un oggetto archiviato specificandone un'altra, devi prima di tutto usare l'operazione di ripristino per creare una copia temporanea dell'oggetto. Utilizzare quindi l'operazione di copia per sovrascrivere l'oggetto specificando S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval o Reduced Redundancy Storage come classe di archiviazione.

Note

L'operazione di copia per gli oggetti ripristinati non è supportata nella console Amazon S3 per oggetti nelle classi di storage Recupero flessibile Amazon S3 Glacier o S3 Glacier Deep Archive. Per questo tipo di operazione di copia, utilizzate l'API AWS Command Line Interface (AWS CLI), the o REST. AWS SDKs

È possibile ripristinare gli oggetti archiviati in queste classi di storage con un massimo di 1.000 transazioni al secondo (TPS) di [richieste di ripristino degli oggetti](#) per account e per Regione AWS.

Considerazioni sui costi

Se si intendono archiviare dati con accesso non frequente per un periodo di mesi o anni, le classi di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive consentono di ridurre i costi di archiviazione. Tuttavia, è consigliabile considerare quanto segue per assicurarsi che la classe di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive sia la scelta appropriata:

- Costi generali di storage: ogni oggetto archiviato richiede 40 KB di metadati aggiuntivi. Ciò include 32 KB di metadati necessari per identificare e recuperare i dati, addebitati alla tariffa predefinita per quella classe di storage. Sono necessari altri 8 KB di dati per mantenere il nome e i metadati definiti dall'utente per gli oggetti archiviati addebitati alla tariffa S3 Standard.

Per l'archiviazione di oggetti di piccole dimensioni, tenere presenti questi costi di storage. Per ridurre i costi aggiuntivi, si possono aggregare diversi oggetti di piccole dimensioni in un numero più contenuto di oggetti di grandi dimensioni.

- Prezzi per il caricamento in più parti: gli oggetti in S3- storage-class-glacier e S3 Glacier Deep Archive vengono fatturati alle tariffe delle classi di storage S3 Standard quando vengono caricati utilizzando caricamenti multipart. Per ulteriori informazioni, consulta [Caricamento in più parti e prezzi](#).
- Costi di storage minimi di 30 giorni: Recupero flessibile S3 Glacier e S3 Glacier Deep Archive sono soluzioni di archiviazione a lungo termine. Il periodo minimo di archiviazione è di 90 giorni per la

classe di archiviazione S3 Glacier Flexible Retrieval e 180 giorni per S3 Glacier Deep Archive. L'eliminazione dei dati archiviati in queste classi di storage è gratuita se gli oggetti eliminati sono archiviati per un tempo superiore al periodo di archiviazione minimo. Se si elimina o si sovrascrive un oggetto archiviato entro il periodo di durata minimo, Amazon S3 addebita i costi per il resto della durata.

- Costi per il recupero dei dati: quando si ripristinano oggetti archiviati in Recupero flessibile S3 Glacier e S3 Glacier Deep Archive, vengono addebitati costi per il recupero dei dati per richiesta. Questi costi variano in base al livello di recupero scelto quando si avvia un ripristino. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).
- Ciclo di vita S3: quando si ripristinano oggetti archiviati in Recupero flessibile S3 Glacier e S3 Glacier Deep Archive, vengono addebitati costi per il recupero dei dati per richiesta. Questi costi variano in base al livello di recupero scelto quando si avvia un ripristino. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Ripristino di oggetti archiviati

Gli oggetti archiviati non sono disponibili per l'accesso in tempo reale. È necessario innanzitutto avviare una richiesta di ripristino e successivamente attendere che venga resa disponibile una copia temporanea dell'oggetto per la durata specificata nella richiesta. Anche dopo avere ricevuto una copia temporanea dell'oggetto ripristinato, la classe di archiviazione dell'oggetto rimane S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Una richiesta di operazioni API [HeadObject](#) o [GetObject](#) restituirà la classe di storage Recupero flessibile S3 Glacier o S3 Glacier Deep Archive.

Note

Quando ripristini un archivio, paghi sia per l'archivio (tariffa per le classi di archiviazione S3 Glacier Flexible Retrieval [Recupero flessibile S3 Glacier] e S3 Glacier Deep Archive [Archiviazione profonda S3 Glacier]) che per una copia temporaneamente ripristinata (tariffa di archiviazione S3 Standard). Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Puoi ripristinare una copia dell'oggetto a livello di programmazione oppure utilizzando la console Amazon S3. Amazon S3 elabora una sola richiesta di ripristino alla volta per oggetto. Per ulteriori informazioni, consulta [Ripristino di un oggetto archiviato](#).

In che modo queste classi di archiviazione differiscono dal servizio Amazon Glacier

Le classi di storage S3 Glacier fanno parte del servizio Amazon S3 e archiviano i dati come oggetti nei bucket S3. Puoi gestire gli oggetti in queste classi di archiviazione utilizzando la console S3 o a livello di codice utilizzando S3 o. APIs SDKs Quando si archiviano oggetti nelle classi di storage S3 Glacier, è possibile utilizzare le funzionalità S3 come la crittografia avanzata, l'assegnazione di tag agli oggetti e le configurazioni del ciclo di vita S3 per gestire l'accessibilità e il costo dei dati.

Important

Si consiglia di utilizzare le classi di storage S3 Glacier all'interno del servizio Amazon S3 per tutti i dati a lungo termine.

Amazon Glacier è un servizio separato che memorizza i dati come archivi all'interno di vault. Questo servizio non supporta le funzionalità di Amazon S3 e non fornisce supporto della console per le operazioni di caricamento e download dei dati. Non è consigliabile utilizzare il servizio Amazon Glacier per i dati a lungo termine. I dati archiviati in questo servizio non sono accessibili dal servizio Amazon S3. Per ulteriori informazioni sul servizio Amazon Glacier, consulta la [Guida per gli sviluppatori di Amazon Glacier](#). Per trasferire dati dal servizio Amazon Glacier a una classe di storage in Amazon S3, consulta Data [Transfer from Amazon Glacier Vaults ad Amazon](#) S3 nella libreria delle soluzioni. AWS

Utilizzo di oggetti archiviati

Per ridurre i costi di archiviazione degli oggetti a cui si accede raramente, è possibile archiviare tali oggetti. Quando si archivia un oggetto, questo viene spostato in una archiviazione a basso costo, il che significa che non è possibile accedervi in tempo reale.

Sebbene gli oggetti archiviati non siano accessibili in tempo reale, è possibile ripristinarli in pochi minuti o ore, a seconda della classe di archiviazione. Puoi ripristinare un oggetto archiviato utilizzando la console Amazon S3, S3 Batch Operations, l'API REST, AWS gli SDK e (). AWS Command Line Interface AWS CLI Per istruzioni, consulta l'argomento [Ripristino di un oggetto archiviato](#).

Gli oggetti Amazon S3 nelle classi o nei livelli di archiviazione seguenti sono archiviati e non sono accessibili in tempo reale:

- Classe di archiviazione S3 Glacier Flexible Retrieval (Recupero flessibile S3 Glacier)

- Classe di archiviazione S3 Glacier Deep Archive (Archiviazione profonda S3 Glacier)
- Il livello S3 Archive Access Intelligent-Tiering
- Il livello S3 Intelligent-Tiering Deep Archive Access

Note

Gli oggetti archiviati nella classe di storage S3 Glacier Instant Retrieval non vengono archiviati. S3 Glacier Instant Retrieval fornisce l'accesso in tempo reale con una latenza di recupero di millisecondi e non richiede un'operazione di ripristino. Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

Per ripristinare gli oggetti, è necessario completare le seguenti operazioni:

- Per gli oggetti nelle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, è necessario avviare una richiesta di ripristino e quindi attendere fino a quando non sia disponibile una copia temporanea dell'oggetto. Quando viene creata una copia temporanea dell'oggetto ripristinato, la classe di archiviazione dell'oggetto rimane la stessa. Una richiesta di operazioni API [HeadObject](#) o [GetObject](#) ripristina la classe di archiviazione S3 Glacier Flexible Retrieval (Recupero flessibile S3 Glacier) o S3 Glacier Deep Archive (Archiviazione profonda S3 Glacier).
- Per gli oggetti nei livelli S3 Intelligent-Tiering Archive Access e S3 Intelligent-Tiering Deep Archive Access, è necessario avviare la richiesta di ripristino e attendere che l'oggetto venga spostato nel livello Frequent Access.

Per maggiori informazioni sul confronto di tutte le classi di storage di Amazon S3, consulta [Comprensione e gestione delle classi di storage Amazon S3](#). Per ulteriori informazioni su S3, vedere. Intelligent-Tiering [the section called “Come funziona S3 Intelligent-Tiering”](#)

Il tempo necessario per completare un processo di ripristino dipende dalla classe o dal livello di archiviazione utilizzato e dall'opzione di recupero specificata: Express (disponibile solo per S3 Glacier Flexible Retrieval e Intelligent-Tiering S3 Archive Access), Standard o Bulk. Per ulteriori informazioni, consulta [Informazioni sulle opzioni di recupero dall'archivio](#).

Puoi ricevere una notifica quando il ripristino viene completato mediante la funzionalità di notifica eventi di Amazon S3. Per ulteriori informazioni, consulta [Notifiche di eventi Amazon S3](#).

Ripristino di oggetti da Amazon Glacier

Quando si utilizza S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, Amazon S3 ripristina una copia temporanea dell'oggetto solo per la durata specificata. Successivamente, elimina la copia ripristinata dell'oggetto. Puoi modificare il periodo di scadenza di una copia ripristinata eseguendo nuovamente una richiesta di ripristino. In questo caso, Amazon S3 aggiorna il periodo di scadenza relativo all'ora corrente.

Note

Quando ripristini un oggetto archiviato da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, paghi sia per l'oggetto archiviato che per una copia temporaneamente ripristinata. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Amazon S3 calcola l'ora di scadenza della copia dell'oggetto ripristinato aggiungendo il numero di giorni specificati nella richiesta di ripristino all'ora in cui è stato completato il ripristino richiesto. Amazon S3 arrotonda quindi l'ora risultante alla mezzanotte UTC (Universal Coordinated Time) del giorno successivo. Ad esempio, supponiamo che la copia di un oggetto ripristinato sia stata creata il 15 ottobre 2012, alle 10:30 AM UTC e che come periodo di ripristino sia stato specificato un valore di tre giorni. In questo caso, la copia ripristinata scade il 19 ottobre 2012, 00:00 UTC; a quel punto Amazon S3 elimina la copia dell'oggetto.

Ripristino di oggetti da S3 Intelligent-Tiering

Quando si ripristina un oggetto dal livello S3 Intelligent-Tiering Archive Access o S3 Intelligent-Tiering Deep Archive Access, l'oggetto torna al livello Intelligent-Tiering S3 Frequent Access. In seguito, se non si accede all'oggetto per 30 giorni consecutivi, l'oggetto viene spostato automaticamente nel livello Infrequent Access (Accesso Infrequente). Dopo un minimo di 90 giorni consecutivi di mancato accesso, l'oggetto passa al livello S3 Intelligent-Tiering Archive Access. Se non si accede all'oggetto dopo un minimo di 180 giorni consecutivi, l'oggetto passa al livello Deep Archive Access (Accesso archiviazione profonda).

Note

A differenza delle classi di storage S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, le richieste di ripristino per oggetti Intelligent-Tiering S3 non accettano il valore. Days

Utilizzo di Operazioni in batch S3 con richieste di ripristino

Per ripristinare più di un oggetto Amazon S3 con una sola richiesta, è possibile utilizzare le operazioni in batch S3. Fornisci alle operazioni in batch S3 un elenco di oggetti su cui operare. Le operazioni in batch S3 richiamano la rispettiva API per eseguire l'operazione specificata. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti contenenti esabyte di dati.

Argomenti

- [Informazioni sulle opzioni di recupero dall'archivio](#)
- [Ripristino di un oggetto archiviato](#)

Informazioni sulle opzioni di recupero dall'archivio

Amazon S3 dispone di tre classi di storage di archiviazione: S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive. Sebbene gli oggetti archiviati nella classe di storage S3 Glacier Instant Retrieval siano immediatamente disponibili utilizzando GET, per accedere ai dati archiviati nelle classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive devi prima recuperare i dati utilizzando l'API REST. [RestoreObject](#) Il ripristino di set di dati composti da decine di milioni di oggetti o centinaia di terabyte di dati potrebbe richiedere più tempo rispetto ai tempi di ripristino tipici e richiedere considerazioni speciali. Per ulteriori informazioni, consulta [Ripristino di set di dati di grandi dimensioni](#).

È possibile scegliere tra tre opzioni di accesso al recupero per ripristinare gli oggetti archiviati in base alla velocità di recupero desiderata: Expedited, Standard e Bulk.

- **Recupero rapido:** accedi rapidamente ai dati archiviati nella classe di storage S3 Glacier Flexible Retrieval o nel livello S3 Archive Access. Intelligent-Tiering È possibile utilizzare questa opzione per richieste urgenti occasionali relative a un massimo di centinaia di oggetti. Gli oggetti di dimensioni inferiori a 250 megabyte vengono in genere resi disponibili entro 1-5 minuti e gli oggetti di dimensioni pari o superiori a 250 megabyte vengono in genere recuperati con una velocità di recupero fino a 300 megabyte al secondo. Inoltre, è possibile acquistare Provisioned Capacity for Expedited retrievals. Provisioned Capacity aiuta a garantire che la capacità di recupero rapido sia disponibile quando ne hai bisogno. Per ulteriori informazioni, consulta [Capacità con provisioning](#).

 Note

I recuperi Expedited sono una funzionalità premium e vengono addebitati in base alla tariffa di richiesta e recupero Expedited. Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

- **Recupero standard:** accedi ai tuoi dati entro diverse ore. Standard è l'opzione predefinita per le richieste che non specificano l'opzione di recupero. I recuperi standard in genere terminano entro 3-5 ore per la classe di storage S3 Glacier Flexible Retrieval o il livello S3 Archive Access. Intelligent-Tiering I recuperi standard in genere terminano entro 12 ore per la classe di storage S3 Glacier Deep Archive o il livello S3 Deep Archive Access. Intelligent-Tiering I recuperi standard sono gratuiti per gli oggetti archiviati nella classe di storage S3. Intelligent-Tiering

 Note

- Per gli oggetti archiviati nella classe di storage S3 Glacier Flexible Retrieval o nel livello S3 Intelligent-Tiering Archive Access, i recuperi standard avviati utilizzando l'operazione di ripristino S3 Batch Operations iniziano in genere in pochi minuti e terminano entro 3-5 ore con un throughput fino a 1-2 petabyte al giorno.
 - Per gli oggetti della classe di storage S3 Glacier Deep Archive o del livello S3 Intelligent-Tiering Deep Archive Access, i recuperi standard avviati utilizzando Batch Operations in genere iniziano a essere completati entro 9 ore con un throughput fino a 1-2 petabyte al giorno.
- **Recupero in blocco:** accedi ai tuoi dati utilizzando l'opzione di recupero più economica nelle classi di storage S3 Glacier. Con i recuperi in blocco, puoi recuperare grandi quantità di dati in modo economico. Per gli oggetti archiviati nella classe di storage S3 Glacier Flexible Retrieval o nel livello S3 Intelligent-Tiering Archive Access, i recuperi in blocco in genere terminano entro 5-12 ore. Per gli oggetti archiviati nella classe di storage S3 Glacier Deep Archive o nel livello S3 Deep Archive Access, questi recuperi in genere terminano entro Intelligent-Tiering 48 ore. I recuperi in blocco sono gratuiti per gli oggetti archiviati nelle classi di storage S3 Glacier Flexible Retrieval o S3. Intelligent-Tiering

La tabella seguente riepiloga le opzioni di recupero archivi. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Per effettuare un ExpeditedStandard, o Bulk recuperare, imposta l'elemento di richiesta nella Tier richiesta di operazione dell'API [RestoreObject](#) REST sull'opzione desiderata o sull'equivalente in () o negli AWS Command Line Interface SDK.AWS CLI AWS Se hai acquistato capacità con provisioning, tutti i recuperi Expedited vengono serviti automaticamente mediante la capacità con provisioning.

Ripristino di set di dati di grandi dimensioni

Il ripristino di set di dati composti da decine di milioni di oggetti o centinaia di terabyte di dati potrebbe richiedere più tempo rispetto ai tempi di ripristino tipici per qualsiasi livello di recupero a causa dei limiti di recupero.

Quando si avviano richieste di ripristino per oggetti archiviati nelle classi di storage S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive o S3, viene applicata una quota di richieste di recupero per l'utente. Intelligent-Tiering Account AWS S3 Glacier supporta richieste di ripristino a una velocità massima di 1.000 transazioni al secondo. Se questa velocità viene superata, le richieste altrimenti valide vengono sottoposte alla limitazione della larghezza di banda della rete o rifiutate e Amazon S3 restituisce un errore `ThrottlingException`. Puoi utilizzare S3 Batch Operations per recuperare molti oggetti con una singola richiesta, sfruttando appieno la percentuale di richieste di ripristino disponibile nel tuo account. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch](#).

Dopo aver avviato le richieste di ripristino, S3 Glacier supporta il ripristino di set di dati di grandi dimensioni con un throughput fino a 1-2 petabyte al giorno per account cliente. Per qualsiasi opzione di recupero, gli oggetti di dimensioni superiori a 5 terabyte impiegheranno più tempo per essere ripristinati con un throughput di recupero fino a 300 megabyte al secondo. Ad esempio, il completamento di un oggetto S3 Glacier Flexible Retrieval da 50 terabyte potrebbe richiedere fino a 48 ore. Se desideri aumentare i limiti di ripristino, puoi contattare l'assistenza. AWS

Capacità con provisioning

La capacità con provisioning assicura che la capacità di recupero per effettuare recuperi di tipo Expedited da S3 Glacier Flexible Retrieval sia disponibile in base alla necessità. Ogni unità di capacità consente di eseguire almeno tre recuperi rapidi ogni 5 minuti e fornisce fino a 300 megabyte al secondo di velocità di recupero.

Senza capacità con provisioning, i recuperi Expedited potrebbero non essere accettati durante periodi di richiesta elevata. Per un accesso rapido e prevedibile a una maggiore quantità di dati, prendi in considerazione l'utilizzo della classe di storage S3 Glacier Instant Retrieval. <https://aws.amazon.com/s3/storage-classes/glacier/instant-retrieval/>

Le unità di capacità assegnate sono allocate a un Account AWS. Pertanto, il richiedente del recupero Expedited dei dati dovrebbe acquistare l'unità di capacità assegnata, non il proprietario del bucket.

È possibile acquistare la capacità assegnata utilizzando la console Amazon S3, la console Amazon Glacier, l'operazione API [REST](#) Purchase Provisioned Capacity, gli SDK o il. AWS CLI. Per informazioni sui prezzi relativi a capacità con provisioning, consulta [Prezzi di Amazon S3](#).

Ripristino di un oggetto archiviato

Gli oggetti Amazon S3 nelle classi o nei livelli di archiviazione seguenti sono archiviati e non sono accessibili in tempo reale:

- Classe di archiviazione S3 Glacier Flexible Retrieval (Recupero flessibile S3 Glacier)
- Classe di archiviazione S3 Glacier Deep Archive (Archiviazione profonda S3 Glacier)
- Il livello S3 Archive Access Intelligent-Tiering
- Il livello S3 Intelligent-Tiering Deep Archive Access

Gli oggetti Amazon S3 memorizzati nelle classi di archiviazione S3 Glacier Flexible Retrieval S3 Glacier Deep Archive non sono immediatamente accessibili. Per accedere a un oggetto in queste classi di storage, è necessario ripristinare una copia temporanea dell'oggetto nel relativo bucket S3 per una durata specificata (numero di giorni). Se vuoi ottenere una copia permanente dell'oggetto, ripristina l'oggetto e creane quindi una copia nel bucket Amazon S3. L'operazione di copia degli oggetti ripristinati non è supportata nella console Amazon S3. Per questo tipo di operazione di copia, usa AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST. A meno che non si crei una copia, l'oggetto verrà comunque archiviato nelle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Per informazioni sull'utilizzo di queste classi di archiviazione, consulta [Classi di storage per oggetti con accesso non frequente](#).

Per accedere agli oggetti nei livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access, è necessario avviare una richiesta di ripristino e attendere che l'oggetto venga spostato nel livello Frequent Access. Quando esegui il ripristino dai livelli Accesso di archiviazione o di archiviazione profonda, l'oggetto passa nuovamente al livello Accesso frequente. Per informazioni sull'utilizzo di queste classi di archiviazione, consulta [Classe di storage per ottimizzare automaticamente i dati con modelli di accesso variabili o sconosciuti](#).

Per informazioni generali sugli oggetti archiviati, consulta [Utilizzo di oggetti archiviati](#).

 Note

- Quando ripristini un oggetto archiviato dalle classi di storage Recupero flessibile S3 Glacier o S3 Glacier Deep Archive, paghi sia per l'oggetto archiviato che per una copia temporaneamente ripristinata.
- Quando ripristini un oggetto da S3 Intelligent-Tiering, non sono previsti costi di recupero per i recuperi standard o in blocco.
- Le richieste di ripristino successive richiamate su oggetti che sono già stati ripristinati vengono fatturate come richieste GET. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Ripristino di un oggetto archiviato

Puoi ripristinare un oggetto archiviato utilizzando la console Amazon S3, l'API REST di Amazon S3, gli AWS SDK, () o S3 Batch Operations. AWS Command Line Interface AWS CLI

Utilizzo della console S3

Ripristino di oggetti mediante la console Amazon S3

Utilizza la seguente procedura per ripristinare un oggetto che è stato archiviato nelle classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive o nei livelli di storage S3 Archive Access o Deep Archive Access. Intelligent-Tiering

Per ripristinare un oggetto archiviato

1. Accedi e apri la console Amazon S3 all'indirizzo. Console di gestione AWS <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket, scegli il nome del bucket contenente gli oggetti che desideri ripristinare.
4. Nell'elenco Objects (Oggetti) selezionare l'oggetto o gli oggetti che si desidera ripristinare, scegliere Actions (Operazioni), quindi selezionare Initiate restore (Avvia ripristino).
5. Se esegui il ripristino da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, immetti il numero di giorni in cui desideri che i dati archiviati siano accessibili nella casella Numero di giorni in cui la copia ripristinata è disponibile.
6. Per Opzioni di recupero, effettua una delle seguenti operazioni:

- Sceglie Recupero Bulk oppure Recupero Standard, quindi seleziona Ripristina.
- Scegli il recupero rapido (disponibile solo per S3 Glacier Flexible Retrieval o S3 Archive Access). Intelligent-Tiering Se stai ripristinando un oggetto in S3 Glacier Flexible Retrieval, puoi scegliere se acquistare capacità assegnata per il recupero Expedited. Se desideri acquistare capacità assegnata, procedi alla fase successiva. Altrimenti, scegli Avvia il ripristino.

Note

Gli oggetti dei livelli S3 Intelligent-Tiering Archive Access e Deep Archive Access vengono ripristinati automaticamente al livello Frequent Access.

7. (Facoltativo) Se stai ripristinando un oggetto in S3 Glacier Flexible Retrieval e scegli Recupero expedited puoi scegliere se acquistare capacità assegnata. La capacità assegnata è disponibile solo per gli oggetti in S3 Glacier Flexible Retrieval. Se disponi già di capacità assegnata, scegli Ripristina per avviare un ripristino mediante capacità assegnata.

Se disponi di capacità assegnata, tutti i recuperi Expedited vengono eseguiti mediante tale capacità assegnata. Per ulteriori informazioni, consulta [Capacità con provisioning](#).

- Se non disponi di capacità assegnata e non desideri acquistarla, scegli Ripristina.
- Se non disponi di capacità assegnata, ma desideri acquistare unità di capacità assegnata (PCU), scegli Acquisto di PCU. Nella finestra di dialogo Acquisto di PCU, scegli quante PCU vuoi acquistare, conferma l'acquisto e poi scegli Acquisto di PCU. Quando ricevi il messaggio Acquisto riuscito, scegli Ripristina per avviare un recupero mediante capacità assegnata.

Utilizzo di AWS CLI

Ripristino di oggetti da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive

L'esempio seguente utilizza il comando `restore-object` per ripristinare l'oggetto *dir1/example.obj* nel bucket *amzn-s3-demo-bucket* per 25 giorni.

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{"Days":25,"GlacierJobParameters":{"Tier":"Standard"}}'
```


Se la sintassi JSON utilizzata nell'esempio genera un errore su un client Windows, sostituire la richiesta di ripristino con la seguente sintassi:

```
--restore-request Days=25,GlacierJobParameters={"Tier"="Standard"}
```

Ripristina gli oggetti da S3 Intelligent-Tiering Archive Access e Deep Archive Access

L'esempio seguente utilizza il comando `restore-object` per ripristinare l'oggetto *dir1/example.obj* nel bucket *amzn-s3-demo-bucket* nel livello Frequent Access.

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{}'
```

Note

A differenza delle classi di storage S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, le richieste di ripristino per oggetti Intelligent-Tiering S3 non accettano il valore. Days

Monitoraggio dello stato del ripristino

Per monitorare lo stato della richiesta `restore-object`, usa il seguente comando `head-object`:

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

Per ulteriori informazioni, consulta [restore-object](#) nella documentazione di riferimento dei comandi della AWS CLI .

Utilizzo della REST API

Amazon S3 fornisce un'operazione API che consente di avviare il ripristino di un oggetto archiviato. Per ulteriori informazioni, consulta [RestoreObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Utilizzo di AWS SDK

Per esempi di come ripristinare oggetti archiviati in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive con gli SDK, consulta Esempi di codice nell'Amazon S3 API Reference. AWS https://docs.aws.amazon.com/AmazonS3/latest/API/s3_example_s3_RestoreObject_section.html

Utilizzo delle operazioni in batch S3

Per ripristinare più di un oggetto archiviato con una sola richiesta, puoi utilizzare le operazioni in batch S3. Fornisci alle operazioni in batch S3 un elenco di oggetti su cui operare. Le operazioni in batch S3 richiamano la rispettiva API per eseguire l'operazione specificata. Un solo processo di operazioni in batch può eseguire l'operazione specificata su miliardi di oggetti contenenti esabyte di dati.

Per creare un processo di operazioni in batch, è necessario disporre di un manifesto che contenga solo gli oggetti che si desidera ripristinare. Puoi creare un manifesto utilizzando inventario S3 oppure puoi fornire un file CSV con le informazioni necessarie. Per ulteriori informazioni, consulta [the section called “Specifica di un manifest”](#).

Prima di creare ed eseguire i processi delle operazioni in batch S3, devi concedere le autorizzazioni ad Amazon S3 per eseguire tali operazioni per tuo conto. Per le autorizzazioni richieste, consulta [the section called “Concessione di autorizzazioni”](#).

Note

I job Batch Operations possono essere eseguiti su oggetti delle classi di storage S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive o su oggetti di livello di storage S3 Archive Access e Deep Archive Access. Intelligent-Tiering Le operazioni in batch non possono operare su entrambi i tipi di oggetti archiviati nello stesso processo. Per ripristinare oggetti di entrambi i tipi, devi creare processi Batch Operations separati.

Per ulteriori informazioni sull'utilizzo delle operazioni in batch per la replica di oggetti esistenti, consulta [the section called “Ripristino di oggetti”](#).

Creazione di un processo di operazioni in batch S3 Initiate Restore Object

1. Accedi e apri la console Amazon S3 all' Console di gestione AWS indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Operazioni in batch.
3. Scegli Crea processo.
4. Per Regione AWS, scegli la regione in cui creare il processo.
5. In Formato manifest scegli il tipo di oggetto manifesto da usare.

- Se scegli il rapporto di inventario S3, inserisci il percorso dell'oggetto `manifest.json` che Amazon S3 ha generato come parte del CSV-formatted rapporto di inventario. Se desideri utilizzare una versione del manifesto diversa da quella più recente, immetti l'ID della versione dell'oggetto `manifest.json`.
 - Se scegli CSV, inserisci il percorso di un CSV-formatted oggetto manifesto. L'oggetto manifesto deve avere il formato descritto nella console. Se desideri utilizzare una versione diversa da quella più recente, puoi includere facoltativamente l'ID della versione dell'oggetto manifesto.
6. Scegli Avanti.
 7. Nella sezione Operazione, scegli Ripristina.
 8. Nella sezione Restore, per Restore source, scegli Glacier Flexible Retrieval o Glacier Deep Archive o Archive Access tier o Deep Intelligent-Tiering Archive Access tier.

Se hai scelto Glacier Flexible Retrieval o Glacier Deep Archive, inserisci un numero per Numero di giorni in cui la copia ripristinata è disponibile.

Per Livello di recupero, scegli il livello che desideri utilizzare.

9. Scegli Avanti.
10. Nella pagina Configura opzioni aggiuntive, compila le seguenti sezioni:

- Nella sezione Altre opzioni, fornisci una descrizione del processo e specifica un numero di priorità per il processo. I numeri più alti indicano una priorità più alta. Per ulteriori informazioni, consulta [the section called “Assegnazione della priorità dei processi”](#).
- Nella sezione Report di completamento, seleziona se le operazioni in batch devono creare un report di completamento. Per ulteriori informazioni sui report di completamento, consulta [the section called “Rapporti di completamento”](#).
- Nella sezione Autorizzazioni, devi concedere ad Amazon S3 le autorizzazioni per eseguire operazioni in batch per tuo conto. Per le autorizzazioni richieste, consulta [the section called “Concessione di autorizzazioni”](#).
- (Facoltativo) Nella sezione Tag dell'attività, aggiungi tag nelle coppie chiave-valore. Per ulteriori informazioni, consulta [the section called “Utilizzo dei tag”](#).

Quando hai terminato, seleziona Successivo.

11. Nella pagina Review (Rivedi), verificare le impostazioni. Se è necessario apportare modifiche, scegliere Previous (Precedente). In caso contrario, scegli Crea processo.

Per ulteriori informazioni sulle operazioni in batch, consulta [Ripristino di oggetti con operazioni in batch](#) e [Creazione di un processo di operazioni in batch S3](#).

Controllo dello stato di ripristino e della data di scadenza

Puoi verificare lo stato di una richiesta di ripristino o la data di scadenza utilizzando la console Amazon S3, Amazon S3 Event Notifications, l'API REST di Amazon S3 o Amazon S3. AWS CLI

Note

Gli oggetti ripristinati dalle classi di storage Recupero flessibile S3 Glacier e S3 Glacier Deep Archive vengono archiviati solo per il numero di giorni specificato. Le procedure seguenti restituiscono la data di scadenza di queste copie.

Gli oggetti ripristinati dai livelli di storage S3 Intelligent-Tiering Archive Access e Deep Archive Access non hanno date di scadenza e vengono invece spostati nuovamente al livello Frequent Access.

Utilizzo della console S3

Verifica dello stato di ripristino e della data di scadenza di un oggetto nella console Amazon S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket, seleziona il nome del bucket contenente l'oggetto che desideri ripristinare.
4. Nell'elenco Oggetti, seleziona l'oggetto che stai ripristinando. Viene visualizzata la pagina dei dettagli dell'oggetto.
 - Se il ripristino non è terminato, una sezione indica **Restauro in corso**.
 - Se il restauro è terminato, una sezione dice **Restauro completato**. Se esegui il ripristino da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, questa sezione indica anche la Data di scadenza del ripristino. In questa data Amazon S3 rimuoverà la copia ripristinata dell'oggetto archiviato.

Utilizzo delle Notifiche di eventi Amazon S3

È possibile impostare la ricezione di una notifica del completamento del ripristino degli oggetti utilizzando l'operazione `s3:ObjectRestore:Completed` con la funzionalità Notifiche di eventi

Amazon S3. Per ulteriori informazioni sull'attivazione delle notifiche degli eventi, consulta [Abilitare le notifiche utilizzando Amazon SQS, Amazon SNS e AWS Lambda](#). Per ulteriori informazioni sui vari tipi di eventi ObjectRestore, consulta [the section called "Tipi di eventi supportati per SQS, SNS e Lambda"](#).

Utilizzo di AWS CLI

Controlla lo stato di ripristino e la data di scadenza di un oggetto con AWS CLI

L'esempio seguente utilizza il comando `head-object` per visualizzare i metadati dell'oggetto *dir1/example.obj* nel bucket *amzn-s3-demo-bucket*. Quando esegui questo comando su un oggetto in fase di ripristino, Amazon S3 indica se il ripristino è in corso e (se applicabile) la data di scadenza.

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

Output previsto (ripristino in corso):

```
{
  "Restore": "ongoing-request=\"true\"",
  "LastModified": "2020-06-16T21:55:22+00:00",
  "ContentLength": 405,
  "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
  "VersionId": "wbYaE2vt0V0iIBXr0qGAJt3fP1cHB8Wi",
  "ContentType": "binary/octet-stream",
  "ServerSideEncryption": "AES256",
  "Metadata": {},
  "StorageClass": "GLACIER"
}
```

Output previsto (ripristino terminato):

```
{
  "Restore": "ongoing-request=\"false\", expiry-date=\"Wed, 12 Aug 2020 00:00:00 GMT\"",
  "LastModified": "2020-06-16T21:55:22+00:00",
  "ContentLength": 405,
  "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
  "VersionId": "wbYaE2vt0V0iIBXr0qGAJt3fP1cHB8Wi",
  "ContentType": "binary/octet-stream",
  "ServerSideEncryption": "AES256",
  "Metadata": {},
}
```

```
"StorageClass": "GLACIER"  
}
```

Per ulteriori informazioni su `head-object`, consulta [head-object](#) nel Riferimento ai comandi AWS CLI .

Utilizzo della REST API

Amazon S3 fornisce un'operazione API per recuperare i metadati degli oggetti. Per verificare lo stato di ripristino e la data di scadenza di un oggetto archiviato utilizzando la REST API, consulta [HeadObject](#) in Amazon Simple Storage Service API Reference.

Aggiornamento della velocità di un ripristino in corso

Puoi aggiornare la velocità di un ripristino mentre il ripristino è in corso.

Per aggiornare un ripristino in corso a un livello più veloce

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Buckets (Bucket) scegliere il nome del bucket che contiene gli oggetti che si desidera ripristinare.
4. Nell'elenco Oggetti, seleziona l'oggetto che stai ripristinando. Viene visualizzata la pagina dei dettagli dell'oggetto. Nella pagina dei dettagli dell'oggetto, scegli Aggiorna livello di recupero. Per informazioni su come verificare lo stato del ripristino di un oggetto, consulta [Controllo dello stato di ripristino e della data di scadenza](#).
5. Seleziona il livello che desideri aggiornare, quindi seleziona Avvia il ripristino.

Gestione del ciclo di vita degli oggetti

Il ciclo di vita S3 consente di archiviare gli oggetti in modo conveniente durante l'intero ciclo di vita trasferendoli in classi di storage a costi inferiori o eliminando gli oggetti scaduti per conto dell'utente. Per gestire il ciclo di vita degli oggetti, creare una configurazione del ciclo di vita S3 per il proprio bucket. Una configurazione del ciclo di vita di S3 è un insieme di regole che definisce le operazioni che Amazon S3 deve applicare a un gruppo di oggetti. Esistono due tipi di operazioni:

- Operazioni di transizione – Queste operazioni definiscono quando gli oggetti passano a un'altra classe di archiviazione. Ad esempio, è possibile scegliere di trasferire gli oggetti nella classe di

Standard-IA storage S3 30 giorni dopo la loro creazione o di archiviare gli oggetti nella classe di storage S3 Glacier Flexible Retrieval un anno dopo averli creati. Per ulteriori informazioni, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).

Le richieste di transizione del ciclo di vita sono soggette a costi. Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

- Operazioni di scadenza – Queste operazioni consentono di specificare la scadenza degli oggetti. Amazon S3 elimina gli oggetti scaduti per tuo conto. Ad esempio, si può scegliere di far scadere gli oggetti dopo che sono stati archiviati per un periodo di conformità normativa. Per ulteriori informazioni, consulta [Oggetti in scadenza](#).

Esistono costi potenziali associati alla scadenza del ciclo di vita solo quando si fanno scadere gli oggetti in una classe di storage con una durata di storage minima. Per ulteriori informazioni, consulta [Costo della durata di archiviazione minima](#).

Important

Bucket per uso generico: non è possibile utilizzare una policy di bucket per impedire eliminazioni o transizioni in base a una regola del ciclo di vita S3. Ad esempio, anche se la policy del bucket nega tutte le azioni per tutti i principali, la configurazione di S3 Lifecycle continua a funzionare normalmente.

Note

S3 Lifecycle non gestisce le annotazioni in modo indipendente. L'archiviazione delle annotazioni viene sempre fatturata alle tariffe standard S3 nello storage Frequent Access, indipendentemente dalla classe di archiviazione dell'oggetto principale. Quando una regola del ciclo di vita fa scadere un oggetto, tutte le annotazioni associate a tale versione dell'oggetto vengono eliminate.

Oggetti esistenti e nuovi

Quando si aggiunge una configurazione del ciclo di vita a un bucket, le regole di configurazione si applicano sia agli oggetti esistenti sia a quelli che vengono aggiunti in un secondo momento. Se, ad esempio, si aggiunge in data odierna una regola di configurazione del ciclo di vita con un'operazione

di scadenza in base a cui gli oggetti scadono 30 giorni dopo la creazione, Amazon S3 inserirà nella coda di eliminazione tutti gli oggetti esistenti creati da più di 30 giorni.

Modifiche nella fatturazione

In caso di ritardo tra il momento in cui un oggetto diventa idoneo per un'operazione del ciclo di vita e il momento in cui Amazon S3 trasferisce o rimuove l'oggetto, le modifiche alla fatturazione vengono applicate non appena l'oggetto diventa idoneo per l'operazione del ciclo di vita. Ad esempio, se è pianificata la scadenza di un oggetto e Amazon S3 non lo rimuove immediatamente, non verrà addebitato alcun costo per lo storage dopo il periodo di scadenza.

L'unica eccezione a questo comportamento è rappresentata dalla presenza di una regola del ciclo di vita per la transizione alla classe di storage S3. Intelligent-Tiering In tal caso, le modifiche alla fatturazione non avvengono finché l'oggetto non è passato a S3. Intelligent-Tiering Per ulteriori informazioni sulle regole del ciclo di vita S3, consulta [Elementi della configurazione del ciclo di vita](#).

Note

Non sono previsti costi di recupero dei dati per le transizioni del ciclo di vita. Tuttavia, sono previsti costi per l'inserimento dei dati per richiesta quando si utilizzano le regole PUT, COPY o del ciclo di vita per spostare i dati in qualsiasi classe di storage S3. Considerare il costo di inserimento dei dati o di transizione prima di spostare gli oggetti in qualsiasi classe di storage. Per ulteriori considerazioni relative ai costi, consulta [Prezzi di Amazon S3](#).

Monitoraggio dell'effetto delle regole del ciclo di vita

Per monitorare l'effetto degli aggiornamenti effettuati dalle regole attive del ciclo di vita, consulta [the section called “Come posso monitorare le azioni intraprese dalle mie regole del ciclo di vita?”](#).

Gestione del ciclo di vita completo degli oggetti

Tramite le regole di configurazione del ciclo di vita S3, è possibile indicare ad Amazon S3 di trasferire gli oggetti in classi di storage meno costose, archivarli o eliminarli. Ad esempio:

- Se vengono caricati dei log periodici su un bucket, l'applicazione potrebbe averne bisogno per una settimana o per un mese. Dopo tale periodo, si potrebbe desiderare di eliminarli.
- Alcuni documenti vengono utilizzati con frequenza per un periodo di tempo limitato. Dopo tale momento, vi si accede raramente. Con il passare del tempo, potrebbe non essere più necessario

avere l'accesso in tempo reale a questi oggetti. Tuttavia, per motivi legati all'organizzazione o alle normative, potrebbe essere necessario conservarli in archivio per un periodo specifico. Dopo tale periodo, è possibile eliminarli.

- È possibile caricare alcuni tipi di dati su Amazon S3 principalmente per finalità di archiviazione. Ad esempio, è possibile conservare archivi multimediali, record sanitari e finanziari, dati di sequenza genomica non elaborati, backup di database a lungo termine e dati che devono essere conservati per esigenze di conformità normativa.

Per gestire l'intero ciclo di vita S3 di un oggetto, è possibile combinare le operazioni sul ciclo di vita sopra citate. Supponiamo ad esempio di creare oggetti con un ciclo di vita ben definito. Nei primi 30 giorni gli oggetti vengono utilizzati frequentemente. Poi, gli oggetti vengono utilizzati raramente fino a 90 giorni. Dopo tale periodo, gli oggetti non sono più necessari ed è quindi possibile archivarli o eliminarli.

In questo scenario, è possibile creare una regola del ciclo di vita S3 in cui si specifica l'azione di transizione iniziale allo storage S3, S3 o S3 One Intelligent-Tiering, un'altra azione di transizione Zone-IA allo storage S3 Glacier Flexible Retrieval per l'archiviazione e un'azione di scadenza. Standard-IA Spostando gli oggetti da una classe di storage all'altra, si risparmia sui costi di storage. Per ulteriori considerazioni relative ai costi, consulta [Prezzi di Amazon S3](#).

Argomenti

- [Trasferimento degli oggetti utilizzando il ciclo di vita Amazon S3](#)
- [Oggetti in scadenza](#)
- [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#)
- [Come il ciclo di vita S3 interagisce con altre configurazioni del bucket](#)
- [Configurazione delle notifiche di eventi del ciclo di vita S3](#)
- [Elementi della configurazione del ciclo di vita](#)
- [In che modo Amazon S3 gestisce i conflitti nelle configurazioni del ciclo di vita](#)
- [Esempi di configurazioni del ciclo di vita S3](#)
- [Risoluzione dei problemi del ciclo di vita di Amazon S3](#)

Trasferimento degli oggetti utilizzando il ciclo di vita Amazon S3

È possibile aggiungere operazioni di transizione a una configurazione del ciclo di vita S3 per indicare ad Amazon S3 di spostare gli oggetti in un'altra classe di storage Amazon S3. Per ulteriori

informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#). Alcuni esempi di quando è possibile utilizzare le configurazioni del ciclo di vita S3 in questo modo includono i seguenti:

- Quando si sa che gli oggetti sono accessibili raramente, è possibile trasferirli alla classe di storage S3. Standard-IA
- Gli oggetti per i quali non è necessario avere l'accesso in tempo reale possono essere archiviati nella classe di storage Recupero flessibile S3 Glacier o S3 Glacier Deep Archive.

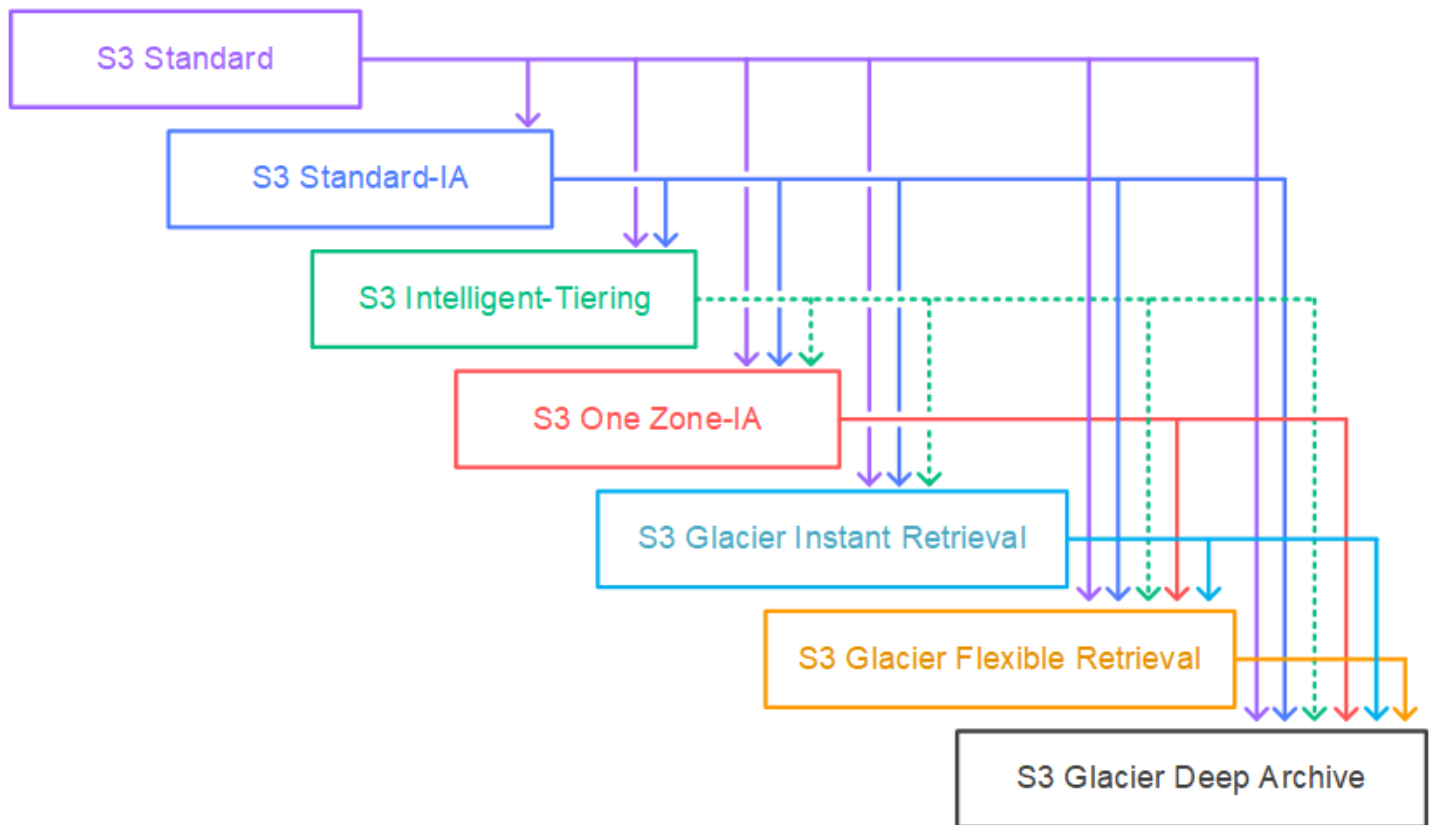
Note

Gli oggetti crittografati rimangono tali durante l'intero processo di transazione tra classi di storage.

Transizioni supportate

In una configurazione del ciclo di vita S3 puoi definire regole per la transizione degli oggetti da una classe di storage a un'altra per risparmiare sui costi di storage. Se non conosci i modelli di accesso dei tuoi oggetti o se i modelli di accesso cambiano nel tempo, puoi passare gli oggetti alla classe di Intelligent-Tiering storage S3 per risparmiare automaticamente sui costi. Per informazioni sulle classi di storage, consultare [Comprensione e gestione delle classi di storage Amazon S3](#).

Amazon S3 supporta un modello a cascata per la transizione tra classi di storage, come mostrato nel diagramma seguente.



Transizioni del ciclo di vita supportate

Amazon S3 supporta le transizioni del ciclo di vita seguenti tra classi di storage tramite una configurazione del ciclo di vita S3.

- Dalla classe di storage S3 Standard alle classi di storage S3, S3 Standard-IA, S3 One, S3 Intelligent-Tiering, S3 Glacier Instant Retrieval, S3 One Zone-IA, S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.
- Dalla classe di storage S3 alle classi Standard-IA di storage S3, S3 One, S3 Glacier Instant Retrieval, S3 Intelligent-Tiering, S3 Glacier Flexible Retrieval o S3 One Zone-IA, S3 Glacier Deep Archive.
- La classe di storage S3 può passare a classi di Intelligent-Tiering storage diverse a seconda del livello di accesso S3. Intelligent-Tiering Le seguenti transizioni sono possibili per ogni livello di accesso.
 - Livello Frequent Access o Infrequent Access alle classi di storage S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.
 - Dal livello Archive Instant Access alle classi di archiviazione S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.

- Dal livello Archive Access alle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.
- Dal livello Deep Archive Access alle classi di archiviazione S3 Glacier Deep Archive.
- Dalla classe di storage S3 One alle classi di Zone-IA storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.
- La classe di archiviazione S3 Glacier Instant Retrieval alle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive.
- Classe di archiviazione S3 Glacier Flexible Retrieval alla classe S3 Glacier Deep Archive.

Note

Per i bucket con controllo delle versioni abilitato o sospeso, non è possibile effettuare la transizione di oggetti con uno stato di replica o. Pending Failed

Vincoli e considerazioni per le transizioni

Alle transizioni tra classi di storage del ciclo di vita si applicano i vincoli seguenti:

Per impostazione predefinita, gli oggetti di dimensioni inferiori a 128 KB non verranno trasferiti ad alcuna classe di storage

Amazon S3 applica un comportamento predefinito alle configurazioni del ciclo di vita S3 che impedisce la transizione di oggetti di dimensioni inferiori a 128 KB a qualsiasi classe di storage. Non è consigliabile eseguire la transizione di oggetti inferiori a 128 KB perché viene addebitata una richiesta di transizione per ogni oggetto. Ciò significa che, per gli oggetti più piccoli, i costi di transizione possono superare i risparmi di storage. Per ulteriori informazioni sui costi delle richieste di transizione, consulta Richieste e recupero dati nella scheda Storage e richieste della pagina [Prezzi di Amazon S3](#).

Per consentire la transizione di oggetti più piccoli, è possibile aggiungere un [filtro per le dimensioni degli oggetti](#) alle regole di transizione del ciclo di vita che specifica una dimensione minima (ObjectSizeGreaterThan) o una dimensione massima (ObjectSizeLessThan) personalizzata. Per ulteriori informazioni, consulta [Esempio: Consentire la transizione di oggetti di dimensioni inferiori a 128 KB](#).

 Note

A settembre 2024 Amazon S3 ha aggiornato il comportamento di transizione predefinito per gli oggetti di piccole dimensioni, come segue:

- Comportamento di transizione predefinito aggiornato: a partire da settembre 2024, il comportamento predefinito impedisce la transizione di oggetti di dimensioni inferiori a 128 KB a qualsiasi classe di storage.
- Comportamento di transizione predefinito precedente: prima di settembre 2024, il comportamento predefinito consentiva la transizione di oggetti di dimensioni inferiori a 128 KB solo nelle classi di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

Le configurazioni create prima di settembre 2024 mantengono il comportamento di transizione precedente a meno che non vengano modificate. In altre parole, se si creano, modificano o eliminano regole, il comportamento di transizione predefinito per la configurazione cambia in base al comportamento aggiornato. Se il caso d'uso lo richiede, è possibile modificare il comportamento di transizione predefinito in modo che gli oggetti di dimensioni inferiori a 128 KB passino a S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive. A tale scopo, utilizza l'intestazione `x-amz-transition-default-minimum-object-size` opzionale in una richiesta [PutBucketLifecycleConfiguration](#).

Viene addebitato il costo della transizione degli oggetti prima della loro durata minima di storage

Alcune classi di storage hanno una durata minima di storage degli oggetti. Se gli oggetti vengono trasferiti da queste classi di storage prima della durata minima, viene addebitato il costo della durata residua. Per ulteriori informazioni su quali classi di storage hanno una durata minima di storage, consulta [Confronto delle classi di storage di Amazon S3](#).

Non è possibile creare una singola regola del ciclo di vita che trasferisca gli oggetti da una classe di storage all'altra prima che sia trascorso il periodo di durata minimo di storage.

Ad esempio, Recupero istantaneo S3 Glacier ha una durata minima di storage di 90 giorni. Non è possibile specificare una regola del ciclo di vita che trasferisca gli oggetti a S3 Glacier Instant Retrieval dopo 4 giorni e quindi trasferisca gli oggetti a S3 Glacier Deep Archive dopo 20 giorni. In questo caso, la transizione a S3 Glacier Deep Archive deve avvenire dopo almeno 94 giorni.

È possibile specificare due regole per ottenere tale risultato, ma occorre pagare i costi di storage per la durata minima. Per ulteriori considerazioni relative ai costi, consulta [Prezzi di Amazon S3](#).

Per ulteriori informazioni sulla creazione di un ciclo di vita S3, consulta [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#).

Tag-based filtri e valutazione dell'idoneità

S3 Lifecycle valuta quotidianamente gli oggetti rispetto ai filtri basati su tag. Quando un oggetto corrisponde a una regola di transizione basata su tag, Amazon S3 mette in coda l'azione per l'elaborazione asincrona. Al momento dell'esecuzione, Amazon S3 rivaluta i tag correnti dell'oggetto. Se il tag di attivazione non è più presente al momento dell'esecuzione dell'azione, la transizione non procede.

Poiché il tempo che intercorre tra la valutazione e l'esecuzione non è deterministico, la rimozione di un tag non garantisce una cancellazione immediata: l'azione può essere eseguita prima che la rimozione del tag venga osservata o la rimozione del tag può avere effetto prima del successivo ciclo di valutazione.

Per impedire in modo affidabile una transizione dopo l'etichettatura di un oggetto, attendi che una notifica degli eventi [del ciclo di vita](#) confermi il completamento dell'azione prima di rimuovere il tag. Se devi impedire una transizione prima che venga eseguita, rimuovi il tag anziché disabilitare la regola (la propagazione degli aggiornamenti delle policy delle regole può richiedere fino a 15 minuti).

Trasferimento nelle classi di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive (archiviazione di oggetti)

Usando una configurazione del ciclo di vita S3, è possibile eseguire la transizione degli oggetti alle classi di storage Recupero flessibile S3 Glacier o S3 Glacier Deep Archive per l'archiviazione.

Prima di archiviare gli oggetti, consultare le sezioni seguenti per alcune considerazioni in merito.

Considerazioni generali

Di seguito sono riportate le considerazioni generali di cui tenere conto prima di archiviare gli oggetti:

- Gli oggetti crittografati rimangono tali durante l'intero processo di transazione tra classi di storage.
- Gli oggetti conservati nelle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive non sono disponibili in tempo reale.

Gli oggetti archiviati sono oggetti di Amazon S3 , tuttavia, prima di poter accedere a un oggetto archiviato, è necessario ripristinarne una copia temporanea. La copia dell'oggetto ripristinato è disponibile solo per la durata che viene specificata nella richiesta di ripristino. Successivamente Amazon S3 elimina la copia temporanea e l'oggetto rimane archiviato in S3 Glacier Flexible Retrieval.

Puoi ripristinare un oggetto utilizzando la console Amazon S3 o a livello di programmazione utilizzando le librerie di wrapper AWS SDK o l'API REST di Amazon S3 nel codice. Per ulteriori informazioni, consulta [Ripristino di un oggetto archiviato](#).

- Gli oggetti conservati nella classe di archiviazione S3 Glacier Flexible Retrieval possono essere trasferiti solo nella classe di archiviazione S3 Glacier Deep Archive.

È possibile utilizzare una regola di configurazione del ciclo di vita S3 per convertire la classe di archiviazione di un oggetto da S3 Glacier Flexible Retrieval alla sola classe di archiviazione S3 Glacier Deep Archive. Se si vuole modificare la classe di archiviazione di un oggetto conservato in Glacier S3 Flexible Retrieval in una classe di archiviazione diversa da S3 Glacier Deep Archive, bisogna prima utilizzare l'operazione di ripristino per creare una copia temporanea dell'oggetto. Quindi utilizza l'operazione di copia per sovrascrivere l'oggetto specificando S3 Standard, S3, S3, S3 One o Reduced Redundancy Intelligent-Tiering come classe di archiviazione Standard-IA. Zone-IA

- La transizione di oggetti nella classe di storage S3 Glacier Deep Archive è unidirezionale.

Non puoi usare una regola di configurazione del ciclo di vita S3 per convertire la classe di storage di un oggetto da S3 Glacier Deep Archive in un'altra classe di storage. Se vuoi cambiare la classe di storage di un oggetto archiviato specificandone un'altra, devi prima di tutto usare l'operazione di ripristino per creare una copia temporanea dell'oggetto. Quindi utilizzate l'operazione di copia per sovrascrivere l'oggetto che specifica S3 Standard, S3, S3, S3 One, S3 Glacier Instant Retrieval Intelligent-Tiering, S3 Glacier Standard-IA Flexible Retrieval o Zone-IA Reduced Redundancy Storage come classe di archiviazione.

Note

L'operazione di copia per gli oggetti ripristinati non è supportata nella console Amazon S3 per oggetti nelle classi di storage Recupero flessibile Amazon S3 Glacier o S3 Glacier Deep Archive. Per questo tipo di operazione di copia, utilizzate (), gli SDK o l'API REST. AWS Command Line Interface AWS CLI AWS

Gli oggetti conservati nelle classi di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive sono visibili e disponibili solo tramite Amazon S3. Non sono disponibili tramite il servizio Amazon Glacier separato.

Questi sono oggetti Amazon S3 e puoi accedervi solo utilizzando la console Amazon S3 o l'API Amazon S3. Non è possibile accedere agli oggetti archiviati tramite la console Amazon Glacier separata o l'API di Amazon Glacier.

Considerazioni sui costi

Se si intendono archiviare dati con accesso non frequente per un periodo di mesi o anni, le classi di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive consentono di ridurre i costi di archiviazione. Tuttavia, è consigliabile considerare quanto segue per assicurarsi che la classe di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive sia la scelta appropriata:

- **Costi generali di archiviazione** – Quando esegui la transizione di oggetti alla classe di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, una quantità fissa di spazio di archiviazione viene aggiunta a ogni oggetto per poter conservare i metadati per la gestione dell'oggetto.
- Per ogni oggetto archiviato in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, Amazon S3 utilizzerà 8 KB di spazio di archiviazione per il nome dell'oggetto e gli altri metadati. Amazon S3 memorizza questi metadati per consentire di generare tramite l'API Amazon S3 un elenco in tempo reale degli oggetti archiviati. Per ulteriori informazioni, consulta [Get Bucket \(List Objects\)](#). Questo spazio di archiviazione aggiuntivo viene addebitato secondo le tariffe di S3 Standard.
- Per ogni oggetto archiviato in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, Amazon S3 aggiungerà 32 KB di spazio di archiviazione per l'indice e i metadati correlati. Questi dati aggiuntivi sono necessari per identificare e ripristinare l'oggetto desiderato. Questo spazio di archiviazione aggiuntivo viene addebitato secondo le tariffe di S3 Glacier Flexible Retrieval o di S3 Glacier Deep Archive.

Per l'archiviazione di oggetti di piccole dimensioni, tenere presenti questi costi di storage. Per ridurre i costi aggiuntivi, si possono aggregare diversi oggetti di piccole dimensioni in un numero più contenuto di oggetti di grandi dimensioni.

- **Numero di giorni pianificati per conservare gli oggetti archiviati** – S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive sono soluzioni di archiviazione a lungo termine. Il periodo minimo di archiviazione è di 90 giorni per la classe di archiviazione S3 Glacier Flexible Retrieval e 180 giorni

per S3 Glacier Deep Archive. L'eliminazione dei dati archiviati in Amazon Glacier è gratuita se gli oggetti eliminati sono archiviati per un tempo superiore al periodo di archiviazione minimo. Se elimini o sovrascrivi un oggetto archiviato entro il periodo di durata minimo, Amazon S3 addebita una tariffa ripartita proporzionalmente di eliminazione anticipata. Per informazioni sulla tariffa di eliminazione anticipata, consulta “Come viene addebitata l'eliminazione di oggetti da Amazon Glacier archiviati da meno di 90 giorni?” nelle [Domande frequenti su Amazon S3](#).

- Costi della richiesta di transizione a S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive – Ogni oggetto che viene trasferito nelle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive costituisce una richiesta di transizione. È previsto un costo per ognuna di queste richieste. Se si ha intenzione di trasferire un elevato numero di oggetti, i costi di richiesta vanno tenuti in considerazione. Se si archivia una combinazione di oggetti che include oggetti di piccole dimensioni, in particolare quelli inferiori a 128 KB, si consiglia di utilizzare il filtro per le dimensioni degli oggetti del ciclo di vita per escludere gli oggetti di piccole dimensioni dalla transizione e ridurre i costi delle richieste.
- Costi di ripristino dei dati da S3 Glacier e S3 Glacier Deep Archive – S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive sono progettati per l'archiviazione a lungo termine di dati ad accesso non frequente. Per informazioni sui costi di ripristino dei dati, consulta “Quanto costa recuperare i dati da Amazon Glacier?” nelle [Domande frequenti su Amazon S3](#). Per informazioni su come ripristinare i dati da Amazon Glacier, consulta [Ripristino di un oggetto archiviato](#).

Note

Il ciclo di vita S3 esegue la transizione degli oggetti in modalità asincrona a Recupero flessibile S3 Glacier e S3 Glacier Deep Archive. Potrebbe esserci un ritardo tra la data di trasferimento nella regola di configurazione del ciclo di vita S3 e la data del trasferimento fisico. Ti verrà addebitata la tariffa della classe di storage di destinazione (S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive) a partire dalla data in cui la regola del ciclo di vita è soddisfatta, anche se la transizione fisica non è ancora avvenuta. A questo punto iniziano anche i costi minimi per la durata di archiviazione (90 giorni per S3 Glacier Flexible Retrieval, 180 giorni per S3 Glacier Deep Archive) e il sovraccarico di archiviazione per oggetto (40 KB in totale, di cui 8 KB addebitati alle tariffe S3 Standard e 32 KB alla tariffa Glacier di destinazione). L'unica eccezione sono le transizioni a S3, in cui le modifiche alla fatturazione avvengono dopo il completamento della transizione fisica. Intelligent-Tiering Per ulteriori informazioni, consulta [Modifiche nella fatturazione](#).

Nella pagina dei dettagli del prodotto Amazon S3 sono disponibili informazioni sui prezzi ed esempi di calcolo per l'archiviazione di oggetti di Amazon S3. Per ulteriori informazioni, consulta i seguenti argomenti:

- “Come vengono calcolati i costi di archiviazione per gli oggetti di Amazon S3 archiviati in Amazon Glacier?” nelle [Domande frequenti su Amazon S3](#).
- “Quali costi vengono addebitati per l'eliminazione di oggetti da Amazon Glacier archiviati da meno di 90 giorni?” nelle [Domande frequenti su Amazon S3](#).
- “Quanto costa recuperare dati da Amazon Glacier?” nelle [Domande frequenti su Amazon S3](#).
- [Prezzi di Amazon S3](#) per informazioni sui costi di storage per le diverse classi di storage.

Ripristino di oggetti archiviati

Gli oggetti archiviati non sono disponibili per l'accesso in tempo reale. È necessario innanzitutto avviare una richiesta di ripristino e successivamente attendere che venga resa disponibile una copia temporanea dell'oggetto per la durata specificata nella richiesta. Anche dopo avere ricevuto una copia temporanea dell'oggetto ripristinato, la classe di archiviazione dell'oggetto rimane S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Una richiesta di operazioni API [HeadObject](#) o [GetObject](#) restituirà la classe di storage Recupero flessibile S3 Glacier o S3 Glacier Deep Archive.

Note

Quando ripristini un archivio, paghi sia per l'archivio (tariffa per le classi di archiviazione S3 Glacier Flexible Retrieval [Recupero flessibile S3 Glacier] e S3 Glacier Deep Archive [Archiviazione profonda S3 Glacier]) che per una copia temporaneamente ripristinata (tariffa di archiviazione S3 Standard). Per informazioni sui prezzi, consulta [Prezzi di Amazon S3](#).

Puoi ripristinare una copia dell'oggetto a livello di programmazione oppure utilizzando la console Amazon S3. Amazon S3 elabora una sola richiesta di ripristino alla volta per oggetto. Per ulteriori informazioni, consulta [Ripristino di un oggetto archiviato](#).

Oggetti in scadenza

Puoi aggiungere azioni di scadenza a una configurazione del ciclo di vita di S3 per indicare ad Amazon S3 di eliminare gli oggetti alla fine del loro ciclo di vita. Quando un oggetto raggiunge la fine del suo ciclo di vita in base alla relativa configurazione, Amazon S3 esegue un'azione `Expiration` in base allo stato del [controllo delle versioni S3](#) in cui si trova il bucket:

- **Bucket senza versione:** Amazon S3 aggiunge l'oggetto alla coda per la rimozione e lo rimuove in modo asincrono e permanente.
- **Versioning-enabled bucket:** se la versione corrente dell'oggetto non è un indicatore di eliminazione, Amazon S3 aggiunge un indicatore di eliminazione con un ID di versione univoco. La versione corrente diventa quindi non corrente e il contrassegno di eliminazione diventa la versione corrente.
- **Versioning-suspended bucket:** Amazon S3 crea un indicatore di eliminazione con null come ID di versione. Il contrassegno di eliminazione sostituisce qualsiasi versione dell'oggetto con ID versione null nella gerarchia delle versioni: questa operazione elimina di fatto l'oggetto.

Per un bucket con versione (ovvero, con controllo delle versioni attivata o sospesa), sono diversi i fattori che governano la gestione dell'operazione `Expiration` da parte di Amazon S3. Per i bucket con controllo delle versioni abilitato o sospeso, vale quanto segue:

- La scadenza dell'oggetto si applica solo alla sua versione corrente (non ha effetto sulle versioni non correnti dell'oggetto).
- Amazon S3 non esegue alcuna operazione se sono presenti una o più versioni dell'oggetto e il contrassegno di eliminazione è la versione corrente.
- Se la versione corrente dell'oggetto è l'unica disponibile e porta anche il contrassegno di eliminazione (noto anche come contrassegno di eliminazione dell'oggetto scaduto, dove tutte le versioni degli oggetti vengono eliminate e rimane solo un contrassegno di eliminazione), Amazon S3 rimuove il contrassegno di eliminazione dall'oggetto scaduto. È possibile inoltre utilizzare l'operazione `Expiration` per indicare ad Amazon S3 di rimuovere i contrassegni di eliminazione degli oggetti scaduti. Per un esempio, consulta [Rimozione dei contrassegni di eliminazione degli oggetti scaduti in un bucket con il controllo delle versioni abilitato](#).
- È possibile utilizzare l'elemento dell'operazione `NoncurrentVersionExpiration` per indicare ad Amazon S3 di eliminare definitivamente le versioni non correnti degli oggetti. Gli oggetti eliminati non possono essere ripristinati. È possibile basare questa scadenza su un certo numero di giorni da quando gli oggetti sono diventati non correnti. Oltre al numero di giorni, è anche possibile fornire un numero massimo di versioni non correnti da conservare (tra 1 e 100). Questo valore specifica quante versioni non correnti più recenti devono esistere prima che Amazon S3 possa eseguire l'operazione associata su una determinata versione. Per specificare il numero massimo di versioni non correnti, è necessario fornire anche un elemento `Filter`. Se non si specifica un elemento `Filter`, Amazon S3 genera un errore `InvalidRequest` quando si fornisce un numero massimo di versioni non correnti. Per ulteriori informazioni sull'uso dell'elemento dell'operazione

NoncurrentVersionExpiration, consulta [the section called “Elementi per la descrizione delle operazioni nel ciclo di vita”](#).

- Amazon S3 non esegue alcuna operazione sulle versioni non correnti degli oggetti a cui è applicata la configurazione S3 Object Lock.
- Per gli oggetti con uno stato di Failed replica Pending o, Amazon S3 non intraprende alcuna azione sulle versioni correnti o non correnti degli oggetti.

Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

 Important

Un oggetto è idoneo per una sola azione del ciclo di vita di S3 al giorno. Quando più regole corrispondono, Amazon S3 applica l'azione meno costosa.

 Important

Quando una configurazione del ciclo di vita S3 contiene più regole, un oggetto può diventare idoneo a più operazioni del ciclo di vita S3 nello stesso giorno. In questi casi, Amazon S3 segue le seguenti regole generali:

- L'eliminazione permanente ha la precedenza sul trasferimento.
- Il trasferimento ha la precedenza sulla creazione dei [contrassegni di eliminazione](#).
- Quando un oggetto è idoneo sia per una transizione S3 Glacier Flexible Retrieval che per una transizione S3 Standard-IA (o S3 One Zone-IA), Amazon S3 sceglie la transizione S3 Glacier Flexible Retrieval.

Per alcuni esempi, consulta [Esempi di sovrapposizione di filtri e conflitto tra operazioni del ciclo di vita](#).

Oggetti esistenti e nuovi

Quando si aggiunge una configurazione del ciclo di vita a un bucket, le regole di configurazione si applicano sia agli oggetti esistenti sia a quelli che vengono aggiunti in un secondo momento. Se, ad esempio, si aggiunge in data odierna una regola di configurazione del ciclo di vita con un'operazione

di scadenza in base a cui gli oggetti con un prefisso specifico scadono 30 giorni dopo la creazione, Amazon S3 inserirà nella coda di eliminazione tutti gli oggetti esistenti creati da più di 30 giorni e che hanno il prefisso specificato.

Important

Non è possibile utilizzare una policy del bucket per impedire eliminazioni o transizioni in base a una regola del ciclo di vita S3. Ad esempio, anche se la policy del bucket nega tutte le azioni per tutti i principali, la configurazione di S3 Lifecycle continua a funzionare normalmente.

Tag-based filtri e valutazione dell'idoneità

S3 Lifecycle valuta quotidianamente gli oggetti rispetto ai filtri basati su tag. Quando un oggetto corrisponde a una regola di scadenza basata su tag, Amazon S3 mette in coda l'azione per l'elaborazione asincrona. Al momento dell'esecuzione, Amazon S3 rivaluta i tag correnti dell'oggetto. Se il tag di attivazione non è più presente al momento dell'esecuzione dell'azione, la scadenza non procede.

Per confermare in modo affidabile che si è verificata una scadenza prima di rimuovere il tag, attendi una notifica degli eventi del [ciclo di vita](#). Se devi evitare una scadenza prima che venga eseguito, rimuovi il tag (gli aggiornamenti dei tag hanno effetto più rapidamente delle modifiche alle regole, la cui propagazione può richiedere fino a 15 minuti).

Come individuare la data di scadenza degli oggetti

Per individuare quando è prevista la scadenza della versione corrente di un oggetto, utilizzare l'operazione API [HeadObject](#) o [GetObject](#). Queste operazioni API restituiscono intestazioni di risposta che forniscono la data e l'ora in cui la versione corrente dell'oggetto non è più inseribile nella cache.

Note

- La data di scadenza dell'oggetto e la data in cui Amazon S3 rimuove un oggetto potrebbero non coincidere. Non è previsto alcun addebito per la scadenza o il tempo di archiviazione associato a un oggetto scaduto.
- Prima di aggiornare, disabilitare o eliminare le regole del ciclo di vita, utilizza le operazioni API LIST (come [ListObjectsV2](#), [ListObjectVersions](#) e [ListMultipartUploads](#))

o [Catalogazione e analisi dei dati con Inventario S3](#) per verificare che Amazon S3 abbia effettuato la transizione e fatto scadere gli oggetti idonei in base ai casi d'uso.

Costo della durata di archiviazione minima

Se crei una regola di scadenza del ciclo di vita di S3 che causa la scadenza degli oggetti che sono rimasti nello Zone-IA storage S3 Standard-IA o S3 One per meno di 30 giorni, ti verranno addebitati 30 giorni. Se viene creata una regola di scadenza del ciclo di vita che determina la scadenza di oggetti che sono stati nella classe di archiviazione S3 Glacier Flexible Retrieval per meno di 90 giorni, verranno comunque addebitati i costi per 90 giorni. Se viene creata una regola di scadenza del ciclo di vita che determina la scadenza di oggetti che sono stati nella classe di storage S3 Glacier Deep Archive per meno di 180 giorni, verranno comunque addebitati i costi per 180 giorni.

Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Impostazione di una configurazione del ciclo di vita S3 in un bucket

Puoi impostare una configurazione del ciclo di vita di Amazon S3 su un bucket utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3. Per informazioni sulla configurazione del ciclo di vita S3, consulta [Gestione del ciclo di vita degli oggetti](#).

Note

Per visualizzare o modificare la configurazione del ciclo di vita di un bucket di directory, utilizza gli SDK o l'API REST di Amazon S3. AWS CLI AWS Per ulteriori informazioni, consulta [Operazioni con S3 Lifecycle per i bucket di directory](#).

Nella configurazione del ciclo di vita S3, si utilizzano le regole del ciclo di vita per definire le operazioni che devono essere eseguite da Amazon S3 durante il ciclo di vita di un oggetto. Ad esempio, è possibile definire regole per trasferire gli oggetti in un'altra classe di storage, archiviare gli oggetti o far scadere (eliminare) gli oggetti dopo un periodo di tempo specificato.

Considerazioni sul ciclo di vita S3

Prima di impostare una configurazione del ciclo di vita, tieni presente quanto segue:

Ritardo di propagazione della configurazione del ciclo di vita

Quando si aggiunge una configurazione del ciclo di vita S3 in un bucket, la propagazione della configurazione nuova o aggiornata a tutti i sistemi Amazon S3 viene in genere completata con un leggero ritardo. Occorrono alcuni minuti prima che la configurazione venga applicata completamente. Questo ritardo può verificarsi anche quando si elimina una configurazione del ciclo di vita S3.

Ritardo di transizione o scadenza

Esiste un ritardo tra il momento in cui una regola del ciclo di vita viene soddisfatta e il completamento dell'operazione relativa alla regola. Ad esempio, supponiamo che un set di oggetti sia scaduto in base a una regola del ciclo di vita il 1° gennaio. Anche se la regola di scadenza è stata soddisfatta il 1° gennaio, Amazon S3 potrebbe effettivamente eliminare questi oggetti solo giorni o addirittura settimane dopo. Questo ritardo si verifica perché il ciclo di vita S3 mette in coda gli oggetti per le transizioni o le scadenze in modo asincrono. Quando aggiungi o modifichi una regola del ciclo di vita, S3 Lifecycle può iniziare a elaborare gli oggetti idonei immediatamente o con un certo ritardo. Quando S3 Lifecycle crea un indicatore di eliminazione o esegue una transizione su un oggetto, il timestamp è impostato sulla mezzanotte UTC del giorno in cui è stata eseguita l'azione, indipendentemente dall'ora effettiva in cui l'azione è stata eseguita. Tuttavia, le modifiche alla fatturazione vengono in genere applicate quando la regola del ciclo di vita viene soddisfatta, anche se l'operazione non è completa. Per ulteriori informazioni, consulta [Modifiche nella fatturazione](#). Per monitorare l'effetto degli aggiornamenti effettuati dalle regole attive del ciclo di vita, consulta [the section called "Come posso monitorare le azioni intraprese dalle mie regole del ciclo di vita?"](#)

Note

Quando viene creata o modificata una regola del ciclo di vita, gli oggetti che già soddisfano i criteri di idoneità possono essere elaborati immediatamente.

Aggiornamento, disabilitazione o eliminazione delle regole del ciclo di vita

Quando una regola del ciclo di vita viene disabilitata o eliminata, dopo un breve ritardo Amazon S3 interrompe la pianificazione dell'eliminazione o del trasferimento di nuovi oggetti. Le pianificazioni degli oggetti già pianificati vengono annullate e gli oggetti non vengono eliminati né spostati.

Note

Prima di aggiornare, disabilitare o eliminare le regole del ciclo di vita, utilizza le operazioni API LIST (come [ListObjectsV2](#), [ListObjectVersions](#) e [ListMultipartUploads](#)) o [Catalogazione e analisi dei dati con Inventario S3](#) per verificare che Amazon S3 abbia effettuato la

transizione e fatto scadere gli oggetti idonei in base ai casi d'uso. Se si verificano problemi con l'aggiornamento, la disabilitazione o l'eliminazione delle regole del ciclo di vita, consulta [Risoluzione dei problemi del ciclo di vita di Amazon S3](#).

Oggetti esistenti e nuovi

Quando si aggiunge una configurazione del ciclo di vita a un bucket, le regole di configurazione si applicano sia agli oggetti esistenti sia a quelli che vengono aggiunti in un secondo momento. Se, ad esempio, si aggiunge in data odierna una regola di configurazione del ciclo di vita con un'operazione di scadenza in base a cui gli oggetti con un prefisso specifico scadono 30 giorni dopo la creazione, Amazon S3 inserirà nella coda di eliminazione tutti gli oggetti esistenti creati da più di 30 giorni e che hanno il prefisso specificato.

Monitoraggio dell'effetto delle regole del ciclo di vita

Per monitorare l'effetto degli aggiornamenti effettuati dalle regole attive del ciclo di vita, consulta [the section called “Come posso monitorare le azioni intraprese dalle mie regole del ciclo di vita?”](#)

Modifiche nella fatturazione

Potrebbe esserci un ritardo tra il momento in cui le regole di configurazione del ciclo di vita vengono soddisfatte e il momento in cui viene avviata l'operazione attivata da tali regole. Le modifiche nella fatturazione avvengono invece non appena la regola di configurazione del ciclo di vita viene soddisfatta, anche se l'operazione non è stata ancora avviata.

Per fare un esempio, dopo la scadenza dell'oggetto, il costo di storage non viene addebitato anche se l'oggetto non viene eliminato immediatamente. Allo stesso modo, non appena scade il tempo di transizione dell'oggetto, vengono addebitate le tariffe di storage Recupero flessibile S3 Glacier anche se l'oggetto non viene trasferito immediatamente alla classe di storage Recupero flessibile S3 Glacier.

Tuttavia, le transizioni del ciclo di vita verso la classe di storage Intelligent-Tiering S3 costituiscono un'eccezione. Le modifiche alla fatturazione avvengono solo dopo che l'oggetto è passato alla classe di storage S3. Intelligent-Tiering

Per le transizioni a S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, il sovraccarico di archiviazione per oggetto (40 KB per oggetto) e la durata minima dello storage (90 giorni per S3 Glacier Flexible Retrieval, 180 giorni per S3 Glacier Deep Archive) iniziano anche quando la regola

del ciclo di vita è soddisfatta, indipendentemente da quando si verifica la transizione fisica. Per ulteriori informazioni sull'overhead di storage di Glacier, vedere [Considerazioni sui costi](#)

Regole multiple o in conflitto

Quando una configurazione del ciclo di vita S3 contiene più regole, un oggetto può diventare idoneo a più operazioni del ciclo di vita S3 nello stesso giorno. In questi casi, Amazon S3 segue le seguenti regole generali:

- L'eliminazione permanente ha la precedenza sul trasferimento.
- Il trasferimento ha la precedenza sulla creazione dei [contrassegni di eliminazione](#).
- Quando un oggetto è idoneo sia per una transizione S3 Glacier Flexible Retrieval che per una transizione S3 Standard-IA (o S3 One Zone-IA), Amazon S3 sceglie la transizione S3 Glacier Flexible Retrieval.

Per alcuni esempi, consulta [Esempi di sovrapposizione di filtri e conflitto tra operazioni del ciclo di vita](#).

Come impostare una configurazione del ciclo di vita S3

Puoi impostare una configurazione del ciclo di vita di Amazon S3 su un bucket generico utilizzando la console Amazon S3, (), gli SDK o l'API REST di Amazon S3. AWS Command Line Interface AWS CLI AWS

Per informazioni su AWS CloudFormation modelli ed esempi, consulta [Lavorare con AWS CloudFormation i modelli e nella Guida per l'utente](#). [AWS::S3::Bucket](#) CloudFormation

Utilizzo della console S3

È possibile definire regole del ciclo di vita per tutti gli oggetti o un sottoinsieme di oggetti in un bucket utilizzando un prefisso condiviso (nomi di oggetti che iniziano con una stringa comune) o un tag. In una regola del ciclo di vita è possibile definire operazioni specifiche per versioni di oggetti correnti e non correnti. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Gestione del ciclo di vita degli oggetti](#)
- [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#)

Per creare una regola del ciclo di vita

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket, seleziona il nome del bucket per il quale desideri creare una regola per il ciclo di vita.
4. Scegliere la scheda Management (Gestione), quindi Create lifecycle rule (Crea regola ciclo di vita).
5. In Lifecycle rule name (Nome regola ciclo di vita) immettere un nome per la regola.

Il nome deve essere univoco all'interno del bucket.

6. Scegliere l'ambito della regola del ciclo di vita:
 - Per applicare questa regola del ciclo di vita a tutti gli oggetti con un prefisso o un tag specifico, scegliere Limita l'ambito a prefissi o tag specifici.
 - Per limitare l'ambito in base al prefisso, in Prefix (Prefisso) immettere il prefisso.
 - Per limitare l'ambito in base al tag, scegliere Add tag (Aggiungi tag) e immettere la chiave e il valore del tag.

Per ulteriori informazioni sui prefissi dei nomi oggetto, consulta [Denominazione di oggetti Amazon S3](#). Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#).

- Per applicare questa regola del ciclo di vita a tutti gli oggetti nel bucket, scegli Questa regola si applica a tutti gli oggetti nel bucket e quindi Confermo che questa regola si applica a tutti gli oggetti nel bucket.
7. Per filtrare una regola in base alle dimensioni dell'oggetto, è possibile selezionare Specifica la dimensione minima dell'oggetto, Specifica la dimensione massima dell'oggetto o entrambe le opzioni.
 - Quando si specifica un valore per Dimensione minima dell'oggetto o Dimensione massima dell'oggetto, il valore deve essere maggiore di 0 byte e massimo 50 TB. È possibile specificare questo valore in byte, KB, MB o GB.
 - Quando si specificano entrambi i valori, la dimensione massima dell'oggetto deve essere superiore alla dimensione minima dell'oggetto.

 Note

I filtri Dimensione minima dell'oggetto e Dimensione massima dell'oggetto escludono i valori specificati. Ad esempio, se si imposta un filtro per far scadere gli oggetti con una Dimensione minima dell'oggetto di 128 KB, gli oggetti la cui dimensione è esattamente 128 KB non scadono. La regola si applica invece solo agli oggetti con dimensioni superiori a 128 KB.

8. In Lifecycle rule actions (Operazioni regola ciclo di vita) scegliere le operazioni da far eseguire alla regola del ciclo di vita:

- Transizione delle versioni correnti degli oggetti tra classi di storage
- Transizione delle versioni precedenti degli oggetti tra classi di storage
- Definizione della scadenza delle versioni correnti degli oggetti

 Note

Per i bucket che non hanno il [controllo delle versioni S3](#) abilitato, la scadenza delle versioni correnti fa sì che Amazon S3 elimini definitivamente gli oggetti. Per ulteriori informazioni, consulta [the section called “Operazioni del ciclo di vita e stato della funzione Controllo delle versioni nel bucket”](#).

- Eliminazione permanente delle versioni precedenti degli oggetti
- Eliminazione dei contrassegni di eliminazione o di caricamenti in più parti incompleti

A seconda delle operazioni scelte, vengono visualizzate opzioni diverse.

9. Per eseguire la transizione delle versioni correnti degli oggetti tra classi di storage, in Transizione delle versioni correnti degli oggetti tra classi di storage procedere come segue:

- a. In Transizione a una classe di storage scegli la classe di storage in cui eseguire la transizione. Per un elenco delle possibili transizioni, consulta [the section called “Transizioni del ciclo di vita supportate”](#). È possibile scegliere tra le seguenti classi di storage:
 - S3 Standard-IA
 - S3 Intelligent-Tiering
 - S3 Uno Zone-IA

- S3 Glacier Instant Retrieval
 - S3 Glacier Flexible Retrieval
 - S3 Glacier Deep Archive
- b. In Days after object creation (Giorni dopo la creazione dell'oggetto) immettere il numero di giorni successivi alla creazione dopo i quali eseguire la transizione dell'oggetto.

Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#). È possibile definire le transizioni per la versione degli oggetti corrente o per quella precedente, oppure per entrambe le versioni: corrente e precedente. La funzione Controllo delle versioni consente di gestire più versioni di un oggetto in un unico bucket. Per ulteriori informazioni sulla funzione Controllo delle versioni, consulta [Utilizzo della console S3](#).

 Important

Quando si sceglie la classe di storage Recupero istantaneo S3 Glacier, Recupero flessibile S3 Glacier o Glacier Deep Archive, gli oggetti rimangono in Amazon S3. Non puoi accedervi direttamente tramite il servizio Amazon Glacier separato. Per ulteriori informazioni, consulta [Trasferimento degli oggetti utilizzando il ciclo di vita Amazon S3](#).

10. Per eseguire la transizione delle versioni non correnti degli oggetti tra classi di storage, in Transizione delle versioni non correnti degli oggetti tra classi di storage procedere come segue:
- a. In Transizione a una classe di storage scegli la classe di storage in cui eseguire la transizione. Per un elenco delle possibili transizioni, consulta [the section called “Transizioni del ciclo di vita supportate”](#). È possibile scegliere tra le seguenti classi di storage:
- S3 Standard-IA
 - S3 Intelligent-Tiering
 - S3 Uno Zone-IA
 - S3 Glacier Instant Retrieval
 - S3 Glacier Flexible Retrieval
 - S3 Glacier Deep Archive
- b. In Giorni dopo i quali l'oggetto diventa non corrente, immettere il numero di giorni successivi alla creazione dopo i quali eseguire la transizione dell'oggetto.

11. Per definire la scadenza delle versioni correnti degli oggetti, in *Expire current versions of objects* (Scadenza versioni attuali degli oggetti) immettere un numero di giorni in *Number of days after object creation* (Numero di giorni dopo la creazione dell'oggetto).

 Important

In un bucket senza versione l'operazione di scadenza comporta la rimozione permanente dell'oggetto da parte di Amazon S3. Per ulteriori informazioni sulle operazioni del ciclo di vita, consulta [Elementi per la descrizione delle operazioni nel ciclo di vita](#).

12. Per eliminare in modo definitivo le versioni precedenti degli oggetti, in *Permanently delete noncurrent versions of objects* (Elimina in modo definitivo le versioni non aggiornate degli oggetti), specifica il numero di giorni nel campo *Days after objects become noncurrent* (Numero di giorni dopo i quali gli oggetti non sono più aggiornati). Facoltativamente puoi specificare il numero di versioni più recenti da mantenere immettendo un valore nel campo *Number of newer versions to retain* (Numero di versioni più recenti da mantenere).
13. In *Delete expired delete markers or incomplete multipart uploads* (Elimina contrassegni di eliminazione scaduti o caricamenti in più parti incompleti) scegliere *Delete expired object delete markers* (Elimina contrassegni di eliminazione oggetti scaduti) e *Delete incomplete multipart uploads* (Elimina caricamenti in più parti incompleti). Immettere quindi il numero di giorni dopo l'avvio dei caricamenti in più parti dopo i quali si desidera terminare e pulire i caricamenti in più parti incompleti.

Per ulteriori informazioni sui caricamenti in più parti, consultare [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

14. Scegli Crea regola.

Se la regola non contiene errori, Amazon S3 la abilita ed è possibile visualizzarla nella scheda Management (Gestione) in Lifecycle rules (Regole ciclo di vita).

Utilizzo di AWS CLI

È possibile utilizzare i seguenti AWS CLI comandi per gestire le configurazioni del ciclo di vita di S3:

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

Per istruzioni sulla configurazione di AWS CLI, consulta [Developing with Amazon S3 using the AWS CLI](#) nell'Amazon S3 API Reference.

La configurazione del ciclo di vita di Amazon S3 è un file XML. Tuttavia, quando si utilizza il formato XML AWS CLI, non è possibile specificare il formato XML. È necessario invece specificare il formato JSON. Di seguito sono riportati alcuni esempi di configurazioni del ciclo di vita XML e le configurazioni JSON equivalenti che è possibile specificare in un comando. AWS CLI

Prendiamo in considerazione la configurazione del ciclo di vita S3 di esempio riportata di seguito:

Example Esempio 1

Example

XML

```
<LifecycleConfiguration>
  <Rule>
    <ID>ExampleRule</ID>
    <Filter>
      <Prefix>documents/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

JSON

```
{
  "Rules": [
    {
      "Filter": {
        "Prefix": "documents/"
      },
      "Status": "Enabled",
```

```
    "Transitions": [  
      {  
        "Days": 365,  
        "StorageClass": "GLACIER"  
      }  
    ],  
    "Expiration": {  
      "Days": 3650  
    },  
    "ID": "ExampleRule"  
  }  
]  
}
```

Example Esempio 2

Example

XML

```
<LifecycleConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">  
  <Rule>  
    <ID>id-1</ID>  
    <Expiration>  
      <Days>1</Days>  
    </Expiration>  
    <Filter>  
      <And>  
        <Prefix>myprefix</Prefix>  
        <Tag>  
          <Key>mytagkey1</Key>  
          <Value>mytagvalue1</Value>  
        </Tag>  
        <Tag>  
          <Key>mytagkey2</Key>  
          <Value>mytagvalue2</Value>  
        </Tag>  
      </And>  
    </Filter>  
    <Status>Enabled</Status>  
  </Rule>  
</LifecycleConfiguration>
```

JSON

```
{
  "Rules": [
    {
      "ID": "id-1",
      "Filter": {
        "And": {
          "Prefix": "myprefix",
          "Tags": [
            {
              "Value": "mytagvalue1",
              "Key": "mytagkey1"
            },
            {
              "Value": "mytagvalue2",
              "Key": "mytagkey2"
            }
          ]
        }
      },
      "Status": "Enabled",
      "Expiration": {
        "Days": 1
      }
    }
  ]
}
```

È possibile testare il codice `put-bucket-lifecycle-configuration` nel modo seguente:

Per testare la configurazione

1. Salvare la configurazione del ciclo di vita JSON in un file (ad esempio, *lifecycle.json*).
2. Esegui il AWS CLI comando seguente per impostare la configurazione del ciclo di vita sul tuo bucket. Sostituisci *user input placeholders* con le informazioni appropriate.

```
$ aws s3api put-bucket-lifecycle-configuration \
--bucket amzn-s3-demo-bucket \
--lifecycle-configuration file://lifecycle.json
```


3. Per verificare, recupera la configurazione del ciclo di vita di S3 utilizzando il comando come segue: `get-bucket-lifecycle-configuration` AWS CLI

```
$ aws s3api get-bucket-lifecycle-configuration \
--bucket amzn-s3-demo-bucket
```

4. Per eliminare la configurazione di S3 Lifecycle, utilizzate il comando come segue: `delete-bucket-lifecycle` AWS CLI

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

Utilizzo di AWS SDK

Java

Puoi utilizzare l' AWS SDK per Java per gestire la configurazione del ciclo di vita S3 di un bucket. Per ulteriori informazioni sulla gestione della configurazione del ciclo di vita S3, consulta [Gestione del ciclo di vita degli oggetti](#).

Note

Quando si aggiunge una configurazione del ciclo di vita S3 a un bucket, Amazon S3 sostituisce l'attuale configurazione del ciclo di vita del bucket, se presente. Per aggiornare una configurazione, la si recupera, si apportano le modifiche desiderate e successivamente si aggiunge la configurazione aggiornata al bucket.

Per gestire la configurazione del ciclo di vita utilizzando l'SDK per Java, puoi AWS :

- Aggiungere la configurazione del ciclo di vita a un bucket.
- Recuperare la configurazione del ciclo di vita e aggiornarla aggiungendo un'altra regola.
- Aggiungere la configurazione del ciclo di vita modificata al bucket. Amazon S3 sostituisce la configurazione esistente.
- Recuperare nuovamente la configurazione e verificare che contenga il numero corretto di regole stampando il numero di regole.
- Eliminare la configurazione del ciclo di vita e verificare che sia stata eliminata cercando di recuperarla nuovamente.

Per esempi di come impostare la configurazione del ciclo di vita su un bucket con l' AWS SDK per Java, consulta [Impostare la configurazione del ciclo di vita su un bucket nell'API Reference di Amazon S3](#).

.NET

Puoi utilizzare per gestire la configurazione del ciclo di vita di S3 AWS SDK per .NET su un bucket. Per ulteriori informazioni sulla gestione della configurazione del ciclo di vita, consulta [Gestione del ciclo di vita degli oggetti](#).

Note

Quando aggiungi una configurazione del ciclo di vita, Amazon S3 sostituisce la configurazione esistente in un bucket specifico. Per aggiornare una configurazione del ciclo di vita esistente, è necessario prima di tutto recuperare la configurazione del ciclo di vita, apportare le modifiche e successivamente aggiungerla nel bucket.

L'esempio seguente mostra come utilizzare la configurazione del ciclo AWS SDK per .NET di vita di un bucket per aggiungere, aggiornare ed eliminare. L'esempio di codice esegue quanto segue:

- Aggiunge una configurazione del ciclo di vita a un bucket
- Recupera la configurazione del ciclo di vita e la aggiorna aggiungendo un'altra regola.
- Aggiunge la configurazione del ciclo di vita modificata al bucket. Amazon S3 sostituisce la configurazione del ciclo di vita esistente.
- Recupera nuovamente la configurazione e la verifica stampando il numero di regole nella configurazione.
- Elimina la configurazione del ciclo di vita e verifica l'eliminazione.

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Nozioni di base su AWS SDK per .NET](#) nella Guida per gli sviluppatori di AWS SDK per .NET .

```
using Amazon;  
using Amazon.S3;  
using Amazon.S3.Model;  
using System;  
using System.Collections.Generic;  
using System.Threading.Tasks;
```

```

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List<LifecycleRule>
                    {
                        new LifecycleRule
                        {
                            Id = "Archive immediately rule",
                            Filter = new LifecycleFilter()
                            {
                                LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                {
                                    Prefix = "glacierobjects/"
                                }
                            },
                            Status = LifecycleRuleStatus.Enabled,
                            Transitions = new List<LifecycleTransition>
                            {
                                new LifecycleTransition
                                {
                                    Days = 0,
                                    StorageClass = S3StorageClass.Glacier
                                }
                            },
                        },
                    },
                },
            }
        }
    }
}

```

```

        new LifecycleRule
        {
            Id = "Archive and then delete rule",
            Filter = new LifecycleFilter()
            {
                LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                {
                    Prefix = "projectdocs/"
                }
            },
            Status = LifecycleRuleStatus.Enabled,
            Transitions = new List<LifecycleTransition>
            {
                new LifecycleTransition
                {
                    Days = 30,
                    StorageClass =
S3StorageClass.StandardInfrequentAccess
                },
                new LifecycleTransition
                {
                    Days = 365,
                    StorageClass = S3StorageClass.Glacier
                }
            },
            Expiration = new LifecycleRuleExpiration()
            {
                Days = 3650
            }
        }
    };

    // Add the configuration to the bucket.
    await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

    // Retrieve an existing configuration.
    lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

    // Add a new rule.
    lifeCycleConfiguration.Rules.Add(new LifecycleRule
    {

```

```
        Id = "NewRule",
        Filter = new LifecycleFilter()
        {
            LifecycleFilterPredicate = new LifecyclePrefixPredicate()
            {
                Prefix = "YearlyDocuments/"
            }
        },
        Expiration = new LifecycleRuleExpiration()
        {
            Days = 3650
        }
    });

    // Add the configuration to the bucket.
    await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

    // Verify that there are now three rules.
    lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
    Console.WriteLine("Expected # of rulest=3; found:{0}",
lifeCycleConfiguration.Rules.Count);

    // Delete the configuration.
    await RemoveLifecycleConfigAsync(client);

    // Retrieve a nonexistent configuration.
    lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

}
catch (AmazonS3Exception e)
{
    Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
}
catch (Exception e)
{
    Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
}

}

static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
```

```

    {

        PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
        {
            BucketName = bucketName,
            Configuration = configuration
        };
        var response = await client.PutLifecycleConfigurationAsync(request);
    }

    static async Task<LifecycleConfiguration>
RetrieveLifecycleConfigAsync(IAmazonS3 client)
    {
        GetLifecycleConfigurationRequest request = new
GetLifecycleConfigurationRequest
        {
            BucketName = bucketName
        };
        var response = await client.GetLifecycleConfigurationAsync(request);
        var configuration = response.Configuration;
        return configuration;
    }

    static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
    {
        DeleteLifecycleConfigurationRequest request = new
DeleteLifecycleConfigurationRequest
        {
            BucketName = bucketName
        };
        await client.DeleteLifecycleConfigurationAsync(request);
    }
}
}

```

Ruby

È possibile utilizzare AWS SDK per Ruby per gestire una configurazione del ciclo di vita S3 su un bucket utilizzando la classe. [AWS::S3::BucketLifecycleConfiguration](#) Per ulteriori informazioni sulla gestione della configurazione del ciclo di vita S3, consulta [Gestione del ciclo di vita degli oggetti](#).

Utilizzo della REST API

Gli argomenti seguenti della Documentazione di riferimento delle API di Amazon Simple Storage Service descrivono le operazioni REST API correlate alla configurazione del ciclo di vita S3:

- [PutBucketLifecycleConfiguration](#)
- [GetBucketLifecycleConfiguration](#)
- [DeleteBucketLifecycle](#)

Risoluzione dei problemi relativi al ciclo di vita di S3

Per i problemi comuni che potrebbero verificarsi durante l'utilizzo del ciclo di vita S3, consulta [the section called “Risoluzione dei problemi del ciclo di vita”](#).

Come il ciclo di vita S3 interagisce con altre configurazioni del bucket

Oltre a quelle del ciclo di vita S3, è possibile associare altre configurazioni al bucket. In questa sezione viene descritto in che modo la configurazione del ciclo di vita S3 è correlata alle altre configurazioni del bucket.

Ciclo di vita S3 e controllo delle versioni S3

Le configurazioni del ciclo di vita S3 possono essere aggiunte a bucket senza versione e a quelli che supportano la funzione Controllo delle versioni. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Un bucket che supporta la funzione Controllo delle versioni mantiene una versione dell'oggetto corrente e zero o più versioni dell'oggetto non correnti. È possibile definire regole del ciclo di vita separate per le versioni dell'oggetto correnti e non correnti.

Per ulteriori informazioni, consulta [Elementi della configurazione del ciclo di vita](#).

Important

Quando una configurazione del ciclo di vita S3 contiene più regole, un oggetto può diventare idoneo a più operazioni del ciclo di vita S3 nello stesso giorno. In questi casi, Amazon S3 segue le seguenti regole generali:

- L'eliminazione permanente ha la precedenza sul trasferimento.

- Il trasferimento ha la precedenza sulla creazione dei [contrassegni di eliminazione](#).
- Quando un oggetto è idoneo sia per una transizione S3 Glacier Flexible Retrieval che per una transizione S3 Standard-IA (o S3 One Zone-IA), Amazon S3 sceglie la transizione S3 Glacier Flexible Retrieval.

Per alcuni esempi, consulta [Esempi di sovrapposizione di filtri e conflitto tra operazioni del ciclo di vita](#).

S3 Lifecycle e S3 Replication

Quando sono abilitati sia S3 Replication che S3 Lifecycle su un bucket, S3 Lifecycle blocca le azioni di scadenza e transizione sugli oggetti con o stato di replica. PENDING FAILED Ciò garantisce che Lifecycle non agisca sugli oggetti finché non sono stati replicati correttamente nel bucket di destinazione.

Gli oggetti passano allo stato di FAILED replica per problemi quali la mancanza delle autorizzazioni dei ruoli di replica, delle autorizzazioni AWS Key Management Service (AWS KMS) o delle autorizzazioni del bucket. Per ulteriori informazioni, consulta [Risoluzione dei problemi nella replica](#).

Gli oggetti con stato di FAILED replica continueranno a sostenere costi di storage anche dopo la data di scadenza del ciclo di vita o di idoneità alla transizione fino alla risoluzione del problema di replica. Una volta corretta la configurazione di replica sottostante o le autorizzazioni IAM, i nuovi oggetti verranno replicati automaticamente. Tuttavia, gli oggetti che hanno già lo stato di FAILED replica non verranno ripetuti automaticamente: è necessario utilizzare S3 Batch Replication per replicarli o eliminarli utilizzando S3 Batch Operations con se non sono più necessari. AWS Lambda Una volta completata la replica (o l'eliminazione) degli oggetti, Lifecycle riprenderà a elaborarli in base alle regole configurate. Per identificare gli oggetti con stato di FAILED replica, puoi utilizzare Amazon CloudWatch metrics (OperationFailedReplication) per monitorare il numero di errori e le tendenze a livello di bucket oppure utilizzare i report di Amazon S3 Inventory, l'API Amazon S3 (orGetObject) HeadObject o Amazon S3 Event Notifications per i dettagli a livello di oggetto.

MFA-enabled Configurazione del ciclo di vita S3 sui bucket

La configurazione del ciclo di vita S3 su bucket configurati per l'autenticazione a più fattori non è supportata. Per ulteriori informazioni, consulta [Configurazione dell'eliminazione di MFA](#).

Ciclo di vita S3 e registrazione

Le azioni del ciclo di vita di Amazon S3 non vengono acquisite dalla registrazione a livello di oggetto. AWS CloudTrail acquisisce le richieste API effettuate agli endpoint Amazon S3 esterni, mentre le azioni del ciclo di vita di S3 vengono eseguite utilizzando endpoint interni di Amazon S3.

Puoi abilitare i log di accesso al server Amazon S3 in un bucket S3 per acquisire Lifecycle-related azioni S3, come le transizioni di oggetti verso un'altra classe di storage e le scadenze degli oggetti che comportano l'eliminazione permanente o l'eliminazione logica. Per ulteriori informazioni, consulta [the section called “Registrazione dell'accesso al server”](#).

Se nel bucket è abilitata la registrazione, i log di accesso al server Amazon S3 segnalano i risultati delle seguenti operazioni:

Log dell'operazione	Description
S3.EXPIRE.OBJECT	Amazon S3 elimina in modo definitivo l'oggetto a causa dell'operazione <code>Expiration</code> del ciclo di vita.
S3.CREATE.DELETEMARKER	Amazon S3 elimina in maniera logica la versione corrente e aggiunge un contrassegno di eliminazione in un bucket con la funzionalità Controllo delle versioni abilitata.
S3.TRANSITION_SIA.OBJECT	Amazon S3 effettua la transizione dell'oggetto nella classe di storage S3. Standard-IA
S3.TRANSITION_ZIA.OBJECT	Amazon S3 effettua la transizione dell'oggetto nella classe di storage S3 One. Zone-IA
S3.TRANSITION_INT.OBJECT	Amazon S3 effettua la transizione dell'oggetto nella classe di storage S3. Intelligent-Tiering
S3.TRANSITION_GIR.OBJECT	Amazon S3 avvia il trasferimento dell'oggetto nella classe di storage Recupero istantaneo S3 Glacier.

Log dell'operazione	Description
S3.TRANSITION.OBJECT	Amazon S3 avvia il trasferimento dell'oggetto nella classe di storage Recupero flessibile S3 Glacier.
S3.TRANSITION_GDA.OBJECT	Amazon S3 avvia il trasferimento dell'oggetto nella classe di storage S3 Glacier Deep Archive.
S3.DELETE.UPLOAD	Amazon S3 interrompe un caricamento in più parti incompleto.

Note

I record dei log di accesso al server Amazon S3 sono inviati nel miglior modo possibile e non possono essere utilizzati per un resoconto completo di tutte le richieste di Amazon S3.

Configurazione delle notifiche di eventi del ciclo di vita S3

Per ricevere una notifica quando Amazon S3 elimina un oggetto o lo trasferisce a un'altra classe di storage Amazon S3 in seguito al rispetto di una regola del ciclo di vita S3, è possibile configurare una notifica di eventi Amazon S3.

È possibile ricevere notifiche per i seguenti eventi del ciclo di vita S3:

- **Eventi di transizione:** utilizzando il tipo di evento `s3:LifecycleTransition` è possibile ricevere una notifica quando un oggetto viene trasferito da una classe di storage Amazon S3 a un'altra mediante una configurazione del ciclo di vita S3.
- **Eventi di scadenza (eliminazione):** con i tipi di evento `LifecycleExpiration`, è possibile ricevere una notifica ogni volta che Amazon S3 elimina un oggetto in base alla configurazione del ciclo di vita S3.

Esistono due tipi di eventi di scadenza:

- Il tipo di evento `s3:LifecycleExpiration:Delete` notifica quando viene eliminato un oggetto in un bucket senza versione. `s3:LifecycleExpiration:Delete` notifica inoltre

quando una versione dell'oggetto viene eliminata definitivamente da una configurazione del ciclo di vita S3.

- Il tipo di evento `s3:LifecycleExpiration:DeleteMarkerCreated` notifica quando il ciclo di vita S3 crea un contrassegno di eliminazione dopo l'eliminazione di una versione corrente di un oggetto in un bucket con versione. S3 Lifecycle imposta l'ora di creazione del marker di eliminazione alle 00:00 UTC (mezzanotte) del giorno corrente. L'ora di creazione potrebbe differire dall'ora dell'evento nella notifica `s3:LifecycleExpiration:DeleteMarkerCreated` inviata da S3. Per ulteriori informazioni, consulta [the section called "Eliminazione di versioni di un oggetto"](#).

Amazon S3 può pubblicare notifiche di eventi su un argomento Amazon Simple Notification Service (Amazon SNS), una coda Amazon Simple Queue Service (Amazon SQS) o una funzione. AWS Lambda Per ulteriori informazioni, consulta [Notifiche di eventi Amazon S3](#).

Per istruzioni su come configurare le notifiche di eventi di Amazon S3, consulta [Abilitare le notifiche di eventi utilizzando Amazon SQS, Amazon SNS e AWS Lambda](#)

Quello che segue è un esempio di un messaggio inviato da Amazon S3 per pubblicare un evento `s3:LifecycleExpiration:Delete`. Per ulteriori informazioni, consulta [the section called "Struttura del messaggio di evento"](#).

```
{
  "Records": [
    {
      "eventVersion": "2.3",
      "eventSource": "aws:s3",
      "awsRegion": "us-west-2",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "LifecycleExpiration:Delete",
      "userIdentity": {
        "principalId": "s3.amazonaws.com"
      },
      "requestParameters": {
        "sourceIPAddress": "s3.amazonaws.com"
      },
      "responseElements": {
        "x-amz-request-id": "C3D13FE58DE4C810",
        "x-amz-id-2": "FMjUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvAN0jpD"
      },
    },
  ],
}
```

```

"s3":{
  "s3SchemaVersion":"1.0",
  "configurationId":"testConfigRule",
  "bucket":{
    "name":"amzn-s3-demo-bucket",
    "ownerIdentity":{
      "principalId":"A3NL1K0ZZKExample"
    },
    "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
  },
  "object":{
    "key":"expiration/delete",
    "sequencer":"0055AED6DCD90281E5",
  }
}
}
]
}

```

I messaggi inviati da Amazon S3 per pubblicare un evento `s3:LifecycleTransition` includono anche le seguenti informazioni:

```

"lifecycleEventData":{
  "transitionEventData": {
    "destinationStorageClass": the destination storage class for the object
  }
}

```

Elementi della configurazione del ciclo di vita

Una configurazione del ciclo di vita S3 è formata da regole che includono diversi elementi che descrivono le azioni che Amazon S3 esegue durante l'intero ciclo di vita di un oggetto. A ogni bucket S3 può essere assegnata una configurazione del ciclo di vita, che può contenere fino a 1.000 regole. La configurazione del ciclo di vita di Amazon S3 viene specificata in formato XML e consiste in una o più regole del ciclo di vita, dove ogni regola è composta da uno o più elementi.

```

<LifecycleConfiguration>
  <Rule>
    <Element>
  </Rule>
  <Rule>

```

```
<Element>
  <Element>
    </Rule>
  </LifecycleConfiguration>
```

Ogni regola è costituita dagli elementi seguenti:

- Metadati della regola tra cui l'ID, nonché uno stato che indica se la regola è abilitata o disabilitata. Se una regola è disabilitata, Amazon S3 non esegue le operazioni in essa specificate.
- Filtro che identifica gli oggetti a cui si applica la regola. È possibile specificare un filtro utilizzando la dimensione dell'oggetto, il prefisso della chiave dell'oggetto, uno o più tag di oggetto oppure una combinazione di filtri.
- Una o più operazioni di transizione o scadenza con una data o un periodo nel ciclo di vita dell'oggetto in cui si desidera che Amazon S3 esegua l'operazione specificata.

Argomenti

- [Elemento ID](#)
- [Elemento Status](#)
- [Elemento Filter](#)
- [Elementi per la descrizione delle operazioni nel ciclo di vita](#)
- [Aggiunta di filtri alle regole del ciclo di vita](#)

Le sezioni che seguono descrivono gli elementi XML contenuti in una configurazione del ciclo di vita S3. Per gli esempi di configurazione, consulta [Esempi di configurazioni del ciclo di vita S3](#).

Elemento ID

Le configurazioni del ciclo di vita sono definite a livello di bucket e ciascun bucket ha una propria configurazione specifica. Una configurazione del ciclo di vita S3 può contenere fino a 1.000 regole per bucket. Questo limite non è regolabile. L'elemento <ID> identifica in modo univoco una regola all'interno della configurazione del ciclo di vita di un bucket. La lunghezza dell'ID è limitata a 255 caratteri.

Elemento Status

Il valore dell'elemento <Status> può essere Enabled o Disabled. Se una regola è disabilitata, Amazon S3 non esegue nessuna delle operazioni in essa definite.

Elemento Filter

Una regola del ciclo di vita S3 può essere valida per tutti gli oggetti di un bucket o solo per un sottoinsieme in base all'elemento `<Filter>` specificato nella regola.

È possibile filtrare gli oggetti per prefisso della chiave, tag dell'oggetto o una combinazione di entrambi (in tal caso, Amazon S3 utilizza un operatore logico AND per combinare i filtri). Per ulteriori informazioni ed esempi sui filtri, consulta [Aggiunta di filtri alle regole del ciclo di vita](#).

- Definizione di un filtro tramite prefissi della chiave: questo esempio illustra una regola del ciclo di vita S3 valida per un sottoinsieme di oggetti in base al prefisso del nome della chiave (`logs/`). Ad esempio, la regola del ciclo di vita è valida per gli oggetti `logs/mylog.txt`, `logs/temp1.txt` e `logs/test.txt`, ma non per l'oggetto `example.jpg`.

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    transition/expiration actions
    ...
  </Rule>
  ...
</LifecycleConfiguration>
```

Per applicare un'operazione per il ciclo di vita a un sottoinsieme di oggetti in base a diversi prefissi del nome della chiave, specificare regole separate e, all'interno di ognuna, specificare un filtro basato sul prefisso. Ad esempio, per descrivere un'operazione per il ciclo di vita per oggetti con prefissi della chiave `projectA/` e `projectB/`, vanno specificate due regole, come illustrato di seguito:

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <Prefix>projectA/</Prefix>
    </Filter>
    transition/expiration actions
    ...
  </Rule>

  <Rule>
```

```

    <Filter>
      <Prefix>projectB/</Prefix>
    </Filter>
    transition/expiration actions
    ...
  </Rule>
</LifecycleConfiguration>

```

Per ulteriori informazioni sulle chiavi degli oggetti, consulta [Denominazione di oggetti Amazon S3](#).

- Definizione di un filtro in base ai tag dell'oggetto: nell'esempio che segue la regola del ciclo di vita specifica un filtro basato su un tag (*key*) e un valore (*value*). La regola si applica quindi solo a un sottoinsieme di oggetti con quel tag specifico.

```

<LifecycleConfiguration>
  <Rule>
    <Filter>
      <Tag>
        <Key>key</Key>
        <Value>value</Value>
      </Tag>
    </Filter>
    transition/expiration actions
    ...
  </Rule>
</LifecycleConfiguration>

```

È possibile specificare un filtro basato su più tag. È necessario racchiudere i tag nell'elemento `<And>` illustrato nell'esempio che segue. La regola indica ad Amazon S3 di eseguire le operazioni del ciclo di vita sugli oggetti con due tag (con la specifica combinazione di chiave e valore).

```

<LifecycleConfiguration>
  <Rule>
    <Filter>
      <And>
        <Tag>
          <Key>key1</Key>
          <Value>value1</Value>
        </Tag>
        <Tag>
          <Key>key2</Key>
          <Value>value2</Value>
        </Tag>
      </And>
    </Filter>
    transition/expiration actions
    ...
  </Rule>
</LifecycleConfiguration>

```

```

        </Tag>
        ...
    </And>
</Filter>
    transition/expiration actions
</Rule>
</Lifecycle>

```

La regola del ciclo di vita si applica agli oggetti che contengono entrambi i tag specificati. Amazon S3 esegue un'operazione logica AND. Tenere presente quanto segue:

- Ogni tag deve corrispondere esattamente sia alla chiave che al valore. Se si specifica solo un elemento `<Key>` e nessun elemento `<Value>`, la regola verrà applicata solo agli oggetti che corrispondono alla chiave del tag e che non hanno un valore specificato.
- La regola si applica a un sottoinsieme di oggetti che ha tutti i tag specificati nella regola. Se a un oggetto sono specificati tag aggiuntivi, la regola verrà comunque applicata.

Note

Quando si specificano più tag in un filtro, ogni chiave del tag deve essere univoca.

- Definizione di un filtro in base al prefisso e a uno o più tag: in una regola del ciclo di vita è possibile specificare un filtro in base al prefisso della chiave e a uno o più tag. Anche in questo caso, è necessario racchiudere tutti gli elementi del filtro nell'elemento `<And>`, come illustrato di seguito.

```

<LifecycleConfiguration>
  <Rule>
    <Filter>
      <And>
        <Prefix>key-prefix</Prefix>
        <Tag>
          <Key>key1</Key>
          <Value>value1</Value>
        </Tag>
        <Tag>
          <Key>key2</Key>
          <Value>value2</Value>
        </Tag>
        ...
      </And>
    </Filter>

```



```

    <Status>Enabled</Status>
    transition/expiration actions
  </Rule>
</LifecycleConfiguration>

```

Amazon S3 combina questi filtri tramite l'operatore logico AND. In altre parole, la regola si applica al sottoinsieme di oggetti con il prefisso della chiave e i tag specificati. Un filtro può avere un solo prefisso e zero o più tag.

- È possibile specificare un filtro vuoto, nel qual caso la regola si applica a tutti gli oggetti nel bucket.

```

<LifecycleConfiguration>
  <Rule>
    <Filter>
    </Filter>
    <Status>Enabled</Status>
    transition/expiration actions
  </Rule>
</LifecycleConfiguration>

```

- Per filtrare una regola per dimensione oggetto, è possibile specificare una dimensione minima (ObjectSizeGreaterThan) o massima (ObjectSizeLessThan) oppure è possibile specificare un intervallo di dimensioni degli oggetti.

I valori delle dimensioni degli oggetti sono espressi in byte. Per impostazione predefinita, gli oggetti di dimensioni inferiori a 128 KB non verranno trasferiti in nessuna classe di storage, a meno che non si specifichi una dimensione minima inferiore (ObjectSizeGreaterThan) o una dimensione massima (ObjectSizeLessThan). Per ulteriori informazioni, consulta [Esempio: Consentire la transizione di oggetti di dimensioni inferiori a 128 KB](#).

```

    <LifecycleConfiguration>
  <Rule>
    <Filter>
      <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
    </Filter>
    <Status>Enabled</Status>
    transition/expiration actions
  </Rule>
</LifecycleConfiguration>

```

Note

I filtri `ObjectSizeGreaterThan` e `ObjectSizeLessThan` escludono i valori specificati. Ad esempio, se imposti oggetti di dimensioni comprese tra 128 KB e 1024 KB per passare dalla classe di archiviazione S3 Standard alla classe di archiviazione S3 Standard-IA, gli oggetti che sono esattamente 1024 KB e 128 KB non passeranno a S3. Standard-IA La regola si applicherà invece solo agli oggetti con dimensioni superiori a 128 KB e inferiori a 1024 KB.

Se stai specificando un intervallo di dimensioni degli oggetti, il numero intero `ObjectSizeGreaterThan` deve essere minore del valore `ObjectSizeLessThan`. Quando si utilizzano più filtri, è necessario racchiudere i filtri in un elemento `<And>`. L'esempio seguente illustra come specificare gli oggetti in un intervallo compreso tra 500 e 64.000 byte.

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <And>
        <Prefix>key-prefix</Prefix>
        <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        <ObjectSizeLessThan>64000</ObjectSizeLessThan>
      </And>
    </Filter>
    <Status>Enabled</Status>
    transition/expiration actions
  </Rule>
</LifecycleConfiguration>
```

Elementi per la descrizione delle operazioni nel ciclo di vita

È possibile indicare ad Amazon S3 di eseguire operazioni specifiche nel ciclo di vita di un oggetto specificando in una regola del ciclo di vita S3 una o più delle seguenti operazioni predefinite, il cui effetto dipende dallo stato della funzione Controllo delle versioni del bucket.

- Elemento dell'operazione **Transition**: l'operazione `Transition` viene impostata per trasferire gli oggetti da una classe di storage a un'altra. Per ulteriori informazioni sul trasferimento degli

oggetti, consulta [Transizioni supportate](#). Al raggiungimento di una data o di un periodo nel ciclo di vita dell'oggetto, Amazon S3 esegue la transizione.

Per un bucket con versione (bucket con funzione Controllo delle versioni attivata o sospesa), l'operazione Transition si applica alla versione corrente dell'oggetto. Per la gestione delle versioni non correnti, Amazon S3 definisce l'operazione NoncurrentVersionTransition (descritta di seguito in questo argomento).

- Elemento dell'operazione **Expiration**: l'operazione Expiration definisce la scadenza degli oggetti identificati nella regola e viene applicata agli oggetti idonei in qualsiasi classe di storage di Amazon S3. Per ulteriori informazioni sulle classi di storage, consulta [Comprensione e gestione delle classi di storage Amazon S3](#). Amazon S3 rende non disponibili tutti gli oggetti scaduti. L'eventuale rimozione permanente degli oggetti dipende dallo stato della funzione Controllo delle versioni del bucket.
- Bucket senza versione: l'operazione Expiration comporta la rimozione permanente dell'oggetto da parte di Amazon S3.
- Bucket con versione – Per un bucket con versione (ovvero, con funzione Controllo delle versioni attivata o sospesa), sono diversi i fattori che governano la gestione dell'operazione Expiration da parte di Amazon S3. Per i bucket con controllo delle versioni abilitata o sospesa, vale quanto segue:
 - L'operazione Expiration si applica solo alla versione corrente (non ha effetto sulle versioni non correnti dell'oggetto).
 - Amazon S3 non esegue alcuna operazione se sono presenti una o più versioni dell'oggetto e il contrassegno di eliminazione è la versione corrente.
 - Se la versione corrente dell'oggetto è l'unica disponibile e porta anche il contrassegno di eliminazione (noto anche come contrassegno di eliminazione dell'oggetto scaduto, dove tutte le versioni degli oggetti vengono eliminate e rimane solo un contrassegno di eliminazione), Amazon S3 rimuove il contrassegno di eliminazione dall'oggetto scaduto. È possibile inoltre utilizzare l'operazione di eliminazione per indicare ad Amazon S3 di rimuovere i contrassegni di eliminazione dell'oggetto scaduto. Per un esempio, consulta [Rimozione dei contrassegni di eliminazione degli oggetti scaduti in un bucket con il controllo delle versioni abilitato](#).

Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Considera inoltre quanto segue durante la configurazione di Amazon S3 per la gestione delle scadenze:

- Versioning-enabled bucket

Se la versione dell'oggetto corrente non è un contrassegno di eliminazione, Amazon S3 aggiunge un contrassegno di eliminazione con un ID versione univoco. La versione corrente diventa quindi non corrente e il contrassegno di eliminazione diventa la versione corrente.

- Versioning-suspended bucket

Per un bucket con funzione Controllo delle versioni sospesa, l'operazione di scadenza comporta la creazione da parte di Amazon S3 di un contrassegno di eliminazione il cui ID versione sarà null. Il contrassegno di eliminazione sostituisce qualsiasi versione dell'oggetto con ID versione null nella gerarchia delle versioni: questa operazione elimina di fatto l'oggetto.

Inoltre, in Amazon S3 sono disponibili le seguenti operazioni, utili per gestire le versioni non correnti degli oggetti in un bucket con versione (ovvero, con funzione Controllo delle versioni attivata o sospesa).

- Elemento dell'operazione **NoncurrentVersionTransition**: utilizzare questa operazione per specificare quando Amazon S3 effettua il trasferimento degli oggetti alla classe di storage specificata. È possibile basare questa transizione su un determinato numero di giorni da quando gli oggetti sono diventati non correnti (<NoncurrentDays>). Oltre al numero di giorni, puoi anche specificare il numero di versioni non correnti (<NewerNoncurrentVersions>) da conservare (tra 1 e 100). Questo valore determina quante versioni non correnti più recenti devono esistere prima che Amazon S3 possa effettuare la transizione di una determinata versione. Amazon S3 trasferirà eventuali versioni aggiuntive non correnti oltre il numero specificato da conservare. Affinché la transizione avvenga, i valori <NoncurrentDays> e <NewerNoncurrentVersions> devono essere entrambi superati.

Per specificare il numero di versioni non correnti da mantenere, devi anche fornire un elemento <Filter>. Se non specifichi un elemento <Filter>, Amazon S3 genera un errore `InvalidRequest` quando indichi il numero di versioni non correnti da mantenere.

Per ulteriori informazioni sul trasferimento degli oggetti, consulta [Transizioni supportate](#). Per informazioni dettagliate su come Amazon S3 calcola la data quando si specifica il numero di giorni nell'operazione `NoncurrentVersionTransition`, consulta [Regole del ciclo di vita basate sull'età di un oggetto](#).

- Elemento dell'operazione **NoncurrentVersionExpiration**: utilizzare questa operazione per indicare ad Amazon S3 di eliminare definitivamente le versioni non correnti degli oggetti. Gli oggetti eliminati non possono essere ripristinati. È possibile basare questa scadenza su un determinato numero di giorni trascorsi da quando gli oggetti sono diventati non correnti (`<NoncurrentDays>`). Oltre al numero di giorni, puoi anche specificare il numero di versioni non correnti (`<NewerNoncurrentVersions>`) da conservare (tra 1 e 100). Questo valore specifica quante versioni non correnti più recenti devono esistere prima che Amazon S3 possa far scadere una determinata versione. Amazon S3 eliminerà definitivamente tutte le versioni non correnti aggiuntive oltre al numero specificato da conservare. Affinché l'eliminazione avvenga, i valori `<NoncurrentDays>` e `<NewerNoncurrentVersions>` devono essere entrambi superati.

Per specificare il numero di versioni non correnti da mantenere, devi anche fornire un elemento `<Filter>`. Se non specifichi un elemento `<Filter>`, Amazon S3 genera un errore `InvalidRequest` quando indichi il numero di versioni non correnti da mantenere.

Il ritardo nella rimozione degli oggetti non correnti può rivelarsi utile per correggere eventuali eliminazioni o sovrascritture accidentali. Ad esempio, è possibile configurare una regola di scadenza perché elimini le versioni cinque giorni dopo essere diventate non correnti. Ad esempio, supponiamo che il giorno 1/1 /2014 alle 10:30 UTC, si crei un oggetto chiamato `photo.gif` (versione ID 111111). Il giorno 1/2 /2014 alle 11:30 UTC, si elimina accidentalmente `photo.gif` (ID versione 111111), creando un indicatore di eliminazione con un nuovo ID di versione (ad esempio l'ID di versione 4857693). A questo punto, si hanno cinque giorni per recuperare la versione originale di `photo.gif` (ID versione 111111) prima che l'eliminazione diventi definitiva. Il giorno 1/8 /2014 alle 00:00 UTC, la regola del ciclo di vita relativa alla scadenza viene eseguita ed eliminata definitivamente `photo.gif` (versione ID 111111), cinque giorni dopo essere diventata una versione non corrente.

Per informazioni dettagliate su come Amazon S3 calcola la data quando si specifica il numero di giorni in un'operazione `NoncurrentVersionExpiration`, consulta [Regole del ciclo di vita basate sull'età di un oggetto](#).

Note

Le configurazioni del ciclo di vita per la scadenza degli oggetti non rimuovono i caricamenti incompleti in più parti. Per eseguire questa operazione, è necessario utilizzare l'operazione di configurazione del ciclo di vita `AbortIncompleteMultipartUpload` descritta più avanti in questa sezione.

Oltre alle operazioni di transizione e scadenza, è possibile utilizzare le seguenti operazioni di configurazione del ciclo di vita per indicare ad Amazon S3 di interrompere i caricamenti in più parti incompleti o di rimuovere i contrassegni di eliminazione degli oggetti scaduti.

- Elemento dell'operazione **AbortIncompleteMultipartUpload**: questo elemento serve a impostare il tempo massimo (in giorni) in cui consentire l'esecuzione dei caricamenti in più parti. Se i caricamenti in più parti applicabili (identificati dal nome della chiave `prefix` specificato nella regola del ciclo di vita) non vengono completati nel periodo di tempo predefinito, Amazon S3 interrompe i caricamenti in più parti incompleti. Per ulteriori informazioni, consulta [Interruzione di un caricamento in più parti](#).

 Note

Non è possibile specificare questa operazione del ciclo di vita in una regola che ha un filtro che utilizza tag di oggetti.

- Elemento dell'operazione **ExpiredObjectDeleteMarker**: in un bucket con la funzione Controllo delle versioni attivata un contrassegno di eliminazione con zero versioni non correnti è definito contrassegno di eliminazione dell'oggetto scaduto. È possibile utilizzare questa operazione del ciclo di vita per indicare ad Amazon S3 di rimuovere i contrassegni di eliminazione degli oggetti scaduti. Per un esempio, consulta [Rimozione dei contrassegni di eliminazione degli oggetti scaduti in un bucket con il controllo delle versioni abilitato](#).

 Note

Non è possibile specificare questa operazione del ciclo di vita in una regola che ha un filtro che utilizza tag di oggetti.

Modalità con cui Amazon S3 calcola da quanto tempo un oggetto è non corrente

In un bucket abilitato al controllo delle versioni, possono essere incluse più versioni di un oggetto. Esiste sempre una versione corrente e zero o più versioni non correnti. Ogni volta che si carica un oggetto, la versione appena aggiunta diventa la versione corrente e quella che lo era in precedenza viene mantenuta come versione non corrente. Per stabilire da quanti giorni è non corrente un oggetto, Amazon S3 considera la data di creazione della versione successiva. Il numero di giorni dalla data di creazione della versione successiva viene utilizzato da Amazon S3 come numero di giorni da cui l'oggetto è non corrente.

Ripristino delle versioni precedenti di un oggetto con l'uso delle configurazioni del ciclo di vita di S3

Come spiegato in [Ripristino di versioni precedenti](#), è possibile utilizzare uno dei due metodi seguenti per recuperare le versioni precedenti di un oggetto:

- Metodo 1: Copiare una versione non corrente dell'oggetto nello stesso bucket. La copia diventa la versione corrente dell'oggetto e vengono conservate tutte le sue versioni.
- Metodo 2: Eliminare definitivamente la versione corrente dell'oggetto. Così facendo, in effetti, la versione prima non corrente diventa la versione corrente dell'oggetto.

Quando si utilizzano le regole di configurazione del ciclo di vita S3 per bucket con funzione Controllo delle versioni abilitata, il Metodo 1 rappresenta la best practice consigliata.

Il ciclo di vita di S3 opera in base a un modello consistente finale. Una versione corrente eliminata definitivamente potrebbe non scomparire finché le modifiche non si propagano a tutti i sistemi Amazon S3. Pertanto, Amazon S3 potrebbe non essere temporaneamente a conoscenza di questa eliminazione. Nel frattempo, la regola del ciclo di vita configurata per la scadenza degli oggetti non correnti potrebbe rimuovere definitivamente tali oggetti, compreso quello da ripristinare. Ne consegue che l'opzione più sicura è la copia della vecchia versione, come consigliato nel Metodo 1.

Operazioni del ciclo di vita e stato della funzione Controllo delle versioni nel bucket

Regole del ciclo di vita basate sull'età di un oggetto

È possibile specificare un periodo di tempo (in numero di giorni) che deve trascorrere dalla creazione (o modifica) dell'oggetto prima che Amazon S3 possa eseguire l'operazione specificata.

Quando si specifica il numero di giorni nelle operazioni Transition ed Expiration in una configurazione del ciclo di vita S3, tenere presente quanto segue:

- Il valore specificato è il numero di giorni dalla creazione dell'oggetto in cui si verificherà l'operazione.
- Amazon S3 calcola l'ora aggiungendo il numero di giorni specificato nella regola all'ora di creazione dell'oggetto e arrotondando l'ora che ne risulta alla mezzanotte UTC del giorno successivo. Ad esempio, se un oggetto è stato creato il 1/15 /2014 alle 10:30 UTC e si specificano 3 giorni in una regola di transizione, la data di transizione dell'oggetto verrà calcolata come 1/19 /2014 00:00 UTC.

 Note

Amazon S3 gestisce solo l'ultima data di modifica per ciascun oggetto. Ad esempio, la console Amazon S3 mostra la data Ultima modifica nel riquadro Proprietà dell'oggetto. Quando si crea un nuovo oggetto, questo valore corrisponderà alla data di creazione. Se l'oggetto viene sostituito, la data cambia di conseguenza. Pertanto, la data di creazione è sinonimo della data Ultima modifica.

Quando si specifica il numero di giorni nelle operazioni `NoncurrentVersionTransition` e `NoncurrentVersionExpiration` in una configurazione del ciclo di vita, tenere presente quanto segue:

- Il valore specificato è il numero di giorni a partire dal momento in cui la versione dell'oggetto diventa non corrente (ovvero, dalla sovrascrittura o eliminazione dell'oggetto), quando Amazon S3 eseguirà l'operazione sugli oggetti specificati.
- Amazon S3 calcola l'ora aggiungendo il numero di giorni specificato nella regola all'ora in cui la nuova versione successiva dell'oggetto viene creata e arrotondando l'ora che ne risulta alla mezzanotte UTC del giorno successivo. Ad esempio, nel tuo bucket, supponiamo di avere una versione corrente di un oggetto creato il 1/1/2014 alle 10:30 UTC. Se la nuova versione dell'oggetto che sostituisce la versione corrente viene creata il 1/15/2014 alle 10:30 UTC e si specificano 3 giorni in una regola di transizione, la data di transizione dell'oggetto viene calcolata come 1/19/2014 00:00 UTC.

Regole del ciclo di vita basate su una data specifica

Quando si specifica un'operazione in una regola del ciclo di vita S3, è possibile specificare la data in cui si desidera che Amazon S3 esegua l'operazione. Alla data specificata, Amazon S3 applica l'operazione a tutti gli oggetti idonei (in base ai criteri di filtro).

Se si specifica un'operazione del ciclo di vita S3 per una data già trascorsa, tutti gli oggetti idonei sono immediatamente qualificati per tale operazione.

 Important

Le operazioni basate su data non sono valide una tantum. Se lo stato della regola è `Enabled`, Amazon S3 continua ad applicare l'operazione basata su data anche dopo che questa è trascorsa.

Si supponga ad esempio di specificare un'operazione `Expiration` basata su data per l'eliminazione di tutti gli oggetti (assumendo che nella regola non siano specificati filtri). Nella data specificata, Amazon S3 applica la scadenza a tutti gli oggetti nel bucket. Amazon S3 continua inoltre ad applicare la scadenza a tutti i nuovi oggetti creati nel bucket. Per interrompere l'operazione, è necessario rimuoverla dalla regola del ciclo di vita, disabilitare la regola o eliminare la regola dalla configurazione del ciclo di vita.

Il valore della data deve essere conforme allo standard ISO 8601. L'ora è sempre la mezzanotte UTC.

Note

Non è possibile creare le regole del ciclo di vita basate su data nella console Amazon S3, ma è possibile visualizzarle, disabilitarle o eliminarle.

Aggiunta di filtri alle regole del ciclo di vita

I filtri sono un elemento opzionale delle regole del ciclo di vita che è possibile utilizzare per specificare gli oggetti a cui si applica la regola.

Per filtrare gli oggetti possono essere utilizzati i seguenti elementi:

Prefisso della chiave

È possibile filtrare gli oggetti in base a un prefisso. Se desideri applicare un'azione del ciclo di vita a un sottoinsieme di oggetti con prefissi diversi, crea regole separate per ciascuna azione.

Tag dell'oggetto

È possibile filtrare gli oggetti in base a uno o più tag. Ogni tag deve corrispondere esattamente sia alla chiave che al valore e, se si specificano più tag, ogni chiave del tag deve essere univoca. Un filtro con più tag dell'oggetto si applica a un sottoinsieme di oggetti con tutti i tag specificati. Se per un oggetto sono specificati tag aggiuntivi, il filtro verrà comunque applicato.

 Note

Se si specifica solo un elemento Key e nessun elemento Value, la regola verrà applicata solo agli oggetti che corrispondono alla chiave del tag e che non hanno un valore specificato.

Dimensione minima o massima dell'oggetto

È possibile filtrare gli oggetti in base alla dimensione. È possibile specificare una dimensione minima (`ObjectSizeGreaterThan`) o una dimensione massima (`ObjectSizeLessThan`) oppure è possibile specificare un intervallo di dimensioni dell'oggetto nello stesso filtro. I valori delle dimensioni degli oggetti sono espressi in byte. La dimensione massima del filtro è di 50 TB. Amazon S3 applica una dimensione minima dell'oggetto predefinita alla configurazione del ciclo di vita. Per ulteriori informazioni, consulta [Esempio: Consentire la transizione di oggetti di dimensioni inferiori a 128 KB](#).

È possibile combinare diversi elementi di filtro, nel qual caso Amazon S3 utilizza un operatore AND logico.

Esempi di filtri

Di seguito sono riportati esempi che mostrano come è possibile utilizzare diversi elementi di filtro:

- Definizione di un filtro tramite prefissi della chiave: questo esempio illustra una regola del ciclo di vita S3 valida per un sottoinsieme di oggetti in base al prefisso del nome della chiave (`logs/`). Ad esempio, la regola del ciclo di vita è valida per gli oggetti `logs/mylog.txt`, `logs/temp1.txt` e `logs/test.txt`, ma non per l'oggetto `example.jpg`.

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    transition/expiration actions
    ...
  </Rule>
  ...
</LifecycleConfiguration>
```

Note

Se si hanno uno o più prefissi che iniziano con gli stessi caratteri, è possibile includere tutti questi prefissi nella regola specificando un prefisso parziale senza barra finale (/) nel filtro. Ad esempio, supponiamo di avere i seguenti prefissi:

```
sales1999/
           sales2000/
           sales2001/
```

Per includere tutti e tre i prefissi nella regola, specificare `sales` come prefisso nella regola del ciclo di vita.

Per applicare un'operazione per il ciclo di vita a un sottoinsieme di oggetti in base a diversi prefissi del nome della chiave, specificare regole separate e, all'interno di ognuna, specificare un filtro basato sul prefisso. Ad esempio, per descrivere un'operazione per il ciclo di vita per oggetti con prefissi della chiave `projectA/` e `projectB/`, vanno specificate due regole, come illustrato di seguito:

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <Prefix>projectA/</Prefix>
    </Filter>
    transition/expiration actions
    ...
  </Rule>

  <Rule>
    <Filter>
      <Prefix>projectB/</Prefix>
    </Filter>
    transition/expiration actions
    ...
  </Rule>
</LifecycleConfiguration>
```

Per ulteriori informazioni sulle chiavi degli oggetti, consulta [Denominazione di oggetti Amazon S3](#).

- Definizione di un filtro in base ai tag dell'oggetto: nell'esempio che segue la regola del ciclo di vita specifica un filtro basato su un tag (*key*) e un valore (*value*). La regola si applica quindi solo a un sottoinsieme di oggetti con quel tag specifico.

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <Tag>
        <Key>key</Key>
        <Value>value</Value>
      </Tag>
    </Filter>
    transition/expiration actions
    ...
  </Rule>
</LifecycleConfiguration>
```

È possibile specificare un filtro basato su più tag. È necessario racchiudere i tag nell'elemento `<And>` illustrato nell'esempio che segue. La regola indica ad Amazon S3 di eseguire le operazioni del ciclo di vita sugli oggetti con due tag (con la specifica combinazione di chiave e valore).

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <And>
        <Tag>
          <Key>key1</Key>
          <Value>value1</Value>
        </Tag>
        <Tag>
          <Key>key2</Key>
          <Value>value2</Value>
        </Tag>
        ...
      </And>
    </Filter>
    transition/expiration actions
  </Rule>
</Lifecycle>
```

La regola del ciclo di vita si applica agli oggetti che contengono entrambi i tag specificati. Amazon S3 esegue un'operazione logica AND. Tenere presente quanto segue:

- Ogni tag deve corrispondere esattamente sia alla chiave che al valore. Se si specifica solo un elemento <Key> e nessun elemento <Value>, la regola verrà applicata solo agli oggetti che corrispondono alla chiave del tag e che non hanno un valore specificato.
- La regola si applica a un sottoinsieme di oggetti che ha tutti i tag specificati nella regola. Se a un oggetto sono specificati tag aggiuntivi, la regola verrà comunque applicata.

Note

Quando si specificano più tag in un filtro, ogni chiave del tag deve essere univoca.

- Definizione di un filtro in base al prefisso e a uno o più tag: in una regola del ciclo di vita è possibile specificare un filtro in base al prefisso della chiave e a uno o più tag. Anche in questo caso, è necessario racchiudere tutti gli elementi del filtro nell'elemento <And>, come illustrato di seguito.

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <And>
        <Prefix>key-prefix</Prefix>
        <Tag>
          <Key>key1</Key>
          <Value>value1</Value>
        </Tag>
        <Tag>
          <Key>key2</Key>
          <Value>value2</Value>
        </Tag>
        ...
      </And>
    </Filter>
    <Status>Enabled</Status>
    transition/expiration actions
  </Rule>
</LifecycleConfiguration>
```

Amazon S3 combina questi filtri tramite l'operatore logico AND. In altre parole, la regola si applica al sottoinsieme di oggetti con il prefisso della chiave e i tag specificati. Un filtro può avere un solo prefisso e zero o più tag.

- Definizione di un filtro vuoto: è possibile specificare un filtro vuoto, nel qual caso la regola si applica a tutti gli oggetti nel bucket.

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
    </Filter>
    <Status>Enabled</Status>
    transition/expiration actions
  </Rule>
</LifecycleConfiguration>
```

- Definizione di un filtro per le dimensioni degli oggetti: per filtrare una regola per dimensione oggetto, è possibile specificare una dimensione minima (`ObjectSizeGreaterThan`) o massima (`ObjectSizeLessThan`) oppure è possibile specificare un intervallo di dimensioni degli oggetti.

I valori delle dimensioni degli oggetti sono espressi in byte. La dimensione massima del filtro è 50 TB. Alcune classi di storage presentano limitazioni relative alle dimensioni minime degli oggetti. Per ulteriori informazioni, consulta [Confronto delle classi di storage di Amazon S3](#).

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
    </Filter>
    <Status>Enabled</Status>
    transition/expiration actions
  </Rule>
</LifecycleConfiguration>
```

Note

I filtri `ObjectSizeGreaterThan` e `ObjectSizeLessThan` escludono i valori specificati. Ad esempio, se imposti oggetti di dimensioni comprese tra 128 KB e 1024 KB per passare dalla classe di archiviazione S3 Standard alla classe di archiviazione S3 Standard-IA, gli oggetti che sono esattamente 1024 KB e 128 KB non passeranno a S3 Standard-IA.

regola si applicherà invece solo agli oggetti con dimensioni superiori a 128 KB e inferiori a 1024 KB.

Se stai specificando un intervallo di dimensioni degli oggetti, il numero intero `ObjectSizeGreaterThan` deve essere minore del valore `ObjectSizeLessThan`. Quando si utilizzano più filtri, è necessario racchiudere i filtri in un elemento `<And>`. L'esempio seguente illustra come specificare gli oggetti in un intervallo compreso tra 500 e 64.000 byte.

```
<LifecycleConfiguration>
  <Rule>
    <Filter>
      <And>
        <Prefix>key-prefix</Prefix>
        <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        <ObjectSizeLessThan>64000</ObjectSizeLessThan>
      </And>
    </Filter>
    <Status>Enabled</Status>
    transition/expiration actions
  </Rule>
</LifecycleConfiguration>
```

In che modo Amazon S3 gestisce i conflitti nelle configurazioni del ciclo di vita

In genere, il ciclo di vita Amazon S3 ottimizza i costi. Ad esempio, se due policy per la scadenza di sovrappongono, verrà onorata la policy per la scadenza più breve in modo che i dati non rimangano archiviati più a lungo del previsto. Analogamente, se due policy di trasferimento si sovrappongono, il ciclo di vita S3 eseguirà la transizione degli oggetti nella classe di storage ottimizzata per i costi.

In entrambi i casi, il ciclo di vita S3 tenta di scegliere il percorso meno costoso per l'utente.

Un'eccezione a questa regola generale riguarda la classe di Intelligent-Tiering archiviazione S3. S3 Intelligent-Tiering è preferito da S3 Lifecycle rispetto a qualsiasi classe di storage, ad eccezione delle classi di storage S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

Quando una configurazione del ciclo di vita S3 contiene più regole, un oggetto può diventare idoneo a più operazioni del ciclo di vita S3 nello stesso giorno. In questi casi, Amazon S3 segue le seguenti regole generali:

- L'eliminazione permanente ha la precedenza sul trasferimento.
- Il trasferimento ha la precedenza sulla creazione dei [contrassegni di eliminazione](#).
- Quando un oggetto è idoneo sia per una transizione S3 Glacier Flexible Retrieval che per una transizione S3 Standard-IA (o S3 One), Amazon S3 sceglie la transizione S3 Glacier Flexible Retrieval. Zone-IA

Esempi di sovrapposizione di filtri e conflitto tra operazioni del ciclo di vita

In una configurazione del ciclo di vita S3 potrebbero venire specificati prefissi o operazioni che si sovrappongono. Negli esempi seguenti viene illustrato in che modo Amazon S3 sceglie di risolvere i potenziali conflitti.

Example 1: sovrapposizione di prefissi (nessun conflitto)

La configurazione di esempio riportata di seguito include due regole in cui sono specificati prefissi che si sovrappongono nel modo seguente:

- La prima regola specifica un filtro vuoto, che indica tutti gli oggetti nel bucket.
- La seconda regola specifica un prefisso del nome della chiave (logs/), che indica solo un sottoinsieme di oggetti.

La regola 1 richiede ad Amazon S3 di eliminare tutti gli oggetti un anno dopo la creazione. La regola 2 richiede ad Amazon S3 di effettuare la transizione di un sottoinsieme di oggetti alla classe di storage S3 30 giorni dopo la creazione. Standard-IA

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
```



```
<Rule>
  <ID>Rule 2</ID>
  <Filter>
    <Prefix>logs/</Prefix>
  </Filter>
  <Status>Enabled</Status>
  <Transition>
    <StorageClass>STANDARD_IA</StorageClass>
    <Days>30</Days>
  </Transition>
</Rule>
</LifecycleConfiguration>
```

Poiché in questo caso non vi è alcun conflitto, Amazon S3 effettuerà la transizione degli oggetti con il `logs/` prefisso alla classe di Standard-IA storage S3 30 giorni dopo la creazione. Una volta passato un anno dalla data di creazione di qualsiasi oggetto, questo verrà eliminato.

Example 2: conflitto tra operazioni del ciclo di vita

Questa configurazione di esempio include due regole che indicano ad Amazon S3 di eseguire due operazioni diverse sullo stesso insieme di oggetti nello stesso momento dell'esistenza degli oggetti:

- Entrambe le regole specificano lo stesso prefisso nel nome della chiave, quindi entrambe le regole si applicano allo stesso insieme di oggetti.
- Entrambe le regole specificano che devono essere applicate 365 giorni dopo la data di creazione degli oggetti.
- Una regola ordina ad Amazon S3 di effettuare la transizione degli oggetti alla classe di Standard-IA storage S3 e un'altra regola richiede che Amazon S3 faccia scadere gli oggetti contemporaneamente.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

```
</Rule>
<Rule>
  <ID>Rule 2</ID>
  <Filter>
    <Prefix>logs/</Prefix>
  </Filter>
  <Status>Enabled</Status>
  <Transition>
    <StorageClass>STANDARD_IA</StorageClass>
    <Days>365</Days>
  </Transition>
</Rule>
</LifecycleConfiguration>
```

In questo caso, dal momento che l'obiettivo è di far scadere (rimuovere) gli oggetti, non ha senso cambiare la classe di archiviazione, quindi Amazon S3 sceglie semplicemente di eseguire l'operazione di scadenza su questi oggetti.

Example 3: sovrapposizione di prefissi con conseguente conflitto tra operazioni del ciclo di vita

In questo esempio la configurazione include due regole, in cui sono specificati prefissi che si sovrappongono nel modo seguente:

- La regola 1 specifica un prefisso vuoto, che indica tutti gli oggetti.
- La regola 2 specifica un prefisso della chiave (logs/), che indica un sottoinsieme di tutti gli oggetti.

Per il sottoinsieme di oggetti con il prefisso nel nome della chiave logs/, si applicano le operazioni del ciclo di vita S3 in entrambe le regole. Una regola indica ad Amazon S3 di trasferire gli oggetti 10 giorni dopo la data di creazione mentre un'altra regola indica ad Amazon S3 di trasferirli 365 giorni dopo la data di creazione.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>10</Days>
```

```
</Transition>
</Rule>
<Rule>
  <ID>Rule 2</ID>
  <Filter>
    <Prefix>logs/</Prefix>
  </Filter>
  <Status>Enabled</Status>
  <Transition>
    <StorageClass>STANDARD_IA</StorageClass>
    <Days>365</Days>
  </Transition>
</Rule>
</LifecycleConfiguration>
```

In questo caso, Amazon S3 sceglie di trasferirli 10 giorni dopo la data di creazione.

Example 4: Tag-based filtraggio e conseguenti azioni contrastanti sul ciclo di vita

Supponiamo di avere la configurazione del ciclo di vita S3 seguente con due regole, in ognuna delle quali è specificato un filtro basato su tag:

- La regola 1 specifica un filtro basato su tag (tag1/value1). Questa regola indica ad Amazon S3 di trasferire gli oggetti nella classe di archiviazione S3 Glacier Flexible Retrieval 365 giorni dopo la data di creazione.
- La regola 2 specifica un filtro basato su tag (tag2/value2). Questa regola indica ad Amazon S3 di far scadere gli oggetti 14 giorni dopo la creazione.

Nell'esempio di seguito viene mostrata la configurazione del ciclo di vita S3.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Tag>
        <Key>tag1</Key>
        <Value>value1</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
```

```
<StorageClass>GLACIER</StorageClass>
  <Days>365</Days>
</Transition>
</Rule>
<Rule>
  <ID>Rule 2</ID>
  <Filter>
    <Tag>
      <Key>tag2</Key>
      <Value>value2</Value>
    </Tag>
  </Filter>
  <Status>Enabled</Status>
  <Expiration>
    <Days>14</Days>
  </Expiration>
</Rule>
</LifecycleConfiguration>
```

Se un oggetto ha entrambi i tag, Amazon S3 deve decidere quale regola seguire. In questo caso, Amazon S3 fa scadere l'oggetto 14 giorni dopo la data di creazione. L'oggetto viene rimosso, quindi non viene eseguita l'operazione di trasferimento.

Esempi di configurazioni del ciclo di vita S3

In questa sezione vengono forniti alcuni esempi di configurazione del ciclo di vita S3. Ogni esempio mostra come si può specificare il codice XML in ciascun scenario di esempio.

Argomenti

- [Archiviazione di tutti gli oggetti entro un giorno dalla creazione](#)
- [Disabilitazione temporanea delle regole del ciclo di vita](#)
- [Abbassamento della classe di storage durante il ciclo di vita di un oggetto](#)
- [Specifica di più regole](#)
- [Specifica di una regola del ciclo di vita per un bucket che supporta la funzionalità Controllo delle versioni](#)
- [Rimozione dei contrassegni di eliminazione degli oggetti scaduti in un bucket con il controllo delle versioni abilitato](#)
- [Configurazione del ciclo di vita per interrompere i caricamenti in più parti](#)

- [Oggetti non correnti in scadenza che non contengono dati](#)
- [Esempio: Consentire la transizione di oggetti di dimensioni inferiori a 128 KB](#)

Archiviazione di tutti gli oggetti entro un giorno dalla creazione

Ogni regola del ciclo di vita S3 include un filtro che è possibile utilizzare per identificare un sottoinsieme di oggetti nel bucket a cui si applica la regola del ciclo di vita S3. Le configurazioni del ciclo di vita S3 seguenti mostrano esempi di come specificare un filtro.

- In questa regola di configurazione del ciclo di vita S3, il filtro specifica un prefisso della chiave (tax/). Pertanto la regola si applica agli oggetti con il prefisso del nome della chiave tax/, ad esempio tax/doc1.txt e tax/doc2.txt.

La regola specifica due operazioni che richiedono ad Amazon S3 di eseguire quanto segue:

- Trasferire gli oggetti nella classe di archiviazione S3 Glacier Flexible Retrieval dopo 365 giorni (un anno) dalla data di creazione.
- Eliminare gli oggetti (operazione Expiration) dopo 3.650 giorni (10 anni) dalla data di creazione.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition and Expiration Rule</ID>
    <Filter>
      <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

Invece di specificare l'età dell'oggetto in termini di giorni dalla data di creazione, è possibile specificare una data per ogni operazione. Non è tuttavia possibile utilizzare sia Date sia Days nella stessa regola.

- Per applicare la regola del ciclo di vita S3 a tutti gli oggetti nel bucket, occorre specificare un prefisso vuoto. Nella configurazione seguente, la regola specifica un'operazione `Transition` che indica ad Amazon S3 di trasferire gli oggetti nella classe di archiviazione S3 Glacier Flexible Retrieval dopo 0 giorni dalla data di creazione. Questa regola indica che gli oggetti sono idonei per l'archiviazione in Recupero flessibile S3 Glacier a mezzanotte UTC dopo la creazione. Per ulteriori informazioni sui vincoli del ciclo di vita, consulta la sezione [Vincoli e considerazioni per le transizioni](#).

```
<LifecycleConfiguration>
  <Rule>
    <ID>Archive all object same-day upon creation</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

- È possibile specificare zero o un prefisso del nome della chiave e zero o più tag di oggetto in un filtro. Nel codice di esempio riportato di seguito la regola del ciclo di vita S3 viene applicata a un sottoinsieme di oggetti con il prefisso della chiave `tax/` e agli oggetti che dispongono di due tag con chiave e valore specifici. Quando si specifica più di un filtro, è necessario includere l'elemento `<And>` come mostrato (Amazon S3 applica un'istruzione AND logica per combinare le condizioni del filtro specificate).

```
...
<Filter>
  <And>
    <Prefix>tax/</Prefix>
    <Tag>
      <Key>key1</Key>
      <Value>value1</Value>
    </Tag>
    <Tag>
      <Key>key2</Key>
      <Value>value2</Value>
    </Tag>
  </And>
</Filter>
```

```
</And>
</Filter>
...
```

- È possibile filtrare gli oggetti in base solo ai tag. La regola del ciclo di vita S3 riportata di seguito, ad esempio, viene applicata agli oggetti che dispongono dei due tag specificati (non viene specificato alcun prefisso).

```
...
<Filter>
  <And>
    <Tag>
      <Key>key1</Key>
      <Value>value1</Value>
    </Tag>
    <Tag>
      <Key>key2</Key>
      <Value>value2</Value>
    </Tag>
  </And>
</Filter>
...
```

Important

Quando una configurazione del ciclo di vita S3 contiene più regole, un oggetto può diventare idoneo a più operazioni del ciclo di vita S3 nello stesso giorno. In questi casi, Amazon S3 segue le seguenti regole generali:

- L'eliminazione permanente ha la precedenza sul trasferimento.
- Il trasferimento ha la precedenza sulla creazione dei [contrassegni di eliminazione](#).
- Quando un oggetto è idoneo sia per una transizione S3 Glacier Flexible Retrieval che per S3 Standard-IA (o S3 One Zone-IA), Amazon S3 sceglie la transizione S3 Glacier Flexible Retrieval.

Per alcuni esempi, consulta [Esempi di sovrapposizione di filtri e conflitto tra operazioni del ciclo di vita](#).

Disabilitazione temporanea delle regole del ciclo di vita

Un regola del ciclo di vita S3 può essere disabilitata temporaneamente mediante l'elemento `status`. Ciò può essere utile se si desidera testare nuove regole o risolvere problemi relativi alla configurazione, senza sovrascrivere le regole esistenti. Nella configurazione del ciclo di vita S3 seguente sono specificate due regole:

- La regola 1 indica ad Amazon S3 di trasferire gli oggetti con il prefisso `logs/` nella classe di archiviazione S3 Glacier Flexible Retrieval subito dopo la creazione.
- La regola 2 indica ad Amazon S3 di trasferire gli oggetti con il prefisso `documents/` nella classe di archiviazione S3 Glacier Flexible Retrieval subito dopo la creazione.

Nella configurazione, la regola 1 è abilitata e la regola 2 è disabilitata. Amazon S3 ignora la regola disabilitata.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule2</ID>
    <Filter>
      <Prefix>documents/</Prefix>
    </Filter>
    <Status>Disabled</Status>
    <Transition>
```



```
<Days>0</Days>
  <StorageClass>GLACIER</StorageClass>
</Transition>
</Rule>
</LifecycleConfiguration>
```

Abbassamento della classe di storage durante il ciclo di vita di un oggetto

In questo esempio, la configurazione del ciclo di vita S3 viene utilizzata per abbassare la classe di archiviazione degli oggetti nel corso della loro esistenza. Tale abbassamento contribuisce a ridurre i costi di storage. Per ulteriori informazioni sui prezzi, consulta la sezione [Prezzi di Amazon S3](#).

Nella configurazione del ciclo di vita S3 riportata di seguito viene specificata una regola che si applica agli oggetti con il prefisso del nome della chiave logs/. Nella regola vengono specificate le seguenti operazioni:

- Due operazioni di trasferimento:
 - Effettua la transizione degli oggetti alla classe di storage S3 30 giorni dopo la creazione. Standard-IA
 - Trasferimento degli oggetti nella classe di archiviazione S3 Glacier Flexible Retrieval dopo 90 giorni dalla data di creazione.
- Una operazione di scadenza che indica ad Amazon S3 di eliminare questi oggetti un anno dopo la creazione.

```
<LifecycleConfiguration>
  <Rule>
    <ID>example-id</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <Transition>
      <Days>90</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
```

```
<Days>365</Days>
</Expiration>
</Rule>
</LifecycleConfiguration>
```

Note

È possibile utilizzare un'unica regola per descrivere tutte le operazioni del ciclo di vita S3, se queste si applicano allo stesso insieme di oggetti (identificati dal filtro). In caso contrario, si possono aggiungere più regole per ogni oggetto specificando un filtro diverso.

Important

Quando una configurazione del ciclo di vita S3 contiene più regole, un oggetto può diventare idoneo a più operazioni del ciclo di vita S3 nello stesso giorno. In questi casi, Amazon S3 segue le seguenti regole generali:

- L'eliminazione permanente ha la precedenza sul trasferimento.
- Il trasferimento ha la precedenza sulla creazione dei [contrassegni di eliminazione](#).
- Quando un oggetto è idoneo sia per una transizione S3 Glacier Flexible Retrieval che per S3 Standard-IA (o S3 One Zone-IA), Amazon S3 sceglie la transizione S3 Glacier Flexible Retrieval.

Per alcuni esempi, consulta [Esempi di sovrapposizione di filtri e conflitto tra operazioni del ciclo di vita](#).

Specifica di più regole

Per eseguire operazioni del ciclo di vita S3 diverse su vari oggetti, è possibile specificare più regole. Nella configurazione del ciclo di vita S3 seguente sono specificate due regole:

- La regola 1 si applica agli oggetti con il prefisso nel nome della chiave `classA/`. Questa regola indica ad Amazon S3 di trasferire gli oggetti alla classe di archiviazione S3 Glacier Flexible Retrieval un anno dopo la creazione e di rimuoverli dopo 10 anni dalla creazione.

- La regola 2 si applica agli oggetti con il prefisso nel nome della chiave `classB/`. Indica ad Amazon S3 di trasferire gli oggetti alla classe di storage S3 90 giorni dopo la creazione e di eliminarli un anno dopo la creazione. Standard-IA

```
<LifecycleConfiguration>
  <Rule>
    <ID>ClassADocRule</ID>
    <Filter>
      <Prefix>classA</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
  <Rule>
    <ID>ClassBDocRule</ID>
    <Filter>
      <Prefix>classB</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>90</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

Important

Quando una configurazione del ciclo di vita S3 contiene più regole, un oggetto può diventare idoneo a più operazioni del ciclo di vita S3 nello stesso giorno. In questi casi, Amazon S3 segue le seguenti regole generali:

- L'eliminazione permanente ha la precedenza sul trasferimento.
- Il trasferimento ha la precedenza sulla creazione dei [contrassegni di eliminazione](#).
- Quando un oggetto è idoneo sia per una transizione S3 Glacier Flexible Retrieval che per una transizione S3 Standard-IA (o S3 One Zone-IA), Amazon S3 sceglie la transizione S3 Glacier Flexible Retrieval.

Per alcuni esempi, consulta [Esempi di sovrapposizione di filtri e conflitto tra operazioni del ciclo di vita](#).

Specifica di una regola del ciclo di vita per un bucket che supporta la funzionalità Controllo delle versioni

Supponiamo di avere un bucket con il controllo delle versioni abilitato. Questo significa che per ogni oggetto esistono una versione corrente e zero o più versioni non correnti. (Per ulteriori informazioni su Controllo versioni S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).)

Nell'esempio seguente si desidera mantenere uno storico di un anno e conservare 5 versioni non correnti. Le configurazioni del ciclo di vita S3 supportano la conservazione da 1 a 100 versioni di qualsiasi oggetto. Tieni presente che devono esistere più di 5 versioni non correnti più recenti prima che Amazon S3 possa far scadere una determinata versione. Amazon S3 eliminerà definitivamente tutte le versioni non correnti aggiuntive oltre al numero specificato da conservare. Affinché l'eliminazione avvenga, i valori `NoncurrentDays` e `NewerNoncurrentVersions` devono essere entrambi superati.

Per risparmiare sui costi di archiviazione è necessario spostare le versioni non correnti in S3 Glacier Flexible Retrieval 30 giorni dopo che diventano non correnti (supponendo che si tratti di dati cold a cui non è necessario accedere in tempo reale). Inoltre, ti aspetti che la frequenza di accesso delle versioni attuali diminuisca 90 giorni dopo la creazione, quindi potresti scegliere di spostare questi oggetti nella classe di storage S3. Standard-IA

```
<LifecycleConfiguration>
  <Rule>
    <ID>sample-rule</ID>
    <Filter>
      <Prefix></Prefix>
```

```
</Filter>
<Status>Enabled</Status>
<Transition>
  <Days>90</Days>
  <StorageClass>STANDARD_IA</StorageClass>
</Transition>
<NoncurrentVersionTransition>
  <NoncurrentDays>30</NoncurrentDays>
  <StorageClass>GLACIER</StorageClass>
</NoncurrentVersionTransition>
<NoncurrentVersionExpiration>
  <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
  <NoncurrentDays>365</NoncurrentDays>
</NoncurrentVersionExpiration>
</Rule>
</LifecycleConfiguration>
```

Rimozione dei contrassegni di eliminazione degli oggetti scaduti in un bucket con il controllo delle versioni abilitato

Un bucket abilitato per la funzione Controllo delle versioni mantiene una versione corrente e zero o più versioni non correnti di ogni oggetto. Quando si elimina un oggetto, tenere presente quanto segue:

- Se non si specifica un ID versione nella richiesta di eliminazione, Amazon S3 aggiunge un contrassegno di eliminazione invece di eliminare l'oggetto. La versione dell'oggetto corrente diventa non corrente, quindi il contrassegno di eliminazione diventa la versione corrente.
- Specificando l'ID versione nella richiesta di eliminazione, Amazon S3 elimina la versione dell'oggetto in modo permanente (non viene creato alcun contrassegno di eliminazione).
- Un contrassegno di eliminazione con zero versioni non correnti viene definito un contrassegno di eliminazione oggetto scaduto.

In questo esempio viene mostrato uno scenario che può creare contrassegni di eliminazione oggetto scaduto nel bucket. Viene inoltre mostrato come utilizzare la configurazione del ciclo di vita S3 per indicare ad Amazon S3 di rimuovere i contrassegni di eliminazione oggetto scaduto.

Supponiamo che tu scriva una configurazione del ciclo di vita S3 che utilizza l'azione `NoncurrentVersionExpiration` per rimuovere le versioni non correnti 30 giorni dopo che sono

diventate tali e per conservare 10 versioni non correnti, come mostrato nell'esempio seguente. Tieni presente che devono esistere più di 10 versioni non correnti più recenti prima che Amazon S3 possa far scadere una determinata versione. Amazon S3 eliminerà definitivamente tutte le versioni non correnti aggiuntive oltre al numero specificato da conservare. Affinché l'eliminazione avvenga, i valori `NoncurrentDays` e `NewerNoncurrentVersions` devono essere entrambi superati.

```
<LifecycleConfiguration>
  <Rule>
    ...
    <NoncurrentVersionExpiration>
      <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
      <NoncurrentDays>30</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```

L'azione `NoncurrentVersionExpiration` non si applica alle versioni correnti dell'oggetto. Rimuove solamente le versioni non correnti.

Per le versioni dell'oggetto correnti esistono le seguenti opzioni per gestirne la durata a seconda che le versioni dell'oggetto correnti seguano un ciclo di vita ben definito:

- Le versioni correnti dell'oggetto seguono un ciclo di vita ben definito.

In questo caso si può utilizzare una configurazione del ciclo di vita S3 con l'operazione `Expiration` per indicare ad Amazon S3 di rimuovere le versioni correnti, come mostrato nell'esempio seguente.

```
<LifecycleConfiguration>
  <Rule>
    ...
    <Expiration>
      <Days>60</Days>
    </Expiration>
    <NoncurrentVersionExpiration>
      <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
      <NoncurrentDays>30</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```

In questo esempio, Amazon S3 rimuove le versioni correnti 60 giorni dopo la data di creazione aggiungendo un contrassegno di eliminazione per ognuna delle versioni dell'oggetto correnti. La versione corrente diventa quindi non corrente e il contrassegno di eliminazione diventa la versione corrente. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Note

Non è possibile specificare sia un tag `Days` che un tag `ExpiredObjectDeleteMarker` sulla stessa regola. Specificando il tag `Days`, Amazon S3 eseguirà automaticamente la pulizia di `ExpiredObjectDeleteMarker` una volta che i contrassegni di eliminazione sono abbastanza vecchi da soddisfare i criteri di età. È possibile creare una regola separata con solo il tag `ExpiredObjectDeleteMarker` per ripulire i contrassegni di eliminazione non appena diventano l'unica versione.

L'operazione `NoncurrentVersionExpiration` nella stessa configurazione del ciclo di vita S3 rimuove gli oggetti non correnti 30 giorni dopo che sono diventati non correnti. Pertanto, in questo esempio, tutte le versioni degli oggetti vengono rimosse in modo permanente 90 giorni dopo la creazione dell'oggetto. Tieni presente che, in questo esempio, devono esistere più di 10 versioni non correnti più recenti prima che Amazon S3 possa far scadere una determinata versione. Amazon S3 eliminerà definitivamente tutte le versioni non correnti aggiuntive oltre al numero specificato da conservare. Affinché l'eliminazione avvenga, i valori `NoncurrentDays` e `NewerNoncurrentVersions` devono essere entrambi superati.

Nonostante i contrassegni di eliminazione degli oggetti scaduti vengano creati durante questo processo, Amazon S3 rileva e rimuove i contrassegni di eliminazione degli oggetti scaduti per te.

- Versioni correnti dell'oggetto che non seguono un ciclo di vita ben definito.

In questo caso è possibile rimuovere gli oggetti manualmente quando non servono più, creando un contrassegno di eliminazione con una o più versioni non correnti. Se la configurazione del ciclo di vita S3 con l'operazione `NoncurrentVersionExpiration` rimuove tutte le versioni non correnti, rimarranno i contrassegni di eliminazione oggetto scaduto.

In questo specifico scenario la configurazione del ciclo di vita S3 fornisce un'operazione `Expiration` che puoi utilizzare per rimuovere i contrassegni di eliminazione oggetto scaduto.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <ExpiredObjectDeleteMarker>true</ExpiredObjectDeleteMarker>
    </Expiration>
    <NoncurrentVersionExpiration>
      <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
      <NoncurrentDays>30</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```

Se si imposta l'elemento `ExpiredObjectDeleteMarker` su `true` nell'operazione `Expiration`, si indica ad Amazon S3 di rimuovere i contrassegni di eliminazione oggetto scaduto.

Note

Quando si specifica l'operazione del ciclo di vita S3 `ExpiredObjectDeleteMarker`, nella regola non può essere specificato un filtro basato su tag.

Configurazione del ciclo di vita per interrompere i caricamenti in più parti

È possibile utilizzare l'operazione REST API di Amazon S3 per il caricamento in più parti per caricare oggetti di grandi dimensioni in parti. Per ulteriori informazioni sui caricamenti in più parti, consulta la sezione [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Utilizzando la configurazione del ciclo di vita S3, è possibile indicare ad Amazon S3 di interrompere i caricamenti in più parti incompleti (identificati dal prefisso della chiave specificato nella regola) se non vengono completati entro un numero specificato di giorni dalla data di avvio. Quando Amazon S3 interrompe un caricamento in più parti, elimina tutte le parti associate al caricamento in più parti. Questo processo aiuta a controllare i costi di archiviazione garantendo che non siano presenti caricamenti in più parti incompleti con parti archiviate in Amazon S3.

Note

Quando si specifica l'operazione del ciclo di vita S3 `AbortIncompleteMultipartUpload`, nella regola non può essere specificato un filtro basato su tag.

Di seguito è riportata una configurazione del ciclo di vita S3 di esempio che specifica una regola con l'operazione `AbortIncompleteMultipartUpload`. Questa operazione richiede ad Amazon S3 di interrompere i caricamenti in più parti incompleti sette giorni dopo l'avvio.

```
<LifecycleConfiguration>
  <Rule>
    <ID>sample-rule</ID>
    <Filter>
      <Prefix>SomeKeyPrefix</Prefix>
    </Filter>
    <Status>rule-status</Status>
    <AbortIncompleteMultipartUpload>
      <DaysAfterInitiation>7</DaysAfterInitiation>
    </AbortIncompleteMultipartUpload>
  </Rule>
</LifecycleConfiguration>
```

Oggetti non correnti in scadenza che non contengono dati

È possibile creare regole per la transizione degli oggetti in base alle dimensioni. Puoi specificare una dimensione minima (`ObjectSizeGreaterThan`) o una dimensione massima (`ObjectSizeLessThan`) oppure puoi specificare un intervallo di dimensioni dell'oggetto (in byte). Quando si utilizzano più filtri, ad esempio un prefisso e una regola di dimensione, è necessario racchiudere i filtri in un elemento `<And>`.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition with a prefix and based on size</ID>
    <Filter>
      <And>
        <Prefix>tax</Prefix>
        <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
      </And>
    </Filter>
```

```
<Status>Enabled</Status>
<Transition>
  <Days>365</Days>
  <StorageClass>GLACIER</StorageClass>
</Transition>
</Rule>
</LifecycleConfiguration>
```

Se stai specificando un intervallo utilizzando entrambi gli elementi `ObjectSizeGreaterThan` e `ObjectSizeLessThan`, la dimensione massima dell'oggetto deve essere maggiore della dimensione minima dell'oggetto. Quando si utilizzano più filtri, è necessario racchiudere i filtri in un elemento `<And>`. L'esempio seguente illustra come specificare gli oggetti in un intervallo compreso tra 500 e 64.000 byte. Quando si specifica un intervallo, i filtri `ObjectSizeGreaterThan` e `ObjectSizeLessThan` escludono i valori specificati. Per ulteriori informazioni, consulta [the section called "Elemento Filter"](#).

```
<LifecycleConfiguration>
  <Rule>
    ...
    <And>
      <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
      <ObjectSizeLessThan>64000</ObjectSizeLessThan>
    </And>
  </Rule>
</LifecycleConfiguration>
```

È inoltre possibile creare regole per far scadere in modo specifico gli oggetti non correnti che non contengono dati, inclusi gli oggetti contrassegno di eliminazione non correnti creati in un bucket abilitato al controllo delle versioni. Nell'esempio seguente viene utilizzata l'azione `NoncurrentVersionExpiration` per rimuovere le versioni non correnti 30 giorni dopo che sono diventate tali e per mantenere 10 versioni non correnti. Nell'esempio viene inoltre utilizzato l'elemento `ObjectSizeLessThan` per filtrare solo gli oggetti senza dati.

Tieni presente che devono esistere più di 10 versioni non correnti più recenti prima che Amazon S3 possa far scadere una determinata versione. Amazon S3 eliminerà definitivamente tutte le versioni non correnti aggiuntive oltre al numero specificato da conservare. Affinché l'eliminazione avvenga, i valori `NoncurrentDays` e `NewerNoncurrentVersions` devono essere entrambi superati.

```
<LifecycleConfiguration>
  <Rule>
```

```
<ID>Expire noncurrent with size less than 1 byte</ID>
<Filter>
  <ObjectSizeLessThan>1</ObjectSizeLessThan>
</Filter>
<Status>Enabled</Status>
<NoncurrentVersionExpiration>
  <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
  <NoncurrentDays>30</NoncurrentDays>
</NoncurrentVersionExpiration>
</Rule>
</LifecycleConfiguration>
```

Esempio: Consentire la transizione di oggetti di dimensioni inferiori a 128 KB

Amazon S3 applica un comportamento predefinito alle configurazioni del ciclo di vita che impedisce la transizione di oggetti di dimensioni inferiori a 128 KB a qualsiasi classe di storage. È possibile consentire la transizione di oggetti più piccoli aggiungendo alla configurazione un filtro di dimensione minima (`ObjectSizeGreaterThan`) o dimensione massima (`ObjectSizeLessThan`) che specifichi una dimensione inferiore. L'esempio seguente consente a qualsiasi oggetto di dimensione inferiore a 128 KB di passare alla classe di storage Recupero istantaneo S3 Glacier:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Allow small object transitions</ID>
    <Filter>
      <ObjectSizeGreaterThan>1</ObjectSizeGreaterThan>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER_IR</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Note

A settembre 2024 Amazon S3 ha aggiornato il comportamento di transizione predefinito per gli oggetti di piccole dimensioni, come segue:

- Comportamento di transizione predefinito aggiornato: a partire da settembre 2024, il comportamento predefinito impedisce la transizione di oggetti di dimensioni inferiori a 128 KB a qualsiasi classe di storage.
- Comportamento di transizione predefinito precedente: prima di settembre 2024, il comportamento predefinito consentiva la transizione di oggetti di dimensioni inferiori a 128 KB solo nelle classi di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

Le configurazioni create prima di settembre 2024 mantengono il comportamento di transizione precedente a meno che non vengano modificate. In altre parole, se si creano, modificano o eliminano regole, il comportamento di transizione predefinito per la configurazione cambia in base al comportamento aggiornato. Se il caso d'uso lo richiede, è possibile modificare il comportamento di transizione predefinito in modo che gli oggetti di dimensioni inferiori a 128 KB passino a S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive. A tale scopo, utilizza l'intestazione `x-amz-transition-object-size-minimum-default` opzionale in una richiesta [PutBucketLifecycleConfiguration](#).

L'esempio seguente mostra come utilizzare l'intestazione `x-amz-transition-object-size-minimum-default` in una richiesta [PutBucketLifecycleConfiguration](#) per applicare il comportamento di transizione predefinito `varies_by_storage_class` a una configurazione del ciclo di vita S3. Questo comportamento consente a un oggetto di dimensioni inferiori a 128 KB di passare alle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Per impostazione predefinita, tutte le altre classi di storage impediscono le transizioni inferiori a 128 KB. È possibile comunque utilizzare filtri personalizzati per modificare la dimensione minima di transizione per qualsiasi classe di storage. I filtri personalizzati hanno sempre la precedenza sul comportamento di transizione predefinito:

```
HTTP/1.1 200
x-amz-transition-object-size-minimum-default: varies_by_storage_class
<?xml version="1.0" encoding="UTF-8"?>
...
```

Risoluzione dei problemi del ciclo di vita di Amazon S3

Le informazioni seguenti possono essere utili per risolvere i problemi con le regole del ciclo di vita di Amazon S3.

Argomenti

- [Ho eseguito un'operazione di elenco sul mio bucket e sono stati visualizzati oggetti che pensavo scaduti o sottoposti a transizione in base a una regola del ciclo di vita.](#)
- [Come posso monitorare le azioni intraprese dalle mie regole del ciclo di vita?](#)
- [Il numero di oggetti S3 continua ad aumentare, anche dopo aver impostato le regole del ciclo di vita su un bucket con la funzionalità Controllo delle versioni abilitata.](#)
- [Come posso svuotare il mio bucket S3 utilizzando le regole del ciclo di vita?](#)
- [La mia fattura Amazon S3 è aumentata dopo la transizione degli oggetti a una classe di archiviazione con costi inferiori.](#)
- [Ho aggiornato la mia policy di bucket, ma i miei oggetti S3 vengono ancora eliminati a causa delle regole del ciclo di vita scadute.](#)
- [Posso recuperare oggetti S3 scaduti in base alle regole del ciclo di vita di S3?](#)
- [Perché le mie azioni di scadenza e transizione del ciclo di vita non vengono eseguite?](#)
- [Come posso escludere un prefisso dalla mia regola del ciclo di vita?](#)
- [Come posso includere più prefissi nella mia regola del ciclo di vita?](#)

Ho eseguito un'operazione di elenco sul mio bucket e sono stati visualizzati oggetti che pensavo scaduti o sottoposti a transizione in base a una regola del ciclo di vita.

Le [transizioni](#) e le [scadenze](#) di oggetti del ciclo di vita S3 sono operazioni asincrone. Pertanto, potrebbe essersi verificato un ritardo tra il momento in cui gli oggetti sono idonei per la scadenza o la transizione e il momento in cui si è effettivamente verificata la transizione o la scadenza. Le modifiche a livello di fatturazione vengono applicate non appena la regola del ciclo di vita viene soddisfatta, anche se l'operazione non è completa. L'eccezione a questo comportamento è se hai una regola del ciclo di vita impostata per la transizione alla classe di storage S3 Intelligent-Tiering . In tal caso, le modifiche alla fatturazione non avvengono finché l'oggetto non è passato a S3 Intelligent-Tiering. Per le transizioni a S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive, la fatturazione in base alla classe di storage di destinazione, il sovraccarico di archiviazione per oggetto (40 KB) e il timer per la durata minima dello storage iniziano quando la regola del ciclo di vita è soddisfatta, anche

se la transizione fisica avviene in modo asincrono. Per ulteriori informazioni sulle modifiche alla fatturazione, consulta [Impostazione della configurazione del ciclo di vita in un bucket](#).

Note

Amazon S3 non effettua la transizione di oggetti di dimensioni inferiori a 128 KB dalla classe di Standard-IA storage S3 Standard o S3 Intelligent-Tiering alla classe di Zone-IA storage S3 Standard-IA, S3 o S3 One.

Come posso monitorare le azioni intraprese dalle mie regole del ciclo di vita?

Per monitorare le azioni intraprese dalle regole del ciclo di vita, è possibile utilizzare le seguenti funzionalità:

- Notifiche eventi S3: è possibile configurare le [Notifiche eventi S3](#) in modo da ricevere notifiche di eventuali eventi di scadenza o transizione del ciclo di vita S3.
- Log degli accessi al server S3: è possibile abilitare i log degli accessi al server per i bucket S3 per acquisire operazioni correlate al ciclo di vita S3, come le transizioni degli oggetti a un'altra classe di storage o le scadenze degli oggetti. Per ulteriori informazioni, consulta [Ciclo di vita e registrazione](#).

Per visualizzare quotidianamente le modifiche allo storage causate dalle azioni del ciclo di vita, ti consigliamo di utilizzare le dashboard di [S3 Storage Lens invece di utilizzare le metriche di Amazon CloudWatch](#). Nel pannello di controllo Storage Lens è possibile visualizzare le metriche seguenti, che monitorano il numero o le dimensioni degli oggetti:

- Byte della versione corrente
- Conteggio oggetti versione corrente
- Byte di versione non correnti
- Conteggio di oggetti versione non corrente
- Conteggio oggetti contrassegno di eliminazione
- Byte di archiviazione dei contrassegni di eliminazione
- Byte con caricamento in più parti incompleto
- Conteggio di oggetti con caricamento in più parti incompleto

Il numero di oggetti S3 continua ad aumentare, anche dopo aver impostato le regole del ciclo di vita su un bucket con la funzionalità Controllo delle versioni abilitata.

Quando un oggetto scade in un [bucket con la funzionalità Controllo delle versioni abilitata](#), l'oggetto non viene eliminato definitivamente dal bucket. Come versione più recente dell'oggetto viene invece creato un [contrassegno di eliminazione](#). I contrassegni di eliminazione vengono comunque conteggiati come oggetti. Pertanto, se viene creata una regola del ciclo di vita per far scadere solo le versioni correnti, il numero di oggetti nel bucket S3 aumenta anziché diminuire.

Ad esempio, supponiamo che un bucket S3 con il controllo delle versioni abilitato contenga 100 oggetti e che una regola del ciclo di vita sia impostata per far scadere le versioni correnti dell'oggetto dopo 7 giorni. Dopo il settimo giorno, il numero di oggetti aumenta a 200 perché vengono creati 100 contrassegni di eliminazione oltre ai 100 oggetti originali, che ora sono versioni non correnti. Per ulteriori informazioni sulle azioni delle regole di configurazione del ciclo di vita S3 per i bucket con il controllo delle versioni abilitato, consulta [Impostazione della configurazione del ciclo di vita in un bucket](#).

Per rimuovere definitivamente gli oggetti, aggiungi un'ulteriore configurazione del ciclo di vita per eliminare le versioni precedenti degli oggetti, i contrassegni di eliminazione scaduti e i caricamenti incompleti in più parti. Per istruzioni su come creare nuove regole del ciclo di vita, consulta [Impostazione della configurazione del ciclo di vita in un bucket](#).

Note

- Amazon S3 arrotonda la data di transizione o scadenza di un oggetto alla mezzanotte UTC del giorno successivo.

Quando valuta gli oggetti per le azioni del ciclo di vita, Amazon S3 utilizza l'ora di creazione degli oggetti in UTC. Ad esempio, considera un bucket senza versione con una regola del ciclo di vita configurata per far scadere gli oggetti dopo un giorno. Supponiamo che un oggetto sia stato creato il 1° gennaio alle 17:05 Pacific Daylight Time (PDT), che corrisponde al 2 gennaio alle 00:05 UTC. L'oggetto diventa vecchio di un giorno alle 00:05 UTC del 3 gennaio, il che lo rende idoneo alla scadenza quando il ciclo di vita S3 restituisce gli oggetti alle 00:00 UTC del 4 gennaio.

Poiché le operazioni del ciclo di vita di Amazon S3 avvengono in modo asincrono, potrebbe verificarsi un certo ritardo tra la data specificata nella regola del ciclo di vita e l'effettiva

transizione fisica dell'oggetto. Per ulteriori informazioni, consulta [Transition or expiration delay](#).

Per ulteriori informazioni, consulta [Regole del ciclo di vita basate sull'età di un oggetto](#).

- Per gli oggetti S3 protetti dalla funzionalità Blocco oggetti, le versioni correnti non vengono eliminate definitivamente. Agli oggetti viene invece aggiunto un contrassegno di eliminazione, che li rende non correnti. Le versioni non correnti vengono quindi conservate e non impostate come definitivamente scadute.

Come posso svuotare il mio bucket S3 utilizzando le regole del ciclo di vita?

Le regole del ciclo di vita S3 sono uno strumento efficace per [svuotare un bucket S3](#) contenente milioni di oggetti. Per eliminare un numero elevato di oggetti dal bucket S3, assicurarsi di utilizzare queste due coppie di regole del ciclo di vita:

- Impostazione come scadute delle versioni correnti degli oggetti ed eliminazione definitiva delle versioni precedenti degli oggetti
- Eliminazione dei contrassegni di eliminazione ed eliminazione dei caricamenti in più parti incompleti

Per la procedura di creazione di una regola di configurazione del ciclo di vita, consulta [Impostazione della configurazione del ciclo di vita in un bucket](#).

Note

Per gli oggetti S3 protetti dalla funzionalità Blocco oggetti, le versioni correnti non vengono eliminate definitivamente. Agli oggetti viene invece aggiunto un contrassegno di eliminazione, che li rende non correnti. Le versioni non correnti vengono quindi conservate e non impostate come definitivamente scadute.

La mia fattura Amazon S3 è aumentata dopo la transizione degli oggetti a una classe di archiviazione con costi inferiori.

Esistono diversi motivi per cui la fattura potrebbe aumentare dopo la transizione degli oggetti a una classe di archiviazione con costi inferiori:

- Costo generale S3 Glacier per oggetti di piccole dimensioni

Per ogni oggetto passato alla classe di archiviazione Recupero flessibile Amazon S3 Glacier o Deep Archive Amazon S3 Glacier, a questo aggiornamento dell'archiviazione è associato un costo generale aggiuntivo di 40 KB. Come parte del costo generale di 40 KB, 8 KB vengono utilizzati per archiviare i metadati e il nome dell'oggetto. Questi 8 KB vengono addebitati in base alle tariffe della classe di archiviazione Amazon S3 Standard. I restanti 32 KB vengono utilizzati per l'indicizzazione e i relativi metadati. Questi 32 KB vengono addebitato in base ai prezzi della classe di archiviazione Recupero flessibile Amazon S3 Glacier o Deep Archive Amazon S3 Glacier.

Pertanto, se si archiviano molti oggetti di dimensioni più piccole, non è consigliabile utilizzare le transizioni del ciclo di vita. Per ridurre eventuali costi aggiuntivi, valuta la possibilità di aggregare diversi oggetti di piccole dimensioni in un numero più contenuto di oggetti di grandi dimensioni prima di eseguirne l'archiviazione in Amazon S3. Per ulteriori informazioni sulle considerazioni relative ai costi, consulta l'argomento relativo al [trasferimento nelle classi di archiviazione Recupero flessibile Amazon S3 Glacier e Deep Archive Amazon S3 Glacier \(archiviazione di oggetti\)](#).

- Costi minimi di archiviazione

Alcune classi di archiviazione S3 hanno requisiti minimi di durata dell'archiviazione. Agli oggetti eliminati, sovrascritti o sottoposti a transizione da tali classi prima del raggiungimento della durata minima viene addebitata una tariffa di transizione o eliminazione anticipata proporzionale. Questi requisiti minimi di durata dell'archiviazione sono i seguenti:

- S3 e S3 One: 30 giorni Standard-IA Zone-IA
- Recupero flessibile Amazon S3 Glacier e Recupero istantaneo Amazon S3 Glacier: 90 giorni
- Deep Archive Amazon S3 Glacier: 180 giorni

Per ulteriori informazioni su questi requisiti, consulta la sezione Vincoli dell'argomento [Trasferimento degli oggetti utilizzando il ciclo di vita S3](#). Per informazioni generali sui prezzi di S3, consulta [Prezzi di Amazon S3](#) e il [Calcolatore dei prezzi AWS](#).

- Costi delle transizioni del ciclo di vita

Ogni volta che un oggetto viene trasferito a una classe di archiviazione diversa mediante una regola del ciclo di vita, Amazon S3 considera tale transizione come un'unica richiesta di transizione. I costi per queste richieste di transizione si aggiungono ai costi validi per le classi di archiviazione in questione. Se si ha intenzione di trasferire un numero elevato di oggetti, è consigliabile considerare i costi delle transizioni richieste in caso di transizione a una classe inferiore. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Ho aggiornato la mia policy di bucket, ma i miei oggetti S3 vengono ancora eliminati a causa delle regole del ciclo di vita scadute.

Le istruzioni Deny in una policy di bucket non impediscono la scadenza degli oggetti definiti in una regola del ciclo di vita. Le operazioni del ciclo di vita (come transizioni o scadenze) non utilizzano l'operazione S3 `DeleteObject`. Le operazioni del ciclo di vita di S3 vengono invece eseguite utilizzando endpoint S3 interni. Per ulteriori informazioni, consulta [Ciclo di vita e registrazione](#).

Per evitare che la regola del ciclo di vita esegua operazioni, è necessario modificare, eliminare o [disabilitare la regola](#).

Posso recuperare oggetti S3 scaduti in base alle regole del ciclo di vita di S3?

L'unico modo per recuperare gli oggetti scaduti in base al ciclo di vita S3 è tramite il controllo delle versioni, che deve essere attivo prima che gli oggetti diventino idonei alla scadenza. Non è possibile annullare le operazioni di scadenza eseguite dalle regole del ciclo di vita. Se gli oggetti vengono eliminati definitivamente in base alle regole del ciclo di vita S3 applicate, non sarà possibile recuperarli. Per abilitare il controllo delle versioni su un bucket, consulta [the section called "Conservazione più versioni degli oggetti"](#).

Se al bucket è stato applicato il controllo delle versioni e le versioni non correnti degli oggetti sono ancora intatte, è possibile [ripristinare le versioni precedenti degli oggetti scaduti](#). Per ulteriori informazioni sul comportamento delle operazioni delle regole del ciclo di vita S3 e sugli stati del controllo delle versioni, consulta la tabella Operazioni del ciclo di vita e stato della funzione Controllo delle versioni nel bucket in [Elementi per la descrizione delle operazioni nel ciclo di vita](#).

Note

Se il bucket S3 è protetto da [Backup AWS](#) o [Replica Amazon S3](#), è anche possibile utilizzare queste funzionalità per recuperare gli oggetti scaduti.

Perché le mie azioni di scadenza e transizione del ciclo di vita non vengono eseguite?

Per un bucket con controllo delle versioni abilitato o sospeso, le seguenti considerazioni determinano come Amazon S3 gestisce l'azione di scadenza:

- La scadenza dell'oggetto si applica solo alla sua versione corrente (non ha effetto sulle versioni non correnti dell'oggetto).

- Amazon S3 non esegue alcuna operazione se sono presenti una o più versioni dell'oggetto e il contrassegno di eliminazione è la versione corrente.
- Amazon S3 non esegue alcuna operazione sulle versioni non correnti degli oggetti a cui è applicato S3 Object Lock.
- Per gli oggetti con uno stato di FAILED replica PENDING o, Amazon S3 non intraprende alcuna azione sulle versioni correnti o non correnti degli oggetti.

Alle transizioni tra classi di storage del ciclo di vita si applicano i vincoli seguenti:

- Per impostazione predefinita, gli oggetti di dimensioni inferiori a 128 KB non verranno trasferiti ad alcuna classe di archiviazione.
- Per i bucket con versioning abilitato o sospeso, gli oggetti con uno stato di FAILED replica PENDING o non possono essere sottoposti a transizione.

Come posso escludere un prefisso dalla mia regola del ciclo di vita?

Il ciclo di vita S3 non supporta l'esclusione di prefissi nelle regole. Utilizza invece i tag per etichettare tutti gli oggetti che si desidera includere nella regola. Per ulteriori informazioni sull'utilizzo dei tag nelle regole del ciclo di vita, consulta [the section called “Archiviazione di tutti gli oggetti entro un giorno dalla creazione”](#).

Come posso includere più prefissi nella mia regola del ciclo di vita?

Il ciclo di vita S3 non supporta l'inclusione di più prefissi nelle regole. Utilizza invece i tag per etichettare tutti gli oggetti che si desidera includere nella regola. Per ulteriori informazioni sull'utilizzo dei tag nelle regole del ciclo di vita, consulta [the section called “Archiviazione di tutti gli oggetti entro un giorno dalla creazione”](#).

Tuttavia, se si hanno uno o più prefissi che iniziano con gli stessi caratteri, è possibile includere tutti questi prefissi nella regola specificando un prefisso parziale senza barra finale (/) nel filtro. Ad esempio, supponiamo di avere i seguenti prefissi:

```
sales1999/  
sales2000/  
sales2001/
```

Per includere tutti e tre i prefissi nella regola, specificare <Prefix>sales</Prefix> nella regola del ciclo di vita.

Registrazione e monitoraggio in Amazon S3

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon S3 e delle tue soluzioni. AWS Ti consigliamo di raccogliere dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. Prima di iniziare il monitoraggio di Amazon S3, è opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Per ulteriori informazioni sulla registrazione e il monitoraggio in Amazon S3, consulta gli argomenti riportati di seguito.

Note

Per ulteriori informazioni sull'uso della classe di storage Amazon S3 Express One Zone con i bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon S3 e delle tue soluzioni. AWS È necessario raccogliere dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. AWS fornisce diversi strumenti per monitorare le risorse di Amazon S3 e rispondere a potenziali incidenti.

Allarmi Amazon CloudWatch

Utilizzando gli CloudWatch allarmi Amazon, osservi una singola metrica in un periodo di tempo specificato. Se la metrica supera una determinata soglia, viene inviata una notifica a un argomento o a una policy di Amazon SNS. AWS Auto Scaling CloudWatch gli allarmi non

richiamano azioni perché si trovano in uno stato particolare. È necessario invece cambiare lo stato e mantenerlo per un numero di periodi specificato. Per ulteriori informazioni, consulta [Metriche di monitoraggio con Amazon CloudWatch](#).

AWS CloudTrail Registri

CloudTrail fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon S3. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon S3, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#).

Amazon GuardDuty

[Amazon GuardDuty](#) è un servizio di rilevamento delle minacce che monitora continuamente i tuoi account, contenitori, carichi di lavoro e i dati all'interno del tuo AWS ambiente per identificare potenziali minacce o rischi per la sicurezza dei tuoi bucket S3. GuardDuty fornisce inoltre un contesto dettagliato sulle minacce rilevate. GuardDuty monitora i registri di AWS CloudTrail gestione delle minacce e fornisce informazioni rilevanti per la sicurezza. Ad esempio, GuardDuty includerà fattori di una richiesta API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e l'API specifica richiesta, che potrebbero essere insoliti nel tuo ambiente. [GuardDuty S3 Protection](#) monitora gli eventi relativi ai dati S3 raccolti da CloudTrail e identifica comportamenti potenzialmente anomali e dannosi in tutti i bucket S3 del tuo ambiente.

Log di accesso Amazon S3

I log di accesso al server forniscono record dettagliati relativi alle richieste che vengono effettuate a un bucket. I log di accesso al server sono utili per numerose applicazioni. Ad esempio, le informazioni del log di accesso possono essere utili nei controlli di accesso e di sicurezza. Puoi inviare i log ad Amazon CloudWatch Logs per l'interrogazione strutturata e l'aggregazione tra account o a un bucket Amazon S3 generico in formato testo senza alcun costo. Per ulteriori informazioni, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

AWS Trusted Advisor

Trusted Advisor si basa sulle migliori pratiche apprese servendo centinaia di migliaia di clienti. AWS Trusted Advisor esamina l'AWS ambiente e quindi formula raccomandazioni laddove esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza. Tutti i AWS clienti hanno accesso a cinque Trusted Advisor controlli. I clienti con un piano di supporto Business o Enterprise possono visualizzare tutti gli Trusted Advisor assegni.

Trusted Advisor dispone dei seguenti S3-related assegni Amazon:

- Registrazione della configurazione dei bucket Amazon S3.
- Controlli della sicurezza per i bucket di Amazon S3 dotati di autorizzazioni di accesso aperte.
- Controlli della tolleranza ai guasti per i bucket di Amazon S3 per i quali la funzione Controllo delle versioni non è abilitata o è sospesa.

Per ulteriori informazioni, consulta [AWS Trusted Advisor](#) nella Guida per l'utente di Supporto .

Amazon S3 Storage Lens

Amazon S3 Storage Lens è una funzionalità di analisi del cloud-storage che può essere utilizzata per ottenere visibilità a livello di organizzazione sull'utilizzo e l'attività dell'object-storage. È possibile utilizzare i parametri di S3 Storage Lens per generare approfondimenti, ad esempio per scoprire la quantità di spazio di archiviazione disponibile nell'intera organizzazione o quali sono i bucket e i prefissi caratterizzati da una crescita più rapida. Puoi anche utilizzare i parametri di S3 Storage Lens per individuare le opportunità di ottimizzazione dei costi, implementare le best practice di protezione e sicurezza dei dati e migliorare le prestazioni dei carichi di lavoro delle applicazioni.

S3 Storage Lens aggrega le metriche e visualizza le informazioni nella sezione Istantanea account della pagina Bucket della console Amazon S3. S3 Storage Lens fornisce anche una dashboard interattiva che può essere utilizzata per visualizzare le intuizioni e le tendenze, segnalare i valori anomali e ricevere raccomandazioni per ottimizzare i costi di storage e applicare le best practice per la protezione dei dati. La tua dashboard offre opzioni dettagliate per generare e visualizzare informazioni dettagliate a livello di organizzazione, account, classe di archiviazione Regione AWS, bucket, prefisso o gruppo Storage Lens. Per ulteriori informazioni, consulta [Informazioni su Amazon S3 Storage Lens](#).

Inventario Amazon S3

Inventario Amazon S3 genera un elenco di oggetti e metadati che è possibile utilizzare per interrogare e gestire gli oggetti. È possibile utilizzare questo report di inventario per generare dati granulari come la dimensione dell'oggetto, la data dell'ultima modifica, lo stato di crittografia e altri campi. Questi report sono disponibili giornalmente o settimanalmente per fornire automaticamente l'elenco più recente.

Ad esempio, è possibile utilizzare Inventario Amazon S3 per verificare e segnalare lo stato di replica e crittografia degli oggetti per esigenze aziendali, di conformità e normative. È inoltre possibile utilizzare Inventario Amazon S3 per semplificare e velocizzare i flussi di processo

aziendali e i processi sui big data, che fornisce un'alternativa pianificata alle operazioni API sincrone List di Amazon S3. Inventario Amazon S3 non utilizza le operazioni dell'API List per verificare gli oggetti e non influisce sulla velocità di richiesta del bucket. Per ulteriori informazioni, consulta [Catalogazione e analisi dei dati con Inventario S3](#).

Notifiche di eventi Amazon S3

Con la funzione Amazon S3 Event Notifications, si ricevono notifiche quando si verificano determinati eventi nel proprio bucket S3. Per abilitare le notifiche, aggiungi una configurazione di notifica che identifichi gli eventi che Amazon S3 deve pubblicare. Per ulteriori informazioni, consulta [Notifiche di eventi Amazon S3](#).

Amazon S3 e AWS X-Ray

AWS X-Ray si integra con Amazon S3 per tracciare le richieste upstream di aggiornamento dei bucket S3 della tua applicazione. Se un servizio traccia le richieste utilizzando l' X-Ray SDK, Amazon S3 può inviare le intestazioni di tracciamento ai sottoscrittori di eventi downstream come λ , Amazon SQS e Amazon SNS. X-Ray abilita i messaggi di tracciamento per le notifiche degli eventi di Amazon S3. Puoi utilizzare la mappa di X-Ray tracciamento per visualizzare le connessioni tra Amazon S3 e altri servizi utilizzati dalla tua applicazione. Per ulteriori informazioni, consulta [Amazon S3 e X-Ray](#)

Le best practice di sicurezza seguenti gestiscono anche il logging e il monitoraggio:

- [Identify and audit all your Amazon S3 buckets](#)
- [Implement monitoring using Amazon Web Services monitoring tools](#)
- [Attiva AWS Config](#)
- [Enable Amazon S3 server access logging](#)
- [Use CloudTrail](#)
- [Monitor Amazon Web Services security advisories](#)

Argomenti

- [Strumenti di monitoraggio](#)
- [Opzioni di registrazione per Amazon S3](#)
- [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#)
- [Registrazione delle richieste con registrazione dell'accesso al server](#)

- [Metriche di monitoraggio con Amazon CloudWatch](#)
- [Notifiche di eventi Amazon S3](#)
- [Monitoraggio dell'attività e dell'utilizzo dello storage con Amazon S3 Storage Lens](#)
- [Catalogazione e analisi dei dati con Inventario S3](#)

Strumenti di monitoraggio

AWS fornisce vari strumenti che puoi usare per monitorare Amazon S3. Alcuni di questi strumenti possono essere configurati in modo che eseguano automaticamente il monitoraggio, mentre altri richiedono l'intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

Strumenti di monitoraggio automatici

Per controllare Amazon S3 e segnalare l'eventuale presenza di problemi, puoi usare gli strumenti di monitoraggio automatici seguenti:

- Amazon CloudWatch Alarms: monitora una singola metrica in un periodo di tempo specificato ed esegui una o più azioni in base al valore della metrica relativo a una determinata soglia in un numero di periodi di tempo. L'azione è una notifica inviata a un argomento di Amazon Simple Notification Service (Amazon SNS) o a una policy di Amazon EC2 Auto Scaling. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare. Lo stato deve essere cambiato e restare costante per un numero specificato di periodi. Per ulteriori informazioni, consulta [Metriche di monitoraggio con Amazon CloudWatch](#).
- AWS CloudTrail Monitoraggio dei registri: condividi i file di CloudTrail registro tra account, monitora i file di registro in tempo reale inviandoli a CloudWatch Logs, scrivi applicazioni di elaborazione dei log in Java e verifica che i file di registro non siano cambiati dopo la consegna entro. CloudTrail Per ulteriori informazioni, consulta [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#).

Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio di Amazon S3 riguarda il monitoraggio manuale degli elementi non coperti dagli CloudWatch allarmi. Amazon S3 e altre Console di gestione AWS dashboard forniscono una panoramica immediata dello stato del tuo ambiente. CloudWatch Trusted Advisor AWS È possibile abilitare la registrazione degli accessi al server, che monitora le richieste

di accesso al bucket. Ogni record del log di accesso contiene i dettagli su una singola richiesta di accesso, ad esempio il richiedente, il nome del bucket, l'ora della richiesta, l'operazione della richiesta, lo stato della risposta e un eventuale codice di errore. Per ulteriori informazioni, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

- Il dashboard Amazon S3 mostra quanto segue:
 - I bucket e gli oggetti e le proprietà in essi contenuti.
- La CloudWatch home page mostra quanto segue:
 - Stato e allarmi attuali
 - Grafici degli allarmi e delle risorse
 - Stato di integrità dei servizi

Inoltre, è possibile utilizzare CloudWatch per effettuare le seguenti operazioni:

- Creare [pannelli di controllo personalizzati](#) per monitorare i servizi di interesse.
- Creare grafici dei dati dei parametri per la risoluzione di problemi e il rilevamento di tendenze.
- Cerca ed esplora tutte le metriche AWS delle tue risorse.
- Crea e modifica gli allarmi per ricevere le notifiche dei problemi.
- AWS Trusted Advisor può aiutarti a monitorare AWS le tue risorse per migliorare le prestazioni, l'affidabilità, la sicurezza e l'efficacia dei costi. Per tutti gli utenti sono disponibili quattro controlli di Trusted Advisor ; per gli utenti con un piano di assistenza Business o Enterprise sono disponibili più di 50 controlli. Per ulteriori informazioni, consulta [AWS Trusted Advisor](#).

Trusted Advisor dispone dei seguenti controlli relativi ad Amazon S3:

- Controlli della configurazione di registrazione dei bucket di Amazon S3.
- Controlli della sicurezza per i bucket di Amazon S3 dotati di autorizzazioni di accesso aperte.
- Controlli della tolleranza ai guasti per i bucket di Amazon S3 per i quali la funzione Controllo delle versioni non è abilitata o è sospesa.

Opzioni di registrazione per Amazon S3

Puoi registrare le azioni intraprese dagli utenti, dai ruoli o Servizi AWS sulle risorse di Amazon S3 e conservare i record di log per scopi di controllo e conformità. A tale scopo, è possibile utilizzare i log degli accessi al server, i log AWS CloudTrail o una combinazione di entrambi. Ti consigliamo di utilizzarlo CloudTrail per registrare le azioni a livello di bucket e a livello di oggetto per le tue risorse Amazon S3. Per ulteriori informazioni su ciascuna opzione, consulta le sezioni riportate di seguito.

- [Registrazione delle richieste con registrazione dell'accesso al server](#)
- [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#)

Amazon S3 offre due percorsi di distribuzione per i log di accesso al server: consegna diretta a un bucket Amazon S3 per uso generico e consegna ad Amazon Logs. CloudWatch Alcune funzionalità nella tabella seguente si applicano ai log di accesso al server solo tramite il percorso di consegna di Amazon CloudWatch Logs, come indicato.

La tabella seguente elenca le proprietà chiave dei CloudTrail log e dei log di accesso al server Amazon S3. Per assicurarti che CloudTrail soddisfi i tuoi requisiti di sicurezza, consulta la tabella e le note.

Proprietà dei log	AWS CloudTrail	Log di server Amazon S3
Può essere inoltrato ad altri sistemi (Amazon CloudWatch Logs, Amazon CloudWatch Events)	Sì	Sì
Distribuisce i log a più destinazioni (ad esempio, invia lo stesso log a due diversi bucket)	Sì	Sì ³
Attiva i log per un sottoinsieme di oggetti (prefisso)	Sì	No
Cross-account consegna dei log (bucket di destinazione e di origine di proprietà di account diversi)	Sì	Sì ³
Convalida dell'integrità del file di log mediante firma digitale o hashing	Sì	No
Valori predefiniti o scelta della crittografia per i file di log	Sì	Sì ³

Proprietà dei log	AWS CloudTrail	Log di server Amazon S3
Operazioni sugli oggetti (mediante le API Amazon S3)	Sì	Sì
Operazioni sui bucket (mediante le API Amazon S3)	Sì	Sì
Interfaccia utente ricercabile per i log	Sì	Sì ³
Campi per i parametri di blocco degli oggetti, proprietà Select di Amazon S3 per i record di log	Sì	No
Campi per Object Size, Total Time, Turn-Around Time e HTTP Referer per i record di log	No	Sì
Transizioni, scadenze e ripristini del ciclo di vita	No	Sì
Logging delle chiavi in un'operazione di eliminazione batch	Sì	Sì
Errori di autenticazione ¹	No	Sì
Account in cui vengono distribuiti i log	Proprietario del bucket ² e richiedente	proprietario del bucket e altri account con consegna Amazon Logs CloudWatch
Performance and Cost	AWS CloudTrail	Amazon S3 Server Logs

Proprietà dei log	AWS CloudTrail	Log di server Amazon S3
Prezzo	Gli eventi di gestione (prima distribuzione) sono gratuiti, gli eventi di dati sono a pagamento, oltre ai log di storage	Nessun costo per la consegna dei bucket Amazon S3 oltre allo storage dei log; tariffe CloudWatch vendute dei log per la consegna di Amazon CloudWatch Logs 3.
Velocità di distribuzione dei log	Eventi di dati ogni 5 minuti, eventi di gestione ogni 15 minuti	Entro qualche ora
Formato dei log	JSON	Space-delimited record di testo per la consegna a un bucket Amazon S3. JSON strutturato per la distribuzione ad Amazon CloudWatch Logs 3.

Note

1. CloudTrail non fornisce registri per le richieste che non superano l'autenticazione (in cui le credenziali fornite non sono valide) o che falliscono a causa del reindirizzamento (codice di errore). 301 Moved Permanently Include, tuttavia, i log di richieste in cui l'autenticazione non riesce (AccessDenied) e delle richieste effettuate da utenti anonimi.
2. Il proprietario del bucket S3 riceve CloudTrail i log quando l'account non ha accesso completo all'oggetto nella richiesta. Per ulteriori informazioni, consulta [Azioni a livello di oggetto Amazon S3 in scenari multi-account](#).
3. Oltre alla consegna diretta a un bucket Amazon S3, puoi inviare i log di accesso al server Amazon S3 ad Amazon Logs. CloudWatch Con questo percorso di consegna, ottieni funzionalità aggiuntive, tra cui l'inoltro verso altre destinazioni, la consegna a più destinazioni, l'aggregazione tra account e più regioni, la AWS KMS crittografia e l'interrogazione interattiva con Logs Insights. CloudWatch Puoi anche inviare questi log alle tabelle Amazon S3 in formato Apache Iceberg per l'analisi SQL. Per ulteriori informazioni, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

4. S3 non supporta la consegna di CloudTrail log o log di accesso al server al richiedente o al proprietario del bucket per le richieste degli endpoint VPC quando la policy degli endpoint VPC le nega o per le richieste che falliscono prima che la policy VPC venga valutata.

Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail

[AWS CloudTrail](#) è un servizio che fornisce un registro delle azioni intraprese da un utente, da un ruolo o da un Servizio AWS. CloudTrail acquisisce tutte le chiamate API per Amazon S3 come eventi. Le chiamate acquisite includono chiamate dalla console Amazon S3 e chiamate di codice alle operazioni API Amazon S3. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon S3, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWS Per ulteriori informazioni, vedere [Utilizzo della cronologia degli CloudTrail eventi nella Guida per l'utente](#). AWS CloudTrail La visualizzazione della cronologia degli eventi è gratuita. CloudTrail

Per una registrazione continua degli eventi negli Account AWS ultimi 90 giorni, crea un trail o un archivio dati sugli [eventi di](#) CloudTrail Lake.

CloudTrail sentieri

Un percorso consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando Console di gestione AWS sono multiregionali. È possibile creare un trail per una

singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata perché registri tutte le attività del tuo Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta [Creating a trail for your Account AWS](#) e [Creating a trail for an organization](#) nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia degli eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia sono previsti costi di archiviazione di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta Prezzi. [AWS CloudTrail](#) Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

CloudTrail Archivi dati per eventi sul lago

CloudTrail Lake ti consente di eseguire SQL-based query sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. <https://orc.apache.org/> ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i [selettori di eventi avanzati](#). I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, vedere [Lavorare con AWS CloudTrail Lake](#) nella Guida per l'utente. AWS CloudTrail

CloudTrail Gli archivi di dati e le interrogazioni relative agli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'[opzione di prezzo](#) da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta [AWS CloudTrail Prezzi](#).

È possibile archiviare i file di log nel bucket per un periodo di tempo indeterminato, ma è anche possibile definire regole per il ciclo di vita di Amazon S3 per archiviare o eliminare automaticamente i file di log. Per impostazione predefinita, i file di log sono crittografati mediante la crittografia lato server (SSE) di Amazon S3.

Utilizzo CloudTrail dei log con i log e CloudWatch i log di accesso al server Amazon S3

AWS CloudTrail i log forniscono una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon S3, mentre i log di accesso al server di Amazon S3 forniscono registrazioni

dettagliate delle richieste effettuate a un bucket S3. Per ulteriori informazioni sul funzionamento dei diversi log e delle relative proprietà, prestazioni e costi, consulta [the section called “Opzioni di registrazione”](#).

Puoi utilizzare AWS CloudTrail i log insieme ai log di accesso al server per Amazon S3. CloudTrail i log forniscono un monitoraggio dettagliato delle API per le operazioni a livello di bucket e di oggetto di Amazon S3. I log di accesso al server per Amazon S3 forniscono visibilità sulle operazioni a livello di oggetto sui dati in Amazon S3. Per ulteriori informazioni sui log degli accessi al server, consultare [Registrazione delle richieste con registrazione dell'accesso al server](#).

Puoi anche utilizzare i CloudTrail log insieme ad Amazon per Amazon S3. CloudWatch CloudTrail l'integrazione con CloudWatch Logs fornisce l'attività dell'API a livello di bucket S3 acquisita CloudTrail da un flusso di CloudWatch log nel gruppo di CloudWatch log specificato. Puoi creare CloudWatch allarmi per monitorare l'attività specifica dell'API e ricevere notifiche e-mail quando si verifica l'attività specifica dell'API. Per ulteriori informazioni sugli CloudWatch allarmi per il monitoraggio di attività specifiche dell'API, consulta la Guida per l'[AWS CloudTrail utente](#). Per ulteriori informazioni sull'utilizzo CloudWatch con Amazon S3, consulta [Metriche di monitoraggio con Amazon CloudWatch](#).

Note

S3 non supporta la consegna dei CloudTrail log al richiedente o al proprietario del bucket per le richieste degli endpoint VPC quando la policy sugli endpoint VPC li nega.

CloudTrail tracciamento con chiamate API SOAP di Amazon S3

CloudTrail tiene traccia delle chiamate API SOAP di Amazon S3. Il supporto SOAP di Amazon S3 su HTTP è obsoleto, ma è comunque disponibile su HTTPS. Per ulteriori informazioni sul supporto SOAP di Amazon S3, consulta [Appendice: API SOAP](#) nella Guida alle API di Amazon S3.

Important

Le funzioni più recenti di Amazon S3 non sono supportate per SOAP. Ti consigliamo di utilizzare l'API REST o gli AWS SDK.

La tabella seguente mostra le azioni SOAP di Amazon S3 tracciate mediante registrazione. CloudTrail

Nome API SOAP	Nome dell'evento API utilizzato nel registro CloudTrail
ListAllMyBuckets	ListBuckets
CreateBucket	CreateBucket
DeleteBucket	DeleteBucket
GetBucketAccessControlPolicy	GetBucketAc1
SetBucketAccessControlPolicy	PutBucketAc1
GetBucketLoggingStatus	GetBucketLogging
SetBucketLoggingStatus	PutBucketLogging

Per ulteriori informazioni su CloudTrail Amazon S3, consulta i seguenti argomenti:

Argomenti

- [Eventi Amazon S3 CloudTrail](#)
- [CloudTrail voci dei file di registro per Amazon S3 e S3 su Outposts](#)
- [Abilitazione della registrazione CloudTrail degli eventi per bucket e oggetti S3](#)
- [Identificazione delle richieste Amazon S3 utilizzando CloudTrail](#)

Eventi Amazon S3 CloudTrail

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon

S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS
Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

Questa sezione fornisce informazioni sugli eventi a cui S3 accede. CloudTrail

Eventi relativi ai dati di Amazon S3 in CloudTrail

Gli [eventi di dati](#) forniscono informazioni sulle operazioni delle risorse eseguite su o in una risorsa (ad esempio, lettura o scrittura su un oggetto Amazon S3). Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati. La cronologia CloudTrail degli eventi non registra gli eventi relativi ai dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni sui prezzi di CloudTrail, consulta [Prezzi di AWS CloudTrail](#).

Puoi registrare gli eventi di dati per i tipi di risorse di Amazon S3 utilizzando la CloudTrail console o AWS CLI le operazioni CloudTrail API. Per ulteriori informazioni su come registrare gli eventi di dati, consulta [Registrazione di eventi di dati con Console di gestione AWS](#) e [Registrazione di eventi di dati con AWS Command Line Interface](#) nella Guida all'utente AWS CloudTrail .

La tabella seguente elenca i tipi di risorse Amazon S3 per i quali è possibile registrare eventi di dati. La colonna Tipo di evento di dati (console) mostra il valore da scegliere dall'elenco dei tipi di eventi di dati sulla CloudTrail console. La colonna del valore resources.type mostra il resources.type valore da specificare durante la configurazione dei selettori di eventi avanzati utilizzando le API or. AWS CLI CloudTrail La CloudTrail colonna Data API loggate mostra le chiamate API registrate per il tipo di risorsa. CloudTrail

Tipo di evento di dati (console)	valore resources.type	API di dati a cui è stato effettuato l'accesso CloudTrail
S3	AWS::S3::Object	<ul style="list-style-type: none">• AbortMultipartUpload• CompleteMultipartUpload• CopyObject• CreateMultipartUpload• DeleteObject

Tipo di evento di dati (console)	valore resources.type	API di dati a cui è stato effettuato l'accesso CloudTrail
		<ul style="list-style-type: none">• DeleteObjectTagging• DeleteObjects• GetObject• GetObjectAcl• GetObjectAttributes• GetObjectLegalHold• GetObjectRetention• GetObjectTagging• GetObjectTorrent• HeadObject• HeadBucket• ListObjectVersions• ListObjects• ListParts• PutObject• PutObjectAcl• PutObjectLegalHold• PutObjectRetention• PutObjectTagging• PutObjectAnnotation• GetObjectAnnotation• ListObjectAnnotations• DeleteObjectAnnotation• RestoreObject• SelectObjectContent• UpdateObjectEncryption• UploadPart• UploadPartCopy

Tipo di evento di dati (console)	valore resources.type	API di dati a cui è stato effettuato l'accesso CloudTrail
S3 Express One Zone	AWS::S3Express::Object	<ul style="list-style-type: none">• AbortMultipartUpload• CompleteMultipartUpload• CreateSession• CopyObject• CreateMultipartUpload• DeleteObject• DeleteObjects• GetObject• GetObjectAttributes• HeadBucket• HeadObject• ListObjectsV2• ListParts• PutObject• UploadPart• UploadPartCopy

Tipo di evento di dati (console)	valore resources.type	API di dati a cui è stato effettuato l'accesso CloudTrail
Punto di accesso S3	AWS::S3::Access Point	<ul style="list-style-type: none">• AbortMultipartUpload• CompleteMultipartUpload• CopyObject (solo copie per la stessa Regione)• CreateMultipartUpload• DeleteObject• DeleteObjectTagging• GetObject• GetObjectAcl• GetObjectAttributes• GetObjectLegalHold• GetObjectRetention• GetObjectTagging• HeadBucket• HeadObject• ListObjects• ListObjectsV2• ListObjectVersions• ListParts• Presign• PutObject• PutObjectLegalHold• PutObjectRetention• PutObjectAcl• PutObjectTagging• RestoreObject• UploadPart

Tipo di evento di dati (console)	valore resources.type	API di dati a cui è stato effettuato l'accesso CloudTrail
		<ul style="list-style-type: none"> • UploadPartCopy (solo copie per la stessa Regione)
S3 Object Lambda	AWS::S3ObjectLambda::AccessPoint	<ul style="list-style-type: none"> • AbortMultipartUpload • CompleteMultipartUpload • CopyObject (solo copie per la stessa Regione) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetObject • GetObjectAcl • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • HeadObject • ListObjects • ListObjectVersions • ListParts • PutObject • PutObjectLegalHold • PutObjectRetention • PutObjectAcl • PutObjectTagging • RestoreObject • UploadPart • WriteGetObjectResponse

Tipo di evento di dati (console)	valore resources.type	API di dati a cui è stato effettuato l'accesso CloudTrail
S3 Outposts	AWS::S3Outposts::Object	<ul style="list-style-type: none"> • AbortMultipartUpload • CompleteMultipartUpload • CopyObject (solo copie per la stessa Regione) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetObject • GetObjectTagging • HeadObject • ListObjects • ListObjectsV2 • ListParts • PutObject • PutObjectTagging • UploadPart • UploadPartCopy

È possibile configurare selettori di eventi avanzati per filtrare i campi `eventName`, `readOnly` e `resources.ARN` per registrare solo gli eventi importanti per l'utente. Per ulteriori informazioni su questi campi, consulta [AdvancedFieldSelector](#) in Riferimento API AWS CloudTrail .

Eventi di gestione di Amazon S3 in CloudTrail

Amazon S3 registra tutte le operazioni del piano di controllo (control-plane) come eventi di gestione. Per ulteriori informazioni sulle operazioni dell'API S3, consulta la [documentazione di riferimento delle API di Amazon S3](#).

In che modo CloudTrail acquisisce le richieste fatte ad Amazon S3

Per impostazione predefinita, CloudTrail registra le chiamate API a livello di bucket S3 effettuate negli ultimi 90 giorni, ma non registra le richieste effettuate agli oggetti. Bucket-level le chiamate includono eventi come `CreateBucket`, `DeleteBucket`, `PutBucketLifecycle`, `PutBucketPolicy`, e così via. Puoi visualizzare gli eventi a livello di bucket sulla CloudTrail console. Tuttavia, non è possibile visualizzare gli eventi di dati (chiamate a livello di oggetto di Amazon S3) da lì: è necessario analizzarli o interrogarli nei log. CloudTrail

Se stai registrando l'attività dei dati con AWS CloudTrail, il record dell'evento per un evento di `DeleteObjects` dati di Amazon S3 include sia l'evento che un `DeleteObject` evento per ogni `DeleteObjects` oggetto eliminato come parte di tale operazione. È possibile escludere la visibilità aggiuntiva sugli oggetti eliminati dal record dell'evento. Per ulteriori informazioni, consulta [Esempi della AWS CLI per filtrare eventi di dati](#) nella Guida per l'utente dell'AWS CloudTrail .

L'`InitiateReplication` evento è incluso `objectAnnotationCount` nel campo. `additionalEventData` Questo valore indica il numero di annotazioni sull'oggetto di origine al momento dell'avvio della replica.

Azioni a livello di account di Amazon S3 tracciate mediante registrazione CloudTrail

CloudTrail registra le azioni a livello di account. I record Amazon S3 vengono scritti insieme ad altri Servizio AWS record in un file di registro. CloudTrail determina quando creare e scrivere su un nuovo file in base a un periodo di tempo e alle dimensioni del file.

Le tabelle di questa sezione elencano le azioni a livello di account di Amazon S3 supportate per la registrazione. CloudTrail

Le azioni API a livello di account di Amazon S3 tracciate dalla registrazione vengono visualizzate con i seguenti nomi di evento CloudTrail . I nomi degli CloudTrail eventi sono diversi dal nome dell'azione API. Ad esempio, `DeletePublicAccessBlock` è `DeleteAccountPublicAccessBlock`.

- [DeleteAccountPublicAccessBlock](#)
- [GetAccountPublicAccessBlock](#)
- [PutAccountPublicAccessBlock](#)

Azioni a livello di bucket di Amazon S3 tracciate mediante registrazione CloudTrail

Per impostazione predefinita, CloudTrail registra le azioni a livello di bucket per bucket generici. I record Amazon S3 vengono scritti insieme ad altri record di AWS servizio in un file di registro. CloudTrail determina quando creare e scrivere su un nuovo file in base a un periodo di tempo e alle dimensioni del file.

Questa sezione elenca le azioni a livello di bucket di Amazon S3 supportate per la registrazione tramite CloudTrail

Le azioni API a livello di bucket di Amazon S3 tracciate dalla registrazione vengono visualizzate con i seguenti nomi di evento CloudTrail. In alcuni casi, il nome dell' CloudTrail evento è diverso dal nome dell'azione API. Ad esempio, PutBucketLifecycleConfiguration è PutBucketLifecycle.

- [CreateBucket](#)
- [CreateBucketMetadataConfiguration](#) (operazione API V2)
- [CreateBucketMetadataTableConfiguration](#) (operazione API V1)
- [DeleteBucket](#)
- [DeleteBucketAnalyticsConfiguration](#)
- [DeleteBucketCors](#)
- [DeleteBucketEncryption](#)
- [DeleteBucketIntelligentTieringConfiguration](#)
- [DeleteBucketInventoryConfiguration](#)
- [DeleteBucketLifecycle](#)
- [DeleteBucketMetadataConfiguration](#) (operazione API V2)
- [DeleteBucketMetadataTableConfiguration](#) (operazione API V1)
- [DeleteBucketMetricsConfiguration](#)
- [DeleteBucketOwnershipControls](#)
- [DeleteBucketPolicy](#)
- [DeleteBucketPublicAccessBlock](#)
- [DeleteBucketReplication](#)
- [DeleteBucketTagging](#)
- [GetAccelerateConfiguration](#)
- [GetBucketAcl](#)

- [GetBucketAnalyticsConfiguration](#)
- [GetBucketCors](#)
- [GetBucketEncryption](#)
- [GetBucketIntelligentTieringConfiguration](#)
- [GetBucketInventoryConfiguration](#)
- [GetBucketLifecycle](#)
- [GetBucketLocation](#)
- [GetBucketLogging](#)
- [GetBucketMetadataConfiguration](#) (operazione API V2)
- [GetBucketMetadataTableConfiguration](#) (operazione API V1)
- [GetBucketMetricsConfiguration](#)
- [GetBucketNotification](#)
- [GetBucketObjectLockConfiguration](#)
- [GetBucketOwnershipControls](#)
- [GetBucketPolicy](#)
- [GetBucketPolicyStatus](#)
- [GetBucketPublicAccessBlock](#)
- [GetBucketReplication](#)
- [GetBucketRequestPayment](#)
- [GetBucketTagging](#)
- [GetBucketVersioning](#)
- [GetBucketWebsite](#)
- [HeadBucket](#)
- [ListBuckets](#)
- [PutAccelerateConfiguration](#)
- [PutBucketAcl](#)
- [PutBucketAnalyticsConfiguration](#)
- [PutBucketCors](#)
- [PutBucketEncryption](#)
- [PutBucketIntelligentTieringConfiguration](#)

- [PutBucketInventoryConfiguration](#)
- [PutBucketLifecycle](#)
- [PutBucketLogging](#)
- [PutBucketMetricsConfiguration](#)
- [PutBucketNotification](#)
- [PutBucketObjectLockConfiguration](#)
- [PutBucketOwnershipControls](#)
- [PutBucketPolicy](#)
- [PutBucketPublicAccessBlock](#)
- [PutBucketReplication](#)
- [PutBucketRequestPayment](#)
- [PutBucketTagging](#)
- [PutBucketVersioning](#)
- [PutBucketWebsite](#)
- [UpdateBucketMetadataJournalTableConfiguration](#)
- [UpdateBucketMetadataInventoryTableConfiguration](#)
- [UpdateBucketMetadataAnnotationTableConfiguration](#)

Oltre a tali operazioni API, è possibile utilizzare anche l'operazione a livello di oggetto [oggetto OPTIONS](#). Questa azione viene trattata come un'azione a livello di bucket nella CloudTrail registrazione perché controlla la configurazione CORS di un bucket.

 Note

L' HeadBucket API è supportata come evento di dati Amazon S3 in. CloudTrail

Azioni a livello di bucket di Amazon S3 Express One Zone (endpoint API regionale) tracciate mediante registrazione CloudTrail

Per impostazione predefinita, CloudTrail registra le azioni a livello di bucket per i bucket di directory come eventi di gestione. Gli eventi eventsource di CloudTrail gestione per S3 Express One Zone sono. `s3express.amazonaws.com`

Le seguenti operazioni dell'API degli endpoint regionali vengono registrate. CloudTrail

- [CreateBucket](#)
- [DeleteBucket](#)
- [DeleteBucketPolicy](#)
- [GetBucketPolicy](#)
- [PutBucketPolicy](#)
- [ListDirectoryBuckets](#)
- [PutBucketEncryption](#)
- [GetBucketEncryption](#)
- [DeleteBucketEncryption](#)

Per ulteriori informazioni, consulta [Registrazione con AWS CloudTrail per S3 Express One Zone](#)

Azioni a livello di oggetto Amazon S3 in scenari multi-account

Di seguito sono riportati casi d'uso speciali che riguardano le chiamate API a livello di oggetto in scenari con più account e il modo in cui vengono segnalati i log. CloudTrail CloudTrail invia i log al richiedente (l'account che ha effettuato la chiamata API), tranne in alcuni casi di accesso negato in cui le voci di registro vengono cancellate o omesse. Quando si imposta l'accesso multiaccount, considerare gli esempi riportati in questa sezione.

Note

Gli esempi presuppongono che i CloudTrail log siano configurati in modo appropriato.

Esempio 1: CloudTrail consegna i log al proprietario del bucket

CloudTrail consegna i log al proprietario del bucket anche se il proprietario del bucket non dispone delle autorizzazioni per la stessa operazione API dell'oggetto. Si consideri il seguente scenario multiaccount:

- L'account A possiede il bucket.
- L'account B (richiedente) tenta di accedere a un oggetto in quel bucket.
- L'account C è proprietario dell'oggetto. L'account C potrebbe essere o non essere lo stesso account dell'account A.

 Note

CloudTrail fornisce sempre i log API a livello di oggetto al richiedente (Account B). CloudTrail inoltre, fornisce gli stessi log al proprietario del bucket (Account A) anche quando il proprietario del bucket non possiede l'oggetto (Account C) o non dispone delle autorizzazioni per le stesse operazioni API su quell'oggetto.

Esempio 2: non CloudTrail fa proliferare gli indirizzi e-mail utilizzati nell'impostazione degli ACL degli oggetti

Si consideri il seguente scenario multiaccount:

- L'account A possiede il bucket.
- L'account B (richiedente) invia una richiesta per impostare un'assegnazione nell'ACL dell'oggetto utilizzando un indirizzo e-mail. Per ulteriori informazioni sulle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

Il richiedente recupera i log insieme alle informazioni dell'e-mail. Tuttavia, il proprietario del bucket, se è idoneo a ricevere i log, come nell'esempio 1, riceve il registro che riporta l'evento. CloudTrail Tuttavia, il proprietario del bucket non riceve le informazioni sulla configurazione dell'ACL, in particolare l'indirizzo e-mail dell'assegnatario e l'assegnazione. L'unica informazione riportata nel log per il proprietario del bucket è che l'account B ha effettuato una chiamata dell'API ACL.

CloudTrail voci dei file di registro per Amazon S3 e S3 su Outposts

 Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite da Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

Un evento rappresenta una singola richiesta da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

Note

Per visualizzare esempi di file di CloudTrail registro per Amazon S3 Express One Zone, consulta Esempi di file di [CloudTrail registro per S3 Express One Zone](#).

Per maggiori informazioni, consulta i seguenti esempi.

Argomenti

- [Esempio: immissione in un file di CloudTrail registro per Amazon S3](#)

Esempio: immissione in un file di CloudTrail registro per Amazon S3

L'esempio seguente mostra una voce di CloudTrail registro che illustra il [GET servizio e PutBucketAcl](#) [GetBucketVersioning](#) le azioni.

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2019-02-01T03:18:19Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "ListBuckets",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "[]",
      "requestParameters": {
        "host": [
```

```

        "s3.us-west-2.amazonaws.com"
    ],
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV2",
        "AuthenticationMethod": "QueryString",
        "aclRequired": "Yes"
    },
    },
    "requestID": "47B8E8D397DCE7A6",
    "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "s3.amazonaws.com"
    }
},
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
    },
    "eventTime": "2019-02-01T03:22:33Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "PutBucketAcl",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "[]",
    "requestParameters": {
        "bucketName": "",
        "AccessControlPolicy": {
            "AccessControlList": {
                "Grant": {
                    "Grantee": {
                        "xsi:type": "CanonicalUser",
                        "xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",

```

```

        "ID":
        "d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
      },
      "Permission": "FULL_CONTROL"
    }
  },
  "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/",
  "Owner": {
    "ID":
    "d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
  }
},
"host": [
  "s3.us-west-2.amazonaws.com"
],
"acl": [
  ""
]
},
"responseElements": null,
"additionalEventData": {
  "SignatureVersion": "SigV4",
  "CipherSuite": "ECDHE-RSA-AES128-SHA",
  "AuthenticationMethod": "AuthHeader"
},
"requestID": "BD8798EACDD16751",
"eventID": "607b9532-1423-41c7-b048-ec2641693c47",
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "s3.amazonaws.com"
}
},
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:user/myUserName",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "myUserName"
  }
}

```

```

    },
    "eventTime": "2019-02-01T03:26:37Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetBucketVersioning",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
    "userAgent": "[]",
    "requestParameters": {
      "host": [
        "s3.us-west-2.amazonaws.com"
      ],
      "bucketName": "amzn-s3-demo-bucket1",
      "versioning": [
        ""
      ]
    },
    "responseElements": null,
    "additionalEventData": {
      "SignatureVersion": "SigV4",
      "CipherSuite": "ECDHE-RSA-AES128-SHA",
      "AuthenticationMethod": "AuthHeader"
    },
    "requestID": "07D681279BD94AED",
    "eventID": "f2b287f3-0df1-4961-a2f4-c4bdfed47657",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "s3.amazonaws.com"
    }
  }
]
}

```

Abilitazione della registrazione CloudTrail degli eventi per bucket e oggetti S3

Puoi utilizzare gli eventi di CloudTrail dati per ottenere informazioni sulle richieste a livello di bucket e oggetto in Amazon S3. Per abilitare gli eventi di CloudTrail dati per tutti i tuoi bucket o per un elenco di bucket specifici, devi [creare un percorso manualmente in CloudTrail](#)

 Note

- L'impostazione predefinita per CloudTrail è trovare solo gli eventi di gestione. Assicurarsi che gli eventi di dati siano abilitati per l'account.
- Con un bucket S3 che genera un carico di lavoro elevato, è possibile generare migliaia di log in un breve lasso di tempo. Tieni presente per quanto tempo scegli di abilitare gli eventi di CloudTrail dati per un bucket occupato.

CloudTrail archivia i log degli eventi di dati di Amazon S3 in un bucket S3 a tua scelta. Prendi in considerazione l'utilizzo di un bucket separato Account AWS per organizzare meglio gli eventi di più bucket che potresti possedere in un posto centrale per facilitare le interrogazioni e l'analisi. AWS Organizations ti aiuta a creare un Account AWS file collegato all'account proprietario del bucket che stai monitorando. Per ulteriori informazioni, vedi [Che cos'è AWS Organizations?](#) nella Guida AWS Organizations per l'utente.

Quando registri gli eventi di dati per un trail in CloudTrail, puoi scegliere di utilizzare selettori di eventi avanzati o selettori di eventi di base per registrare eventi di dati per oggetti archiviati in bucket generici. Per registrare gli eventi di dati per gli oggetti memorizzati nei bucket della directory, è necessario utilizzare selettori di eventi avanzati. Per ulteriori informazioni, consulta [Registrazione con S3 Express One AWS CloudTrail Zone](#).

Quando crei un percorso nella CloudTrail console utilizzando selettori di eventi avanzati, nella sezione eventi dati, puoi scegliere Registra tutti gli eventi per il modello Log selector per registrare tutti gli eventi a livello di oggetto. Quando crei un percorso nella CloudTrail console utilizzando selettori di eventi di base, nella sezione eventi dati, puoi selezionare la casella di controllo Seleziona tutti i bucket S3 nel tuo account per registrare tutti gli eventi a livello di oggetto.

 Note

- È una best practice la creazione di una configurazione del ciclo di vita per il bucket degli eventi di dati AWS CloudTrail. Definisci la configurazione del ciclo di vita in modo tale da rimuovere periodicamente i file di log al termine del periodo di tempo desiderato per l'audit. In questo modo, si riduce la quantità di dati analizzati da Athena per ogni query. Per ulteriori informazioni, consulta [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#).

- Per ulteriori informazioni sul formato della registrazione, consulta [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#).
- Per esempi di come interrogare CloudTrail i log, consulta il post del AWS Big Data Blog [Analyze Security, Compliance, and Operational Activity Using and Amazon Athena. AWS CloudTrail](#)

Abilitazione della registrazione per gli oggetti in un bucket utilizzando la console

È possibile utilizzare la AWS CloudTrail console per configurare un CloudTrail percorso per registrare gli eventi di dati per gli oggetti in un bucket S3. CloudTrail supporta la registrazione di operazioni API a livello di oggetto di Amazon S3 come, e. GetObject DeleteObject PutObject Questi eventi vengono chiamati eventi di dati.

Per impostazione predefinita, i CloudTrail percorsi non registrano eventi di dati, ma puoi configurare i percorsi per registrare eventi di dati per i bucket S3 specificati o per registrare eventi di dati per tutti i bucket Amazon S3 presenti nel tuo. Account AWS Per ulteriori informazioni, consulta [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#).

CloudTrail non inserisce eventi di dati nella cronologia degli eventi. CloudTrail Inoltre, non tutte le azioni a livello di bucket sono inserite nella cronologia degli eventi. CloudTrail Per ulteriori informazioni sulle azioni API a livello di bucket di Amazon S3 tracciate mediante registrazione, consulta. CloudTrail [Azioni a livello di bucket di Amazon S3 tracciate mediante registrazione CloudTrail](#) Per ulteriori informazioni su come interrogare CloudTrail i log, consulta l'articolo del AWS Knowledge Center sull'[uso dei pattern di filtro di Amazon Logs e Amazon CloudWatch Athena per interrogare i log. CloudTrail](#)

Note

Se stai registrando l'attività dei dati con AWS CloudTrail, il record dell'evento per un evento di DeleteObjects dati di Amazon S3 include sia l>DeleteObjectsevento che un DeleteObject evento per ogni oggetto eliminato come parte di tale operazione. È possibile escludere la visibilità aggiuntiva sugli oggetti eliminati dal record dell'evento. Per ulteriori informazioni, consulta [Esempi della AWS CLI per filtrare eventi di dati](#) nella Guida per l'utente dell'AWS CloudTrail .

Per abilitare la registrazione degli eventi di CloudTrail dati per gli oggetti in un bucket S3 generico o in un bucket di directory S3, consulta [Creating a trail with the console nella Guida per l'utente. CloudTrail](#) AWS CloudTrail

Per ulteriori informazioni sulla registrazione dei log di un oggetto in un bucket di directory S3, consulta [Registrazione con AWS CloudTrail per bucket di directory](#).

Per informazioni sull'utilizzo della CloudTrail console per configurare un percorso per la registrazione degli eventi relativi ai dati S3, consulta Registrazione degli eventi relativi ai dati nella [Guida per l'utente](#). AWS CloudTrail

Per disabilitare la registrazione degli eventi di CloudTrail dati per gli oggetti in un bucket S3, vedi [Eliminazione di un percorso con la console nella Guida per l' CloudTrail utente](#). AWS CloudTrail

 Important

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di AWS CloudTrail](#).

Per ulteriori informazioni sulla CloudTrail registrazione con i bucket S3, consulta i seguenti argomenti:

- [Creazione di un bucket per uso generico](#)
- [Visualizzazione delle proprietà di un bucket per uso generico S3](#)
- [Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail](#)
- [Utilizzo dei file di CloudTrail registro](#) nella Guida per l'utente AWS CloudTrail

Identificazione delle richieste Amazon S3 utilizzando CloudTrail

In Amazon S3, puoi identificare le richieste utilizzando un registro AWS CloudTrail degli eventi. AWS CloudTrail è il modo preferito per identificare le richieste di Amazon S3, ma se utilizzi i log di accesso al server Amazon S3, consulta. [the section called “Identificazione delle richieste S3”](#)

Argomenti

- [Identificazione delle richieste effettuate ad Amazon S3 in un registro CloudTrail](#)
- [Identificazione delle richieste Amazon S3 Signature versione 2 utilizzando CloudTrail](#)
- [Identificazione dell'accesso agli oggetti S3 utilizzando CloudTrail](#)

Identificazione delle richieste effettuate ad Amazon S3 in un registro CloudTrail

Dopo aver configurato CloudTrail la distribuzione degli eventi a un bucket, dovresti iniziare a vedere gli oggetti arrivare al bucket di destinazione sulla console Amazon S3. Questi sono formattati come riportato di seguito:

```
s3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/Region/yyyy/mm/dd
```

Gli eventi registrati CloudTrail vengono archiviati come oggetti gzipped JSON compressi nel bucket S3. Per trovare in modo efficiente le richieste, dovresti utilizzare un servizio come Amazon Athena per indicizzare e interrogare i log. CloudTrail

Per ulteriori informazioni su CloudTrail e Athena, consulta [Creating the table for AWS CloudTrail logs in Athena using partition projection](#) nella Amazon Athena User Guide.

Identificazione delle richieste Amazon S3 Signature versione 2 utilizzando CloudTrail

Puoi utilizzare un registro CloudTrail eventi per identificare quale versione di firma API è stata utilizzata per firmare una richiesta in Amazon S3. Questa possibilità è importante perché il supporto di Signature Version 2 sta per essere disattivato perché obsoleto. Dopo, Amazon S3 non accetterà più le richieste che usano Signature Version 2 e tutte le richieste dovranno usare la firma Signature Version 4.

Ti consigliamo vivamente di CloudTrail utilizzarlo per determinare se qualcuno dei tuoi flussi di lavoro utilizza la firma Signature versione 2. Nel caso, correggili aggiornando le librerie e il codice in modo che utilizzino invece Signature Version 4 per evitare qualsiasi impatto sul business.

Per ulteriori informazioni, consulta [Annuncio: AWS CloudTrail per Amazon S3 vengono aggiunti nuovi campi per un controllo](#) di sicurezza avanzato. AWS re:Post

Note

CloudTrail gli eventi per Amazon S3 includono la versione della firma nei dettagli della richiesta sotto il nome chiave di `additionalEventData`. Per trovare la versione della firma sulle richieste fatte per oggetti in Amazon S3, ad esempio GET, e sulle DELETE richieste PUT, devi abilitare gli eventi CloudTrail relativi ai dati. (Questa funzionalità è disattivata per impostazione predefinita).

AWS CloudTrail è il metodo preferito per identificare le richieste di Signature Version 2. Se utilizzi i log degli accessi del server Amazon S3, consulta [Identificazione delle richieste di Signature Version 2](#).

Argomenti

- [Esempi di query Athena per l'identificazione di richieste Amazon S3 Signature versione 2](#)
- [Partizionamento dei dati di Signature versione 2](#)

Esempi di query Athena per l'identificazione di richieste Amazon S3 Signature versione 2

Example— Seleziona tutti gli eventi di Signature Version 2 e stampa solo EventTime, S3_Action, Region Request_Parameters, SourceIP e UserAgent

Nella query Athena seguente sostituisci *s3_cloudtrail_events_db.cloudtrail_table* con i dettagli Athena e aumenta o rimuovi il limite in base alle necessità.

```
SELECT EventTime, EventName as S3_Action, requestParameters as Request_Parameters,  
       awsregion as AWS_Region, sourceipaddress as Source_IP, useragent as User_Agent  
FROM s3_cloudtrail_events_db.cloudtrail_table  
WHERE eventsource='s3.amazonaws.com'  
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'  
LIMIT 10;
```

Example- Selezionare tutti i richiedenti che inviano traffico di tipo Signature versione 2

```
SELECT useridentity.arn, Count(requestid) as RequestCount  
FROM s3_cloudtrail_events_db.cloudtrail_table  
WHERE eventsource='s3.amazonaws.com'  
      and json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'  
Group by useridentity.arn
```

Partizionamento dei dati di Signature versione 2

Se è necessario eseguire query su una grande quantità di dati, è possibile ridurre i costi e i tempi di esecuzione di Athena creando una tabella partizionata.

Per farlo, creare una nuova tabella con partizioni nel modo seguente.

```
CREATE EXTERNAL TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned(  
    eventversion STRING,  
    userIdentity STRUCT<  
        type:STRING,  
        principalid:STRING,  
        arn:STRING,  
        accountid:STRING,  
        invokedby:STRING,  
        accesskeyid:STRING,  
        userName:STRING,  
    sessioncontext:STRUCT<  
        attributes:STRUCT<  
            mfaauthenticated:STRING,  
            creationdate:STRING>,  
        sessionIssuer:STRUCT<  
            type:STRING,  
            principalId:STRING,  
            arn:STRING,  
            accountId:STRING,  
            userName:STRING>  
        >  
    >,  
    eventTime STRING,  
    eventSource STRING,  
    eventName STRING,  
    awsRegion STRING,  
    sourceIpAddress STRING,  
    userAgent STRING,  
    errorCode STRING,  
    errorMessage STRING,  
    requestParameters STRING,  
    responseElements STRING,  
    additionalEventData STRING,  
    requestId STRING,  
    eventId STRING,  
    resources ARRAY<STRUCT<ARN:STRING,accountId: STRING,type:STRING>>,  
    eventType STRING,  
    apiVersion STRING,  
    readOnly STRING,  
    recipientAccountId STRING,  
    serviceEventDetails STRING,
```

```

        sharedEventID STRING,
        vpcEndpointId STRING
    )
    PARTITIONED BY (region string, year string, month string, day string)
    ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
    STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
    OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
    LOCATION 's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/';

```

Quindi creare le partizioni individualmente. Non è possibile ottenere risultati da date che non sono state create.

```

ALTER TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned ADD
    PARTITION (region= 'us-east-1', year= '2019', month= '02', day= '19') LOCATION
    's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/CloudTrail/us-east-1/2019/02/19/'
    PARTITION (region= 'us-west-1', year= '2019', month= '02', day= '19') LOCATION
    's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/CloudTrail/us-west-1/2019/02/19/'
    PARTITION (region= 'us-west-2', year= '2019', month= '02', day= '19') LOCATION
    's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/CloudTrail/us-west-2/2019/02/19/'
    PARTITION (region= 'ap-southeast-1', year= '2019', month= '02', day= '19') LOCATION
    's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/CloudTrail/ap-southeast-1/2019/02/19/'
    PARTITION (region= 'ap-southeast-2', year= '2019', month= '02', day= '19') LOCATION
    's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/CloudTrail/ap-southeast-2/2019/02/19/'
    PARTITION (region= 'ap-northeast-1', year= '2019', month= '02', day= '19') LOCATION
    's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/CloudTrail/ap-northeast-1/2019/02/19/'
    PARTITION (region= 'eu-west-1', year= '2019', month= '02', day= '19') LOCATION
    's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/CloudTrail/eu-west-1/2019/02/19/'
    PARTITION (region= 'sa-east-1', year= '2019', month= '02', day= '19') LOCATION
    's3://amzn-s3-demo-bucket1/AWSLogs/11112223333/CloudTrail/sa-east-1/2019/02/19/';

```

È quindi possibile effettuare la richiesta sulla base di queste partizioni e non è necessario caricare l'intero bucket.

```

SELECT useridentity.arn,
Count(requestid) AS RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table_partitioned
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'

```

```
AND region='us-east-1'  
AND year='2019'  
AND month='02'  
AND day='19'  
Group by useridentity.arn
```

Identificazione dell'accesso agli oggetti S3 utilizzando CloudTrail

Puoi utilizzare i registri AWS CloudTrail degli eventi per identificare le richieste di accesso agli oggetti di Amazon S3 per eventi di dati come `GetObject` `DeleteObject` `PutObject`, e e scoprire informazioni aggiuntive su tali richieste.

Note

Se stai registrando l'attività dei dati con AWS CloudTrail, il record dell'evento per un evento di `DeleteObjects` dati di Amazon S3 include sia l'`DeleteObject` evento che un `DeleteObject` evento per ogni oggetto eliminato come parte di tale operazione. È possibile escludere la visibilità aggiuntiva sugli oggetti eliminati dal record dell'evento. Per ulteriori informazioni, consulta [Esempi della AWS CLI per filtrare eventi di dati](#) nella Guida per l'utente dell'AWS CloudTrail .

L'esempio seguente mostra come ottenere tutte le richieste di PUT oggetti per Amazon S3 da un AWS CloudTrail registro eventi.

Argomenti

- [Esempi di query Athena per l'identificazione di richieste di accesso agli oggetti Amazon S3](#)

Esempi di query Athena per l'identificazione di richieste di accesso agli oggetti Amazon S3

Negli esempi di query Athena seguenti sostituisci

`s3_cloudtrail_events_db.cloudtrail_table` con i dettagli Athena e modifica l'intervallo della data in base alle necessità.

Example— Seleziona tutti gli eventi che hanno richieste di accesso agli oggetti PUT e stampa solo `EventTime`, `sourceIP` `EventSource`, `UserAgent` `BucketName`, `object` e `UserArn`

```
SELECT
```



```

    eventTime,
    eventName,
    eventSource,
    sourceIpAddress,
    userAgent,
    json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
    json_extract_scalar(requestParameters, '$.key') as object,
    userIdentity.arn as userArn
FROM
    s3_cloudtrail_events_db.cloudtrail_table
WHERE
    eventName = 'PutObject'
    AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'

```

Example— Seleziona tutti gli eventi che hanno richieste di accesso agli oggetti GET e stampa solo,, sourceIP EventTime,, EventSource, object e UserArn UserAgent BucketName

```

SELECT
    eventTime,
    eventName,
    eventSource,
    sourceIpAddress,
    userAgent,
    json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
    json_extract_scalar(requestParameters, '$.key') as object,
    userIdentity.arn as userArn
FROM
    s3_cloudtrail_events_db.cloudtrail_table
WHERE
    eventName = 'GetObject'
    AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'

```

Example— Seleziona tutti gli eventi anonimi dei richiedenti in un bucket in un determinato periodo e stampa solo EventTime,, sourceIP,, EventName EventSource, userArn e AccountID UserAgent BucketName

```

SELECT
    eventTime,
    eventName,
    eventSource,
    sourceIpAddress,

```

```
userAgent,  
json_extract_scalar(requestParameters, '$.bucketName') as bucketName,  
userIdentity.arn as userArn,  
userIdentity.accountId  
FROM  
  s3_cloudtrail_events_db.cloudtrail_table  
WHERE  
  userIdentity.accountId = 'anonymous'  
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example: identifica tutte le richieste che richiedono una ACL per l'autorizzazione

L'esempio di query Amazon Athena seguente mostra come identificare tutte le richieste relative ai bucket S3 che richiedono una lista di controllo degli accessi (ACL) per l'autorizzazione. Se la richiesta richiede una ACL per l'autorizzazione, il valore `aclRequired` in `additionalEventData` è `Yes`. Se non sono richieste ACL, `aclRequired` non è presente. È possibile utilizzare queste informazioni per eseguire la migrazione delle autorizzazioni ACL alle policy di bucket appropriate. Dopo aver creato queste policy per i bucket, è possibile disabilitare le ACL per questi bucket. Per ulteriori informazioni sulla disabilitazione delle ACL, consulta [Prerequisiti per la disabilitazione delle ACL](#).

```
SELECT  
  eventTime,  
  eventName,  
  eventSource,  
  sourceIpAddress,  
  userAgent,  
  userIdentity.arn as userArn,  
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,  
  json_extract_scalar(requestParameters, '$.key') as object,  
  json_extract_scalar(additionalEventData, '$.aclRequired') as aclRequired  
FROM  
  s3_cloudtrail_events_db.cloudtrail_table  
WHERE  
  json_extract_scalar(additionalEventData, '$.aclRequired') = 'Yes'  
  AND eventTime BETWEEN '2022-05-10T00:00:00Z' and '2022-08-10T00:00:00Z'
```

Note

- Questi esempi di query possono essere utili anche per il monitoraggio della sicurezza. Puoi rivedere i risultati per le chiamate `PutObject` o `GetObject` da indirizzi IP o richiedenti imprevisti o non autorizzati e per l'identificazione di eventuali richieste anonime ai bucket.

- La query recupera solo le informazioni a partire dall'orario in cui è stata abilitata la registrazione.

Se utilizzi i log di accesso al server Amazon S3, consulta [Identificazione delle richieste di accesso agli oggetti](#).

Registrazione delle richieste con registrazione dell'accesso al server

La registrazione degli accessi al server fornisce record dettagliati per le richieste che sono effettuate a un bucket. I log di accesso al server possono essere utilizzati per l'analisi operativa, per comprendere il livello di sicurezza e per ricaricare gli utenti.

Amazon S3 raccoglie periodicamente i record dei log di accesso, li consolida e li consegna alla destinazione prescelta. Puoi inviare i log ad Amazon Logs o a un CloudWatch bucket Amazon S3 per uso generico.

Note

I log di accesso al server non registrano informazioni sugli errori di reindirizzamento in regioni errate per le regioni avviate dopo il 20 marzo 2019. Wrong-Region gli errori di reindirizzamento si verificano quando una richiesta per un oggetto o un bucket viene effettuata al di fuori della regione in cui esiste il bucket.

Opzioni di distribuzione

È possibile inviare i log di accesso al server a due destinazioni. Puoi usarne uno o entrambi.

- Amazon CloudWatch Logs: invia i log in formato strutturato a un gruppo di CloudWatch log Logs. Puoi interrogare i CloudWatch log con Logs Insights, aggregare i log tra account e regioni e crittografare i log con AWS KMS. Dal gruppo di log, puoi anche inviare i log ad Amazon S3 in formato JSON o Apache Parquet oppure eseguire il mirroring dei log alle tabelle S3 in formato Apache Iceberg per l'analisi SQL. CloudWatch Si applicano le tariffe di inserimento dei log di venduto.

- Bucket Amazon S3 per uso generico: consegna i log in formato di testo delimitato da spazi a un bucket Amazon S3 specificato. La consegna dei log è gratuita. Paghi solo per l'archiviazione dei file di registro. Il bucket di destinazione deve trovarsi nello stesso bucket Regione AWS e Account AWS nel bucket di origine.

La tabella seguente mette a confronto le due opzioni di consegna.

Confronto delle opzioni di consegna dei log di accesso al server

Funzionalità	Amazon CloudWatch Logs	Bucket per uso generico Amazon S3
Destinazioni	CloudWatch Gruppo di log, Amazon S3 (JSON o Parquet) o Amazon Data Firehose. La distribuzione del gruppo di CloudWatch log Logs può essere estesa per eseguire il mirroring dei log su tabelle S3 in formato Iceberg.	Bucket Amazon S3 (testo delimitato da spazi)
Formato dei log	JSON strutturato (gruppo di log), JSON o Apache Parquet (Amazon S3), Apache Iceberg (tabelle S3)	Space-delimited testo
Esecuzione di query	CloudWatch Logs Insights (gruppo di log), Amazon Athena o Spark (tabelle S3)	Amazon Athena
Analisi SQL tramite tabelle S3	Sì (mirror Iceberg automatico)	No (richiede ETL)
Cross-account aggregazione	Sì (le destinazioni Amazon S3 e Firehose supportano la consegna tra più account)	No (solo per lo stesso account)

Funzionalità	Amazon CloudWatch Logs	Bucket per uso generico Amazon S3
Cross-Region aggregazione	Sì (le destinazioni Amazon S3 e Firehose supportano la consegna in più regioni)	No (solo nella stessa regione)
AWS KMS crittografia	Sì	No (SSE-S3 solo)
Configurazione	CloudWatch API di log o console Amazon S3	API o console Amazon S3 (PutBucketLogging
Latenza di consegna	Entro qualche ora	Entro qualche ora

Best-effort consegna dei log del server

I record dei log degli accessi al server vengono distribuiti sulla base del miglior tentativo. La maggior parte delle richieste di un bucket correttamente configurato per la registrazione determinano la consegna di un report del log. La maggior parte dei record vengono distribuiti entro qualche ora dal momento della creazione, ma possono essere distribuiti come maggiore frequenza.

La completezza e la tempestività della registrazione del server non è tuttavia garantita. È possibile che il record del log per una richiesta specifica venga consegnato molto tempo dopo l'elaborazione effettiva della richiesta o non venga consegnato affatto. Potresti persino notare la duplicazione di un record di log. Lo scopo dei log del server è fornire un'idea della natura del traffico nel bucket. Sebbene sia raro perdere i record di log o vedere la duplicazione di un record di log, tieni presente che la registrazione di log del server non intende essere un resoconto completo di tutte le richieste.

Data la natura basata sul miglior tentativo possibile della registrazione di log del server, i report di utilizzo potrebbero includere una o più richieste di accesso che non appaiono in un log del server consegnato. Puoi trovare questi report di utilizzo in Report costi e utilizzo nella console Gestione costi e fatturazione AWS .

Tempo richiesto per l'applicazione delle modifiche dello stato di registrazione del bucket

L'applicazione effettiva delle modifiche dello stato di registrazione di un bucket sulla distribuzione dei file di log richiede tempo. Ad esempio, se abiliti la registrazione per un bucket, è possibile che

nell'ora successiva alcune richieste vengano registrate nel log e altre no. Supponiamo di modificare il bucket di destinazione per la registrazione dal bucket A al bucket B. Nell'ora successiva, alcuni log potrebbero continuare a essere consegnati al bucket A, mentre altri potrebbero essere consegnati al nuovo bucket di destinazione B. Analogamente, se si modifica il gruppo di log Logs utilizzato per la consegna, alcuni CloudWatch log potrebbero continuare a essere consegnati al gruppo di log precedente durante la transizione. In tutti i casi, le nuove impostazioni diventano effettive automaticamente.

Prezzi

Il costo della registrazione degli accessi al server dipende dall'opzione di consegna utilizzata.

- Amazon CloudWatch Logs: l'acquisizione viene pagata in base alle tariffe CloudWatch vendute, con prezzi a più livelli basati sul volume. CloudWatch Logs comprime i log prima dell'archiviazione, quindi il volume archiviato è significativamente inferiore al volume ingerito. Se abiliti il mirror di S3 Tables, non sono previsti costi aggiuntivi per l'archiviazione o la manutenzione del tavolo. Paghi solo per le richieste di query ai prezzi di S3 Tables. Per le tariffe correnti, consulta i [CloudWatch prezzi](#).
- Bucket per uso generico Amazon S3: la consegna dei log è gratuita. Paghi solo per l'archiviazione dei file di registro alle tariffe di archiviazione standard di Amazon S3. Il costo di trasferimento dei dati per la consegna dei file di log non viene valutato, ma viene addebitata la normale tariffa di trasferimento dei dati per l'accesso ai file di log. Per le tariffe attuali, consulta i prezzi di [Amazon S3](#).

Per ulteriori informazioni sulla fornitura e l'utilizzo dei log di accesso al server, consulta le seguenti sezioni.

Invio dei log ad Amazon CloudWatch Logs

Quando fornisci i log di accesso al server ad Amazon CloudWatch Logs, ottieni log JSON strutturati che puoi interrogare in modo interattivo con CloudWatch Logs Insights, aggregarli tra account e regioni e, facoltativamente, rispecchiare su tabelle S3 in formato Apache Iceberg per l'analisi SQL. Puoi anche inviare i log ad Amazon S3 in formato JSON o Apache Parquet o indirizzarli tramite Amazon Data Firehose.

Argomenti

- [Invio dei log di accesso al server a Logs CloudWatch](#)

- [Formato del registro in CloudWatch Logs](#)
- [Gestione della conservazione dei log](#)
- [Interrogazione dei CloudWatch log con Logs Insights](#)
- [Interrogazione dei log di accesso nelle tabelle S3](#)
- [Risoluzione dei problemi relativi alla consegna dei log CloudWatch](#)

Invio dei log di accesso al server a Logs CloudWatch

Puoi fornire i log di accesso al server Amazon S3 a un gruppo di log Logs utilizzando Amazon CloudWatch Logs venduto log delivery. CloudWatch Una volta che i log sono in CloudWatch Logs, puoi interrogarli con CloudWatch Logs Insights, aggregarli tra account e regioni, crittografarli con AWS Key Management Service (AWS KMS) e, facoltativamente, inviarli alle tabelle Amazon S3 in formato Apache Iceberg per l'analisi SQL. Puoi anche inviare i log ad Amazon S3 in formato JSON o Apache Parquet o indirizzarli tramite Amazon Data Firehose.

La distribuzione viene configurata utilizzando le API CloudWatch Logs, non le API di Amazon S3. Specifici un gruppo di log per ogni bucket di origine. Più bucket possono condividere lo stesso gruppo di log oppure ogni bucket può consegnare il proprio.

Tip

Puoi configurare più destinazioni per lo stesso bucket. Ad esempio, esegui la consegna a un gruppo di CloudWatch log Logs per eseguire query interattive e contemporaneamente distribuisce ad Amazon S3 in formato Parquet per la conservazione a lungo termine a costi inferiori.

Note

CloudWatch Logs venduto log delivery supporta anche Amazon Data Firehose e Amazon S3 come destinazioni di consegna, incluso il formato di output Apache Parquet. Questa pagina descrive la destinazione del gruppo di CloudWatch log Logs, che supporta anche l'integrazione di S3 Tables per l'analisi SQL. Per informazioni sulle destinazioni Firehose e Amazon S3, consulta [Enable logging from AWS services](#) nella Amazon CloudWatch Logs User Guide.

 Note

Per informazioni sulla distribuzione dei log di accesso al server a un bucket generico Amazon S3, consulta invece. [Abilitazione della registrazione degli accessi al server Amazon S3](#)

Prerequisiti

Prima di configurare la consegna, è necessario quanto segue:

- Un bucket Amazon S3 per uso generico (il bucket di origine che desideri registrare).
- Un gruppo di CloudWatch log Logs nello stesso del bucket Regione AWS di origine.
- Autorizzazioni IAM per il chiamante. Come minimo, sono necessarie le seguenti autorizzazioni:
 - `logs:PutDeliverySource`
 - `logs:PutDeliveryDestination`
 - `logs:CreateDelivery`
 - `s3:AllowVendedLogDeliveryForResource`(nel bucket di origine)

Se intendi abilitare l'integrazione con S3 Tables, avrai bisogno anche di:

- `observabilityadmin:CreateS3TableIntegration`
- `logs:AssociateSourceToS3TableIntegration`
- `s3tables:CreateTableBucket`
- `s3tables:PutTableBucketEncryption`
- `s3tables:PutTableBucketPolicy`

Impostazione della consegna (AWS CLI)

Per configurare l'invio dei log di accesso al server a CloudWatch Logs utilizzando il AWS Command Line Interface, completare i tre passaggi seguenti.

1. Crea una fonte di consegna. Questo registra il tuo bucket Amazon S3 come fonte di log con Logs. CloudWatch

```
aws logs put-delivery-source \  
  --name my-sal-source \  
  --resource-arn arn:aws:s3:::my-bucket \  
  --destination-arn arn:aws:logs:region:account-id:log-group:log-group-name
```



```
--log-type S3_SERVER_ACCESS_LOGS
```

2. Crea una destinazione di consegna. Specifica il gruppo di CloudWatch log Logs in cui verranno consegnati i log.

```
aws logs put-delivery-destination \  
  --name my-sal-destination \  
  --delivery-destination-configuration '{"destinationResourceArn":  
  "arn:aws:logs:us-east-1:123456789012:log-group:my-sal-logs"}'
```

3. Crea una consegna. Questo collega l'origine alla destinazione e avvia la consegna del registro.

```
aws logs create-delivery \  
  --delivery-source-name my-sal-source \  
  --delivery-destination-arn arn:aws:logs:us-east-1:123456789012:delivery-  
  destination:my-sal-destination
```

Dopo aver completato questi passaggi, Amazon S3 inizia a fornire i log di accesso al server al tuo gruppo di CloudWatch log Logs. La propagazione della configurazione richiede 15-20 minuti. Dopo la propagazione, la consegna dei log inizia in genere entro poche ore. Vengono registrate solo le nuove richieste: non è previsto il backfill dei dati storici.

Configurazione della consegna (console Amazon S3)

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Scegli il nome del bucket di origine per il quale desideri abilitare la registrazione.
4. Scegliere la scheda Properties (Proprietà).
5. Nella sezione Invio dei log di accesso al server ai CloudWatch log, scegli Modifica.
6. Scegli Abilita .
7. Seleziona o crea un gruppo di CloudWatch log Logs come destinazione di consegna.
8. (Facoltativo) Per inviare i log a S3 Tables in formato Apache Iceberg, seleziona Abilita l'integrazione con S3 Tables.
9. Scegli Save changes (Salva modifiche).

Dopo il salvataggio, la sezione Consegna dei log di accesso al server ai log mostra il gruppo di CloudWatch log abilitato.

Impostazione della consegna (CloudFormation)

È possibile utilizzarlo AWS CloudFormation per automatizzare la configurazione della consegna dei log di accesso al server ai CloudWatch log. Il modello seguente crea le risorse richieste: un ruolo IAM, un gruppo di CloudWatch log Logs, una fonte di consegna, una destinazione di consegna e una consegna.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: S3 Access Logs delivery to CloudWatch Logs

Parameters:
  SourceBucketArn:
    Type: String
    Description: ARN of the S3 bucket to enable access logging
  LogGroupName:
    Type: String
    Default: /aws/s3/access-logs
    Description: CloudWatch Log Group name for SAL delivery

Resources:
  SALLogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Ref LogGroupName
      RetentionInDays: 180

  SALDeliverySource:
    Type: AWS::Logs::DeliverySource
    Properties:
      Name: !Sub '${AWS::StackName}-sal-source'
      ResourceArn: !Ref SourceBucketArn
      LogType: S3_SERVER_ACCESS_LOGS

  SALDeliveryDestination:
    Type: AWS::Logs::DeliveryDestination
    Properties:
      Name: !Sub '${AWS::StackName}-sal-destination'
      DestinationResourceArn: !GetAtt SALLogGroup.Arn

  SALDelivery:
    Type: AWS::Logs::Delivery
    Properties:
      DeliverySourceName: !Ref SALDeliverySource
```

```
DeliveryDestinationArn: !GetAtt SALDeliveryDestination.Arn
```

Abilitazione dell'integrazione con S3 Tables (opzionale)

Quando abiliti l'integrazione con S3 Tables, CloudWatch Logs invia automaticamente i log di accesso al server in formato Apache Iceberg al bucket di tabelle `aws-cloudwatch` gestito nel tuo account. Puoi quindi interrogare questi dati utilizzando Amazon Athena, Amazon Redshift o qualsiasi strumento. Iceberg-compatible

Non sono previsti costi aggiuntivi per l'archiviazione o la manutenzione delle tabelle nell'integrazione di S3 Tables. Paghi solo per l'inserimento CloudWatch dei log e per le richieste di query ai prezzi di S3 Tables.

1. Crea l'integrazione di S3 Tables (una volta per account per regione).

```
aws observabilityadmin create-s3-table-integration \  
  --role-arn arn:aws:iam::123456789012:role/CWLogsS3TableIntegrationRole \  
  --encryption '{"SseAlgorithm": "AES256"}'
```

Il ruolo IAM deve fidarsi del responsabile del `logs.amazonaws.com` servizio e concedere l'`logs:integrateWithS3Table` autorizzazione. Di seguito è illustrato un esempio di policy di attendibilità:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "logs.amazonaws.com"  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {  
        "StringEquals": {  
          "aws:SourceAccount": "123456789012"  
        },  
        "ArnLike": {  
          "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:log-group:log-  
group-name"  
        }  
      }  
    }  
  ]  
}
```

```
}
]
}
```

Il ruolo richiede anche la seguente politica di autorizzazione:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "logs:integrateWithS3Table",
      "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:log-group-name",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

2. Associa la fonte di consegna all'integrazione.

```
aws logs associate-source-to-s3-table-integration \
  --integration-arn integration-arn \
  --data-source '{"name":"amazon_s3","type":"server_access"}
```

Dopo questi passaggi, CloudWatch Logs crea il bucket di tabelle `aws-cloudwatch` gestite e inizia a fornire i log in formato Iceberg. I dati vengono in genere visualizzati entro un'ora dalla prima consegna a CloudWatch Logs.

Per informazioni sull'interrogazione dell'integrazione con S3 Tables, consulta [Interrogazione dei log di accesso nelle tabelle S3](#)

Cross-account e aggregazione interregionale

Il percorso di consegna CloudWatch dei log supporta l'aggregazione dei log tra account e tra regioni con due opzioni:

- CloudWatch L'osservabilità tra più account consente di interrogare i log esistenti tra gli account senza copiare i dati.
- CloudWatch La centralizzazione dei log consente di consolidare i log di più account e regioni in un gruppo di log centrale, utilizzando opzionalmente filtri di abbonamento per l'inoltro selettivo.

Per le configurazioni con più account, gli amministratori possono utilizzare le regole di abilitazione di CloudWatch Telemetry Config per abilitare automaticamente la distribuzione dei log di accesso al server tra gli account membri. AWS Organizations

Note

Le regole di abilitazione attualmente non supportano l'abilitazione automatica dell'integrazione con S3 Tables. È necessario abilitare l'integrazione separatamente in ciascun account.

Encryption (Crittografia)

È possibile crittografare i log di accesso al server inviati a CloudWatch Logs configurando AWS KMS la crittografia nel gruppo di log. Quando i log di accesso al server vengono inviati a quel gruppo di log, vengono crittografati con la tua AWS KMS chiave. Ciò risolve una limitazione fondamentale del percorso di distribuzione dei bucket generici di Amazon S3, che supporta solo SSE-S3 la crittografia.

Se abiliti l'integrazione di S3 Tables con un gruppo AWS KMS di log crittografato, devi concedere autorizzazioni aggiuntive nella tua policy AWS KMS chiave ai seguenti service principal:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnableCWSystemTablesKeyUsage",
      "Effect": "Allow",
      "Principal": {
        "Service": "systemtables.cloudwatch.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
    }
  ],
}
```

```

    "Resource": "arn:aws:kms:us-east-1:123456789012:key/key-id",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    },
  },
  {
    "Sid": "EnableS3TablesMaintenanceKeyUsage",
    "Effect": "Allow",
    "Principal": {
      "Service": "maintenance.s3tables.amazonaws.com"
    },
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:us-east-1:123456789012:key/key-id",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "table-bucket-arn/*"
      }
    }
  }
]
}

```

Il `systemtables.cloudwatch.amazonaws.com` principale viene utilizzato da CloudWatch Logs per scrivere i log su S3 Tables. Il `maintenance.s3tables.amazonaws.com` principale viene utilizzato da S3 Tables per operazioni Iceberg come la compattazione.

Disattivazione della consegna

Per interrompere l'invio dei log di accesso al server a CloudWatch Logs, puoi eliminare la consegna o la fonte di consegna:

- **Elimina la consegna:** interrompe la consegna dei log ma mantiene intatta la configurazione dell'origine di consegna. Puoi creare una nuova consegna in un secondo momento senza riconfigurare l'origine.

```

aws logs delete-delivery \
  --id delivery-id

```

- Elimina l'origine di consegna: rimuove completamente la configurazione di origine. Usalo se non desideri più che il bucket sia associato alla consegna di CloudWatch Logs.

```
aws logs delete-delivery-source \  
  --name delivery-source-name
```

I log forniti in precedenza rimangono nel gruppo di log e nell'integrazione di S3 Tables (se abilitata). L'eliminazione della consegna non rimuove i dati di registro esistenti.

Formato del registro in CloudWatch Logs

Quando i log di accesso al server Amazon S3 vengono inviati ad Amazon CloudWatch Logs, ogni record di log è un oggetto JSON strutturato. È diverso dal formato di testo delimitato da spazi utilizzato per la consegna a un bucket generico Amazon S3. Il formato strutturato rende i campi direttamente interrogabili in Logs Insights senza l'analisi delle espressioni regolari. CloudWatch

Note

Per il formato di testo delimitato da spazi utilizzato per la distribuzione generica in bucket, consulta. [Formato del log di accesso al server Amazon S3](#)

Campi del record di log

La tabella seguente descrive i campi di ogni record del registro di accesso al server inviato a Logs. CloudWatch

Campi del log di accesso al server in CloudWatch Logs

Campo	Tipo	Description
schema_version_id	stringa	Identificatore di versione per lo schema dei record di log (ad esempio, V_1_0). Utilizza questo campo per rilevare le modifiche allo schema quando vengono aggiunti nuovi campi nelle versioni future.
bucket_arn	stringa	ARN del bucket di origine.

Campo	Tipo	Description
bucket_name	stringa	Nome del bucket a cui è stata effettuata la richiesta. Derivato dal bucket ARN.
request_time	stringa	Ora di ricezione della richiesta, in UTC. Formattato come ISO 8601 (). yyyy-MM-dd 'T' HH:mm:ss.SSS 'Z' Nell'integrazione di S3 Tables (Iceberg), questo campo è memorizzato come. timestamp tz
bucket_owner_id	stringa	ID utente canonico del proprietario del bucket di origine.
remote_ip	stringa	Indirizzo IP apparente del richiedente. L'impostazione predefinita è null se non disponibile.
requester	stringa	ID utente canonico del richiedente o per richieste non autenticate. null Per gli utenti e i ruoli IAM, questo è l'ARN.
request_id	stringa	Identificatore univoco generato da Amazon S3 per ogni richiesta. Il valore predefinito è se non disponibile. null
operation	stringa	L'operazione che è stata eseguita, ad esempio REST.GET.OBJECT o REST.PUT.OBJECT Il valore predefinito è null se non disponibile.
key_name	stringa	Chiave oggetto nella richiesta o null se l'operazione non coinvolge un oggetto.
request_uri	stringa	La Request-URI parte del messaggio di richiesta HTTP, o null se non disponibile.
http_status	int	Codice di stato HTTP numerico della risposta, ad esempio 200 o 403. Il valore predefinito è null se non disponibile.

Campo	Tipo	Description
<code>error_code</code>	stringa	Codice di errore Amazon S3, ad esempio <code>NoSuchKey</code> o <code>AccessDenied</code> , o <code>null</code> se non si è verificato alcun errore.
<code>bytes_sent_size</code>	Long	Numero di byte di risposta inviati, escluso il sovraccarico del protocollo HTTP. Il valore predefinito è se non disponibile. <code>null</code>
<code>object_size</code>	Long	Dimensione totale dell'oggetto. Il valore predefinito è <code>null</code> se non disponibile.
<code>total_duration</code>	Long	Tempo totale della richiesta dal momento in cui è stata ricevuta all'ultimo byte della risposta inviata, in millisecondi. Il valore predefinito è se non disponibile. <code>null</code>
<code>turn_around_duration</code>	Long	Tempo impiegato da Amazon S3 per l'elaborazione della richiesta, in millisecondi. Questo valore viene misurato dal momento in cui è stato ricevuto l'ultimo byte della richiesta fino al momento in cui è stato inviato il primo byte della risposta. Il valore predefinito è se non disponibile. <code>null</code>
<code>referer</code>	stringa	Valore dell' <code>Referer</code> intestazione HTTP, <code>null</code> se non presente.
<code>user_agent</code>	stringa	Valore dell' <code>User-Agent</code> intestazione HTTP. Il valore predefinito è <code>null</code> se non disponibile.
<code>version_id</code>	stringa	ID di versione nella richiesta o <code>null</code> se l'operazione non coinvolge un oggetto con versione.
<code>host_id</code>	stringa	ID di richiesta esteso Amazon S3 (<code>x-amz-id-2</code>). L'impostazione predefinita è <code>null</code> se non disponibile.

Campo	Tipo	Description
<code>signature_version</code>	stringa	Versione della firma utilizzata per autenticare la richiesta: o. SigV2 SigV4 L'impostazione predefinita è per le richieste non null autenticate.
<code>cipher_suite</code>	stringa	Suite di crittografia TLS negoziata per le richieste HTTPS o per HTTP. null
<code>authentication_type</code>	stringa	Tipo di autenticazione della richiesta:AuthHeader,, o. QueryString null
<code>host_header</code>	stringa	Endpoint utilizzato per connettersi ad Amazon S3. L'impostazione predefinita è se non disponibile. null
<code>tls_version</code>	stringa	Versione TLS negoziata dal cliente:TLSv1.1,, TLSv1.2 o. TLSv1.3 null
<code>access_point_arn</code>	stringa	ARN del punto di accesso utilizzato per la richiesta o null se la richiesta non ha utilizzato un punto di accesso.
<code>acl_required</code>	booleano	Se era richiesto un ACL per la richiesta. Il valore predefinito è null quando non applicabile.
<code>source_region</code>	stringa	Regione AWS da cui ha avuto origine la richiesta o null quando non è possibile determinare la Regione di origine. Gli esempi includono PrivateLink connessioni, connessioni Direct Connect, Bring your own IP address (BYOIP), indirizzi non AWS IP e registri generati da azioni basate su policy come il ciclo di vita e il checksum.

Esempio di record di registro

Di seguito è riportato un esempio di record del registro degli accessi al server visualizzato in CloudWatch Logs.

```
{
  "schema_version_id": "V_1_0",
  "bucket_arn": "arn:aws:s3::my-data-bucket",
  "bucket_name": "my-data-bucket",
  "request_time": "2026-04-29T14:32:16.000Z",
  "bucket_owner_id":
"79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be",
  "remote_ip": "203.0.113.45",
  "requester": "arn:aws:iam::123456789012:role/DataAnalystRole",
  "request_id": "3E57427F33A59F07",
  "operation": "REST.GET.OBJECT",
  "key_name": "reports/2026/quarterly-summary.parquet",
  "request_uri": "GET /my-data-bucket/reports/2026/quarterly-summary.parquet HTTP/1.1",
  "http_status": 200,
  "error_code": null,
  "bytes_sent_size": 1048576,
  "object_size": 1048576,
  "total_duration": 45,
  "turn_around_duration": 12,
  "referer": null,
  "user_agent": "aws-sdk-java/2.20.0",
  "version_id": null,
  "host_id": "s9lzHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=",
  "signature_version": "SigV4",
  "cipher_suite": "TLS_AES_128_GCM_SHA256",
  "authentication_type": "AuthHeader",
  "host_header": "my-data-bucket.s3.us-east-1.amazonaws.com",
  "tls_version": "TLSv1.3",
  "access_point_arn": null,
  "acl_required": false,
  "source_region": "us-east-1"
}
```

Differenze rispetto al formato di registro bucket per uso generico

Il formato di registro dei CloudWatch log dei log è diverso dal formato di registro bucket per uso generico nei seguenti modi:

- **Formato:** CloudWatch i log sono oggetti JSON strutturati. I bucket log generici sono testo delimitato da spazi.

- **Nomi dei campi:** il formato CloudWatch Logs utilizza nomi di campo descrittivi separati da trattini bassi (ad esempio,,). `bytes_sent_size` `total_duration` `key_name` `authentication_type` Il formato bucket per uso generico è un testo posizionale delimitato da spazi senza colonne denominate.
- **Campi aggiuntivi:** il formato CloudWatch Logs include `schema_version_id` `ebucket_arn`, che non sono presenti nel formato di testo bucket per uso generico.
- **Nessuna analisi richiesta:** poiché CloudWatch i log di Logs sono JSON strutturati, puoi interrogare i singoli campi direttamente in CloudWatch Logs Insights senza l'analisi delle espressioni regolari. Il formato di testo bucket per uso generico richiede un'espressione regolare o un parser personalizzato per estrarre i campi.

Gestione della conservazione dei log

Quando si forniscono i log di accesso al server a CloudWatch Logs, la conservazione dei log è controllata dall'impostazione di conservazione sul gruppo di log. La conservazione viene impostata quando si crea il gruppo di log o lo si aggiorna in qualsiasi momento utilizzando la console CloudWatch Logs o l'API. AWS CLI

Le opzioni di conservazione vanno da 1 giorno a 10 anni, oppure puoi scegliere di non far scadere mai i log. Quando i dati di registro raggiungono la fine del periodo di conservazione, vengono automaticamente eliminati dal gruppo di log.

Se hai abilitato il mirror di S3 Tables per il tuo gruppo di log, i dati rispecchiati nella tabella S3 seguono la stessa conservazione. Quando i dati di log scadono dal gruppo di log, i record corrispondenti vengono rimossi dalla tabella S3. Non è necessario gestire la conservazione separatamente per la tabella S3.

Per impostare o aggiornare la conservazione dei gruppi di log

1. Apri la console CloudWatch Logs [CloudWatch nella console Logs](#).
2. Seleziona il gruppo di log che riceve i log di accesso al server.
3. Scegli Azioni, quindi Modifica le impostazioni di conservazione.
4. Seleziona un periodo di conservazione e scegli Salva.

Per impostare la conservazione utilizzando AWS CLI:

```
aws logs put-retention-policy \
```

```
--log-group-name "/aws/vendedlogs/s3/DOC-EXAMPLE-BUCKET/S3_SERVER_ACCESS_LOGS" \  
--retention-in-days 90
```

Per ulteriori informazioni, vedere [Modificare la conservazione dei dati di registro in CloudWatch Logs](#) nella CloudWatch Logs User Guide.

Interrogazione dei CloudWatch log con Logs Insights

CloudWatch Logs Insights ti consente di cercare e analizzare in modo interattivo i dati dei log di accesso al server. Le query vengono eseguite sul gruppo di log in cui vengono inviati i log e restituiscono risultati in pochi secondi.

Note

Per interrogare i log consegnati a un bucket Amazon S3 per uso generico, consulta. [Esecuzione di query sui log degli accessi per le richieste tramite Amazon Athena](#) Per interrogare il mirror di S3 Tables con SQL, consulta. [Interrogazione dei log di accesso nelle tabelle S3](#)

Nozioni di base

1. Apri la CloudWatch console all'indirizzo. <https://console.aws.amazon.com/cloudwatch/>
2. Nel pannello di navigazione, scegli Logs, quindi Logs Insights.
3. Seleziona il tuo gruppo di log di accesso al server dal selettore del gruppo di log.
4. Scegli un intervallo di tempo per la tua richiesta.
5. Inserisci una query e scegli Esegui query.

Analisi del traffico

Le seguenti domande ti aiutano a comprendere il volume delle richieste e i modelli di traffico.

Example Volume delle richieste nel tempo

```
stats count(*) as requests by bin(5m) as interval  
| sort interval asc
```

Example Richiedi una combinazione per tipo di operazione

```
stats count(*) as cnt by operation
| sort cnt desc
```

Example Traffico per secchio

```
stats count(*) as requests, sum(bytes_sent_size) as bytes_out by bucket_arn
| sort requests desc
```

Risoluzione dei problemi

Le seguenti domande consentono di identificare e diagnosticare gli errori.

Example Ripartizione del tasso di errore

```
filter http_status >= 400
| stats count(*) as error_count by http_status, error_code, operation
| sort error_count desc
```

Example 403 Richieste di accesso negato

```
filter http_status = 403
| stats count(*) as denied_count by key_name, remote_ip, requester
| sort denied_count desc
```

Example 404 Richieste non trovate

```
filter http_status = 404
| stats count(*) as miss_count by key_name, error_code, remote_ip
| sort miss_count desc
```

Example 503 eventi SlowDown (throttling)

```
filter http_status = 503
| stats count(*) as throttle_count by key_name, remote_ip
| sort throttle_count desc
```

Modelli di accesso

Le seguenti domande ti aiutano a capire chi accede ai tuoi dati e in che modo.

Example Traffico per IP di origine

```
stats count(*) as total_requests,  
      sum(http_status >= 400) as errors,  
      sum(bytes_sent_size) as bytes_transferred  
  by remote_ip  
| sort total_requests desc
```

Example Operazioni per richiedente

```
stats count(*) as requests by requester, operation  
| sort requests desc
```

Example Chiavi più utilizzate

```
filter operation like /REST\.(GET|PUT)\.OBJECT/  
| stats count(*) as access_count, sum(bytes_sent_size) as bytes_out by key_name  
| sort access_count desc  
| limit 10
```

Analisi della latenza

Le seguenti domande consentono di identificare le richieste lente e le tendenze della latenza.

Example Latenza per tipo di operazione

```
filter operation like /REST\.(GET|PUT)\.OBJECT/  
| stats avg(total_duration) as avg_ms,  
      pct(total_duration, 50) as p50_ms,  
      pct(total_duration, 95) as p95_ms,  
      max(total_duration) as max_ms,  
      count(*) as requests  
  by operation
```

Example Tasti più lenti per latenza p95

```
filter operation like /REST\.GET\.OBJECT/  
| stats avg(total_duration) as avg_ms,  
      pct(total_duration, 95) as p95_ms,  
      count(*) as requests  
  by key_name
```

```
| sort p95_ms desc
| limit 10
```

Example Latenza nel tempo

```
filter operation like /REST\.(GET|PUT)\.OBJECT/
| stats avg(total_duration) as avg_ms, pct(total_duration, 95) as p95_ms by bin(5m) as
  interval
| sort interval asc
```

Attribuzione dei costi

Le seguenti domande aiutano a comprendere il trasferimento dei dati e a identificare i fattori di costo.

Example Trasferimento dei dati per operazione

```
filter operation like /REST\.(GET|PUT|DELETE)\.OBJECT/
| stats sum(bytes_sent_size) as total_bytes_out,
  sum(object_size) as total_object_bytes,
  count(*) as request_count
  by operation
| sort total_bytes_out desc
```

Example Oggetti più grandi serviti

```
filter operation like /REST\.GET\.OBJECT/ and bytes_sent_size > 0
| stats max(object_size) as max_size, avg(object_size) as avg_size, count(*) as reads
  by key_name
| sort max_size desc
| limit 10
```

Analisi della sicurezza

Le seguenti domande consentono di rilevare modelli di accesso sospetti.

Example IP con tassi di errore elevati

```
stats count(*) as total,
  sum(http_status >= 400) as errors
  by remote_ip
| filter errors > 10
```



```
| sort errors desc
```

Example Tentativi di accesso falliti tramite chiave

```
filter http_status >= 400
| stats count(*) as attempts by remote_ip, key_name, operation, http_status
| sort attempts desc
| limit 20
```

Example Distribuzione della versione TLS

```
stats count(*) as cnt by tls_version
| sort cnt desc
```

Interrogazione dei log di accesso nelle tabelle S3

Quando abiliti l'integrazione con Amazon S3 Tables, Amazon CloudWatch Logs invia i log di accesso al server in formato Apache Iceberg al bucket di tabelle gestite. `aws-cloudwatch` Poiché i dati sono in formato Iceberg, puoi interrogarli con qualsiasi strumento che supporti Apache Iceberg, tra cui:

- Amazon Athena: esegui query SQL direttamente dalla console Athena utilizzando il catalogo S3 Tables.
- Amazon SageMaker Unified Studio: utilizza l'editor SQL integrato per interrogare i dati di log insieme ad altri carichi di lavoro di analisi.
- Amazon Redshift: interroga le tabelle Iceberg tramite Redshift Spectrum o integrazione diretta.
- Apache Spark su Amazon EMR: utilizza Spark SQL o l'API con il connettore Iceberg. DataFrame
- Open-source strumenti: qualsiasi strumento che supporti il catalogo REST di Apache Iceberg, come Trino, DuckDB o. Pylceberg

Note

Per interrogare i CloudWatch log in modo interattivo in Logs Insights (senza SQL), vedi. [Interrogazione dei CloudWatch log con Logs Insights](#)

Prerequisiti

Prima di poter interrogare i log di accesso in S3 Tables, devi completare quanto segue:

1. Abilita l'integrazione di S3 Tables. Consulta [Abilitazione dell'integrazione con S3 Tables \(opzionale\)](#).
2. Abilita l'integrazione di S3 Tables con i servizi di analisi. Nella console Amazon S3, vai a **Table buckets** e scegli **Abilita integrazione**. Questo crea il catalogo `s3tablescatalog` federato in Data Catalog e rende le tabelle visibili ai servizi di analisi. Per impostazione predefinita, l'accesso è controllato tramite le autorizzazioni IAM. Puoi opzionalmente utilizzarlo AWS Lake Formation per un controllo granulare degli accessi. Per ulteriori informazioni, consulta [Integrazione delle tabelle S3 con i servizi di analisi. AWS](#)
3. Attendi che i dati vengano compilati. I dati vengono in genere visualizzati entro un'ora dalla prima consegna a CloudWatch Logs.

Connessione ad Amazon Athena

1. Apri la console Athena all'indirizzo <https://console.aws.amazon.com/athena/>.
2. Nell'editor di query, seleziona il catalogo Amazon S3 Tables dal menu a discesa dell'origine dati.
3. Le tabelle di log vengono visualizzate nell'elenco del database sotto il `logs` namespace.

Il nome della tabella per i log di accesso al server è `amazon_s3__server_access`. Il riferimento completo alla tabella è:

```
"s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"
```

Analisi del traffico

Example Volume delle richieste nel tempo

```
SELECT date_trunc('minute', request_time) AS interval,
       COUNT(*) AS requests
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"
GROUP BY date_trunc('minute', request_time)
ORDER BY interval ASC;
```

Example Richiedi una combinazione per tipo di operazione

```
SELECT operation, COUNT(*) AS cnt
```

```
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
GROUP BY operation  
ORDER BY cnt DESC;
```

Example Traffico per secchio

```
SELECT bucket_arn, COUNT(*) AS requests, SUM(bytes_sent_size) AS bytes_out  
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
GROUP BY bucket_arn  
ORDER BY requests DESC;
```

Risoluzione dei problemi

Example Ripartizione del tasso di errore

```
SELECT http_status, error_code, operation, COUNT(*) AS error_count  
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE http_status >= 400  
GROUP BY http_status, error_code, operation  
ORDER BY error_count DESC;
```

Example 403 Richieste di accesso negato

```
SELECT key_name, remote_ip, requester, COUNT(*) AS denied_count  
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE http_status = 403  
GROUP BY key_name, remote_ip, requester  
ORDER BY denied_count DESC;
```

Example 404 Richieste non trovate

```
SELECT key_name, error_code, remote_ip, COUNT(*) AS miss_count  
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE http_status = 404  
GROUP BY key_name, error_code, remote_ip  
ORDER BY miss_count DESC;
```

Example 503 eventi SlowDown (throttling)

```
SELECT key_name, remote_ip, COUNT(*) AS throttle_count
```

```
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE http_status = 503  
GROUP BY key_name, remote_ip  
ORDER BY throttle_count DESC;
```

Modelli di accesso

Example Traffico per IP di origine

```
SELECT remote_ip,  
       COUNT(*) AS total_requests,  
       SUM(CASE WHEN http_status >= 400 THEN 1 ELSE 0 END) AS errors,  
       SUM(bytes_sent_size) AS bytes_transferred  
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
GROUP BY remote_ip  
ORDER BY total_requests DESC;
```

Example Operazioni per richiedente

```
SELECT requester, operation, COUNT(*) AS requests  
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
GROUP BY requester, operation  
ORDER BY requests DESC;
```

Example Chiavi più utilizzate

```
SELECT key_name, COUNT(*) AS access_count, SUM(bytes_sent_size) AS bytes_out  
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE operation IN ('REST.GET.OBJECT', 'REST.PUT.OBJECT')  
GROUP BY key_name  
ORDER BY access_count DESC  
LIMIT 10;
```

Analisi della latenza

Example Latenza per tipo di operazione

```
SELECT operation,  
       AVG(total_duration) AS avg_ms,  
       APPROX_PERCENTILE(total_duration, 0.5) AS p50_ms,
```

```
APPROX_PERCENTILE(total_duration, 0.95) AS p95_ms,  
MAX(total_duration) AS max_ms,  
COUNT(*) AS requests  
FROM "s3tablesatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE operation IN ('REST.GET.OBJECT', 'REST.PUT.OBJECT')  
GROUP BY operation;
```

Example Tasti più lenti per latenza p95

```
SELECT key_name,  
AVG(total_duration) AS avg_ms,  
APPROX_PERCENTILE(total_duration, 0.95) AS p95_ms,  
COUNT(*) AS requests  
FROM "s3tablesatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE operation = 'REST.GET.OBJECT'  
GROUP BY key_name  
ORDER BY p95_ms DESC  
LIMIT 10;
```

Example Latenza nel tempo

```
SELECT date_trunc('minute', request_time) AS interval,  
AVG(total_duration) AS avg_ms,  
APPROX_PERCENTILE(total_duration, 0.95) AS p95_ms  
FROM "s3tablesatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE operation IN ('REST.GET.OBJECT', 'REST.PUT.OBJECT')  
GROUP BY date_trunc('minute', request_time)  
ORDER BY interval ASC;
```

Attribuzione dei costi

Example Trasferimento dei dati per operazione

```
SELECT operation,  
SUM(bytes_sent_size) AS total_bytes_out,  
SUM(object_size) AS total_object_bytes,  
COUNT(*) AS request_count  
FROM "s3tablesatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"  
WHERE operation IN ('REST.GET.OBJECT', 'REST.PUT.OBJECT', 'REST.DELETE.OBJECT')  
GROUP BY operation  
ORDER BY total_bytes_out DESC;
```

Example Oggetti più grandi serviti

```
SELECT key_name, MAX(object_size) AS max_size, AVG(object_size) AS avg_size, COUNT(*)
  AS reads
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"
WHERE operation = 'REST.GET.OBJECT' AND bytes_sent_size > 0
GROUP BY key_name
ORDER BY max_size DESC
LIMIT 10;
```

Analisi della sicurezza

Example IP con alti tassi di errore

```
SELECT remote_ip,
  COUNT(*) AS total,
  SUM(CASE WHEN http_status >= 400 THEN 1 ELSE 0 END) AS errors
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"
GROUP BY remote_ip
HAVING SUM(CASE WHEN http_status >= 400 THEN 1 ELSE 0 END) > 10
ORDER BY errors DESC;
```

Example Tentativi di accesso falliti tramite chiave

```
SELECT remote_ip, key_name, operation, http_status, COUNT(*) AS attempts
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"
WHERE http_status >= 400
GROUP BY remote_ip, key_name, operation, http_status
ORDER BY attempts DESC
LIMIT 20;
```

Example Distribuzione della versione TLS

```
SELECT tls_version, COUNT(*) AS cnt
FROM "s3tablescatalog/aws-cloudwatch"."logs"."amazon_s3__server_access"
GROUP BY tls_version
ORDER BY cnt DESC;
```

Utilizzo di agenti AI per interrogare i log di accesso al server Amazon S3

MCP-compatible Gli agenti di intelligenza artificiale possono scoprire le tabelle S3 che contengono i log di accesso al server Amazon S3, generare query SQL e analizzare i risultati. Poiché i log di

accesso al server Amazon S3 vengono esportati come tabelle Iceberg nel `aws-cloudwatch-tables` bucket, gli agenti possono interrogarli tramite lo stesso catalogo S3 Tables che usi con Amazon Athena, Amazon EMR, Amazon Redshift o qualsiasi altro strumento. Iceberg-compatible

L'[Agent Toolkit for AWS](#) fornisce competenze che forniscono agli agenti procedure convalidate per lavorare con i dati. AWS L'[abilità](#) Querying CloudWatch Logs system tables esegue query SQL sui dati di CloudWatch log esportati in tabelle S3, inclusi i log di accesso al server Amazon S3 nel bucket delle tabelle. `aws-cloudwatch` Per utilizzarla, scarica la skill dal repository GitHub e aggiungila alla directory delle competenze del tuo agente.

Ad esempio, puoi chiedere a un agente di mostrare i primi 10 indirizzi IP di origine in base al numero di richieste nei log di accesso al server S3 nelle ultime 24 ore. L'agente utilizza l'abilità per individuare la tabella del registro degli accessi ed eseguire la query in Athena.

Risoluzione dei problemi relativi alla consegna dei log CloudWatch

I log non compaiono nel gruppo di CloudWatch log Logs

Se hai configurato la consegna ma non vedi i log nel tuo gruppo di CloudWatch log Logs, controlla quanto segue:

- Verifica che la consegna sia attiva. Esegui `aws logs describe-deliveries` e conferma che lo stato della spedizione sia pari a `ACTIVE`.
- Verifica l'origine della spedizione. Esegui `aws logs describe-delivery-sources` e conferma che l'ARN del bucket di origine e il tipo di log (`S3_SERVER_ACCESS_LOGS`) siano corretti.
- Verifica che il bucket di origine abbia traffico. I log di accesso al server vengono generati solo quando vengono effettuate richieste al bucket di origine. Se il bucket non ha traffico, non viene prodotto alcun registro.
- Controlla la regione del gruppo di log. Il gruppo di log deve trovarsi nella Regione AWS stesso bucket di origine.
- Attendi il tempo necessario per la consegna iniziale. Dopo l'installazione, potrebbero essere necessari alcuni minuti prima che vengano visualizzati i primi registri.

L'integrazione con S3 Tables non viene compilata

Se i log vengono visualizzati in CloudWatch Logs ma l'integrazione con S3 Tables è vuota, controlla quanto segue:

- Verifica che l'integrazione esista. Nella CloudWatch console, vai su Impostazioni , Globale e conferma che è elencata un'integrazione con tabella S3.
- Verifica che la fonte sia associata. Esegui `aws logs list-sources-for-s3-table-integration --integration-arn integration-arn` e conferma che il nome e il tipo di origine della spedizione siano visualizzati nell'elenco.
- Controlla le autorizzazioni del ruolo del servizio. Il ruolo IAM utilizzato per l'integrazione deve avere l'ambito dell'`logs:integrateWithS3Table` autorizzazione per l'ARN del gruppo di log. Consulta [Abilitazione dell'integrazione con S3 Tables \(opzionale\)](#).
- Conferma che il bucket della **aws-cloudwatch** tabella esista. Nella console Amazon S3, vai a Table bucket e cerca il `aws-cloudwatch` bucket. Se non esiste, l'integrazione potrebbe non essere stata completata correttamente.
- Attendi il tempo necessario per la visualizzazione dei dati. L'integrazione potrebbe essere in ritardo rispetto alla consegna CloudWatch dei log. I dati vengono in genere visualizzati entro un'ora dalla prima consegna a CloudWatch Logs.
- Verifica che l'integrazione elabori solo i nuovi dati. L'integrazione con S3 Tables non riempie i log precedenti alla creazione dell'associazione. Solo gli eventi di registro aggiunti dopo l'associazione vengono recapitati a S3 Tables.

Errori di autorizzazione

Di seguito sono riportati gli errori di autorizzazione più comuni e come risolverli.

- Accesso negato attivato **PutDeliverySource**: il chiamante necessita dell'`s3:AllowVendedLogDeliveryForResource` autorizzazione `logs:PutDeliverySource` and.
- Accesso negato attivato **CreateDelivery**: il chiamante necessita dell'`logs:CreateDelivery` autorizzazione.
- Accesso negato attivato **CreateS3TableIntegration**: il chiamante necessita dell'`observabilityadmin:CreateS3TableIntegration` autorizzazione, più `s3tables:CreateTableBuckets` `s3tables:PutTableBucketEncryption`, e `s3tables:PutTableBucketPolicy`
- AWS KMS errori nel gruppo di log: se il gruppo di log utilizza AWS KMS la crittografia, verifica che la policy AWS KMS chiave conceda l'accesso al principale del servizio CloudWatch Logs. Consulta [Encryption \(Crittografia\)](#).

- AWS KMS errori nell'integrazione di S3 Tables: se il tuo gruppo di log utilizza la AWS KMS crittografia e l'integrazione con S3 Tables è abilitata, verifica che la policy AWS KMS chiave conceda l'accesso a entrambi `e.systemtables.cloudwatch.amazonaws.com` `maintenance.s3tables.amazonaws.com` Consulta [Encryption \(Crittografia\)](#).
- Accesso negato durante l'interrogazione in Athena: verifica che il responsabile IAM che esegue la query disponga delle autorizzazioni per accedere al bucket di `aws-cloudwatch` tabelle e al catalogo S3 Tables. Se stai utilizzando AWS Lake Formation, verifica che SELECT le sovvenzioni siano disponibili. DESCRIBE

La consegna è stata interrotta inaspettatamente

Se i log sono stati consegnati in precedenza ma sono stati interrotti, controlla quanto segue:

- Il bucket di origine è stato eliminato. Se il bucket di origine è stato eliminato, la consegna si interrompe. Se il bucket viene ricreato, devi creare nuovamente una nuova consegna.
- Gruppo di log eliminato. Se il gruppo di log è stato eliminato, la consegna si interrompe. Crea un nuovo gruppo di log e aggiorna la destinazione di consegna.
- Autorizzazioni IAM revoked. Se le autorizzazioni richieste per la consegna sono state rimosse, la consegna potrebbe interrompersi. Verifica che la configurazione di consegna disponga ancora delle autorizzazioni richieste.
- Quote di servizio. Controlla le quote del servizio CloudWatch Logs per i limiti di consegna per account. Potresti aver raggiunto il numero massimo di consegne.

Gestione dei costi di ingestione

Se i costi di inserimento dei CloudWatch log sono superiori al previsto, considera quanto segue:

- Riduci la conservazione. Imposta un periodo di conservazione più breve sul gruppo di log per ridurre i costi di archiviazione. CloudWatch I registri eliminano automaticamente i dati che superano il periodo di conservazione.
- Esamina il traffico del bucket di origine. High-traffic i bucket generano più log. Valuta se tutti i bucket di origine richiedono la consegna CloudWatch dei log o se il percorso di consegna dei bucket generici gratuito è sufficiente per alcuni bucket.
- Utilizza prezzi basati sul volume. CloudWatch I prezzi di importazione dei log venduti sono suddivisi in base al volume. I volumi più elevati ricevono tariffe per GB inferiori. Per le tariffe correnti, consulta [CloudWatch i prezzi](#).

Invio di log a un bucket Amazon S3 per uso generico

Quando invii i log di accesso al server a un bucket Amazon S3 per uso generico, i log vengono scritti in formato di testo delimitato da spazi. La consegna dei log è gratuita. Il bucket di destinazione deve trovarsi nello stesso bucket Regione AWS e Account AWS nel bucket di origine.

Argomenti

- [Abilitazione della registrazione degli accessi al server Amazon S3](#)
- [Formato del log di accesso al server Amazon S3](#)
- [Gestione della conservazione dei log](#)
- [Utilizzo dei log degli accessi al server Amazon S3 per identificare le richieste](#)
- [Risoluzione dei problemi di registrazione degli accessi al server](#)

Abilitazione della registrazione degli accessi al server Amazon S3

La registrazione degli accessi al server fornisce record dettagliati per le richieste che sono effettuate a un bucket Amazon S3. I log di accesso al server sono utili per numerose applicazioni. Ad esempio, le informazioni del log di accesso possono essere utili nei controlli di accesso e di sicurezza. Queste informazioni possono essere utili anche per comprendere la base clienti e la fattura Amazon S3.

Note

Questa pagina descrive la distribuzione dei log di accesso al server a un bucket Amazon S3 per uso generico. Puoi anche fornire log ad Amazon CloudWatch Logs per interrogazioni strutturate, aggregazione tra account e mirroring opzionale su tabelle S3. Per ulteriori informazioni, consulta [Invio dei log di accesso al server a Logs CloudWatch](#).

Per impostazione predefinita, Amazon S3 non raccoglie i log di accesso al server. Quando abiliti la registrazione di log, Amazon S3 fornisce i log degli accessi per un bucket di origine a un bucket di destinazione scelto (noto anche come bucket target). Il bucket di destinazione deve trovarsi nello stesso bucket Regione AWS e nel bucket Account AWS di origine.

Un record di log degli accessi contiene informazioni dettagliate sulle richieste effettuate a un bucket, tra cui il tipo di richiesta, le risorse specificate nella richiesta, nonché l'ora e la data di elaborazione della richiesta. Per ulteriori informazioni sui principi di base della registrazione, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

 Important

- L'abilitazione della registrazione degli accessi al server per un bucket Amazon S3 non prevede addebiti aggiuntivi. Tuttavia, i file di log distribuiti dal sistema accumulano i consueti addebiti per lo storage. È possibile eliminare i file di log in qualsiasi momento. Il costo di trasferimento dei dati per la consegna dei file di log non viene valutato, ma viene addebitata la normale tariffa di trasferimento dei dati per l'accesso ai file di log.
- Il bucket di destinazione non deve avere la registrazione di log degli accessi al server abilitata. I registri possono essere distribuiti a tutti i bucket di cui si è proprietari che si trovano nella stessa regione del bucket di origine, incluso il bucket di origine stesso. Tuttavia, la distribuzione dei log nel bucket di origine causa un ciclo infinito di log e non è consigliata. Tuttavia, per una gestione più semplice dei log, si consiglia di salvare i log di accesso in un bucket diverso.
- I bucket S3 con S3 Object Lock abilitato non possono essere utilizzati come bucket di destinazione per i log degli accessi al server. Il bucket di destinazione non deve avere una configurazione del periodo di conservazione predefinita.
- Il bucket di destinazione non deve avere l'opzione di pagamento a carico del cliente abilitata.

Puoi abilitare o disabilitare la registrazione degli accessi al server utilizzando la console Amazon S3, l'API Amazon S3, AWS Command Line Interface (AWS CLI) o gli SDK. AWS

Autorizzazioni per la distribuzione dei registri

Amazon S3 utilizza uno speciale account di recapito dei registri per scrivere i registri degli accessi nel server. Queste scritture sono soggette alle normali restrizioni del controllo accessi. Per la consegna di log degli accessi, è necessario concedere al principale (`logging.s3.amazonaws.com`) del servizio di registrazione di log l'accesso al bucket di destinazione.

Per concedere le autorizzazioni ad Amazon S3 per la consegna di log, è possibile utilizzare una policy del bucket o le liste di controllo degli accessi (ACL) del bucket, a seconda delle impostazioni di Proprietà dell'oggetto S3 del bucket di destinazione. Invece di una lista di controllo degli accessi (ACL) consigliamo di utilizzare una policy del bucket.

 Note

La concessione `s3:PutObject` al servizio di registrazione principale non è sufficiente se il bucket di destinazione utilizza la crittografia predefinita. SSE-KMS Il bucket di destinazione deve utilizzare le chiavi gestite di Amazon S3 (). SSE-S3 Se il bucket di destinazione utilizza SSE-KMS, Amazon S3 potrebbe fornire oggetti di log crittografati con una chiave a cui non puoi accedere.

Impostazione proprietario del bucket applicato per S3 Object Ownership

Se il bucket di destinazione utilizza l'impostazione proprietario del bucket applicato per Proprietà dell'oggetto, le ACL vengono disabilitate e non influiscono più sulle autorizzazioni. In questo caso, è necessario aggiornare la policy del bucket nel bucket di destinazione per concedere l'accesso al principale del servizio di registrazione di log. Non è possibile aggiornare l'ACL del bucket per concedere l'accesso al gruppo di consegna di log S3. Inoltre, non puoi includere concessioni di destinazione (note anche come concessioni target) nella configurazione [PutBucketLogging](#).

Per informazioni sulla migrazione delle ACL del bucket esistenti per la consegna dei log degli accessi a una policy del bucket, consulta [Concedere l'accesso al gruppo di consegna di log S3 per la registrazione di log degli accessi al server](#). Per ulteriori informazioni su Object Ownership, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#). Quando crei nuovi bucket, le ACL sono disabilitate per impostazione predefinita.

Concessione dell'accesso utilizzando una policy del bucket

Per concedere l'accesso utilizzando la policy del bucket nel bucket di destinazione, aggiorna la policy del bucket per concedere l'autorizzazione `s3:PutObject` al principale del servizio di registrazione di log. Se utilizzi la console di Amazon S3 per abilitare la registrazione di log degli accessi al server, la console aggiorna automaticamente la policy nel bucket di destinazione per concedere tali autorizzazioni al principale del servizio di registrazione di log. Se abiliti la registrazione di log degli accessi al server a livello di programmazione, puoi aggiornare manualmente la policy del bucket per il bucket di destinazione per concedere l'accesso al principale del servizio di registrazione di log.

Per un esempio di policy del bucket che concede l'accesso al principale del servizio di registrazione di log, consulta [the section called “Concedi le autorizzazioni al principale del servizio di registrazione di log utilizzando una policy del bucket”](#).

Concessione dell'accesso utilizzando le liste di controllo degli accessi (ACL) del bucket

Puoi utilizzare in alternativa le liste di controllo degli accessi (ACL) del bucket per concedere l'accesso per la consegna di log degli accessi. Aggiungi una voce apposita nell'ACL di bucket che conceda autorizzazioni WRITE e READ_ACP al gruppo di distribuzione di registri S3. Tuttavia, non è consigliabile concedere l'accesso al gruppo di distribuzione dei log S3 tramite le ACL bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#). Per informazioni sulla migrazione delle ACL del bucket esistenti per la consegna dei log degli accessi a una policy del bucket, consulta [Concedere l'accesso al gruppo di consegna di log S3 per la registrazione di log degli accessi al server](#). Per un esempio di ACL che concede l'accesso al principale del servizio di registrazione di log, consulta [the section called "Concedere autorizzazioni al gruppo di distribuzione dei log utilizzando l'ACL bucket"](#).

Concedi le autorizzazioni al principale del servizio di registrazione di log utilizzando una policy del bucket

Questo esempio di policy del bucket concede autorizzazioni `s3:PutObject` al principale del servizio di registrazione di log (`logging.s3.amazonaws.com`). Per utilizzare questa policy del bucket, sostituisci *user input placeholders* con le tue informazioni. Nella politica seguente, *amzn-s3-demo-destination-bucket* è il bucket di destinazione in cui verranno consegnati i log di accesso al server ed *amzn-s3-demo-source-bucket* è il bucket di origine. *EXAMPLE-LOGGING-PREFIX* è il prefisso di destinazione opzionale (noto anche come prefisso di destinazione) che desideri utilizzare per i tuoi oggetti di registro. *SOURCE-ACCOUNT-ID* è il proprietario del Account AWS bucket di origine.

Note

Se nella policy del bucket sono presenti istruzioni Deny, assicurati che non impediscano ad Amazon S3 di distribuire i log di accesso.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3ServerAccessLogsPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
```

```
    },
    "Action": [
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/EXAMPLE-LOGGING-PREFIX*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
        },
        "StringEquals": {
            "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
        }
    }
}
```

Concedere autorizzazioni al gruppo di distribuzione dei log utilizzando l'ACL bucket

 Note

Come best practice di sicurezza, Amazon S3 disabilita le liste di controllo degli accessi (ACL) per impostazione predefinita in tutti i nuovi bucket. Per ulteriori informazioni sulle autorizzazioni ACL nella console di Amazon S3, consulta [Configurazione delle ACL](#).

Sebbene questo approccio non sia consigliato, puoi concedere le autorizzazioni al gruppo di consegna di log utilizzando una ACL di bucket. Tuttavia, se il bucket di destinazione utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, non puoi impostare le ACL di bucket o di oggetti. Inoltre, non puoi includere concessioni di destinazione (note anche come concessioni target) nella configurazione [PutBucketLogging](#). Invece, utilizza una policy del bucket per concedere l'accesso al principale del servizio di registrazione (`logging.s3.amazonaws.com`). Per ulteriori informazioni, consulta [Autorizzazioni per la distribuzione dei registri](#).

Nelle liste di controllo degli accessi del bucket, il gruppo di consegna di log è rappresentato dall'URL seguente.

```
http://acs.amazonaws.com/groups/s3/LogDelivery
```

Per concedere le autorizzazioni WRITE e READ_ACP (lettura ACL), aggiungi le seguenti concessioni all'ACL di bucket di destinazione:

```
<Grant>
  <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
    <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
  </Grantee>
  <Permission>WRITE</Permission>
</Grant>
<Grant>
  <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
    <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
  </Grantee>
  <Permission>READ_ACP</Permission>
</Grant>
```

Per esempi sull'aggiunta a livello di programmazione di concessioni ACL, consulta la sezione [Configurazione delle ACL](#).

Important

Quando abiliti la registrazione degli accessi al server Amazon S3 utilizzando AWS CloudFormation un bucket e utilizzi gli ACL per concedere l'accesso al gruppo di distribuzione dei log S3, devi aggiungere anche "al tuo modello. AccessControl": "LogDeliveryWrite" CloudFormation Farlo è importante perché puoi concedere tali autorizzazioni solo creando un ACL per il bucket, ma non puoi creare ACL personalizzati per i bucket in. CloudFormation È possibile utilizzare solo ACL predefiniti con. CloudFormation

Come abilitare la registrazione degli accessi al server

Per abilitare la registrazione degli accessi al server utilizzando la console Amazon S3, l'API REST di Amazon S3, AWS gli SDK e AWS CLI utilizza le seguenti procedure.

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.

3. Nell'elenco dei bucket scegli il nome del bucket per il quale desideri abilitare la registrazione dei log degli accessi al server.
4. Scegliere Properties (Proprietà).
5. Nella sezione Server access logging (Registrazione degli accessi al server) scegliere Edit (Modifica).
6. In Registrazione degli accessi al server, seleziona Abilita.
7. In Bucket di destinazione, specifica un bucket e un prefisso opzionale. Se specifichi un prefisso, ti consigliamo di includere una barra in avanti (/) dopo il prefisso per facilitare la ricerca dei log.

 Note

L'indicazione di un prefisso con una barra (/) semplifica l'individuazione degli oggetti del log. Se, ad esempio, specifichi il valore di prefisso `logs/`, la chiave di ogni oggetto del log creato da Amazon S3 è preceduta dal prefisso `logs/`, come segue:

```
logs/2013-11-01-21-32-16-E568B2907131C0C0
```

Se specifichi il valore del prefisso `logs`, l'oggetto del log viene visualizzato come segue:

```
logs2013-11-01-21-32-16-E568B2907131C0C0
```

8. In Formato della chiave dell'oggetto di log, esegui una delle seguenti operazioni:
 - Per scegliere un partizionamento non basato sulla data, scegli `[DestinationPrefix] [YYYY] - [MM] - [DD] - [hh] - [mm] - [ss] - []`. UniqueString
 - Per scegliere il partizionamento basato sulla data, scegli `[DestinationPrefix] [SourceAccountId]/[SourceRegion]/[YYYYSourceBucket]/[MM]/[DD]/[YYYY] - [MM] - [MM] - [DD] - [hh] - [mm] - [ss] - [UniqueString]`, quindi scegli Ora evento S3 o Tempo di consegna del file di registro.
9. Scegli Save changes (Salva modifiche).

Quando abiliti la registrazione di log degli accessi al server in un bucket, la console abilita la registrazione nel bucket di origine e aggiorna la policy del bucket per il bucket di destinazione in modo da concedere autorizzazioni `s3:PutObject` al principale del servizio di registrazione di log (`logging.s3.amazonaws.com`). Per ulteriori informazioni su questa policy del bucket,

consulta [Concedi le autorizzazioni al principale del servizio di registrazione di log utilizzando una policy del bucket](#).

Puoi visualizzare i log nel bucket di destinazione. Dopo aver abilitato la registrazione degli accessi al server, potrebbero essere necessarie ore prima che i log vengano consegnati al bucket di destinazione.

Per ulteriori informazioni, consulta [Visualizzazione delle proprietà di un bucket per uso generico S3](#).

Utilizzo della REST API

Per abilitare i log, devi inviare una richiesta [PutBucketLogging](#) per aggiungere la configurazione della registrazione di log nel bucket di origine. La richiesta specifica il bucket di destinazione (noto anche come bucket target) e, facoltativamente, il prefisso da utilizzare con tutte le chiavi degli oggetti del log.

L'esempio seguente identifica *amzn-s3-demo-destination-bucket* come bucket di destinazione e *logs/* come prefisso.

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
  </LoggingEnabled>
</BucketLoggingStatus>
```

L'esempio seguente identifica *amzn-s3-demo-destination-bucket* come bucket di destinazione, *logs/* come prefisso e EventTime come il formato della chiave dell'oggetto di log.

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
    <TargetObjectKeyFormat>
      <PartitionedPrefix>
        <PartitionDateSource>EventTime</PartitionDateSource>
      </PartitionedPrefix>
    </TargetObjectKeyFormat>
  </LoggingEnabled>
</BucketLoggingStatus>
```

Gli oggetti del registri vengono scritti dall'account di distribuzione di log S3 e sono di proprietà di tale account. Al proprietario del bucket vengono concesse autorizzazioni complete sugli oggetti del log. Puoi usare in modo opzionale le concessioni di destinazione (note anche come concessioni target) per concedere le autorizzazioni ad altri utenti in modo che possano accedere ai log. Per ulteriori informazioni, consulta [PutBucketLogging](#).

Note

Se il bucket di destinazione utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, non puoi utilizzare le concessioni di destinazione per assegnare autorizzazioni ad altri utenti. Per concedere autorizzazioni ad altri utenti, puoi aggiornare la policy del bucket nel bucket di destinazione. Per ulteriori informazioni, consulta [Autorizzazioni per la distribuzione dei registri](#).

Per recuperare la configurazione di registrazione di log su un bucket, utilizza l'operazione API [GetBucketLogging](#).

Per eliminare la configurazione della registrazione di log, devi inviare una richiesta `PutBucketLogging` con un elemento `BucketLoggingStatus` vuoto:

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
</BucketLoggingStatus>
```

Per abilitare la registrazione su un bucket, puoi utilizzare l'API Amazon S3 o le librerie wrapper AWS SDK.

Utilizzo di AWS SDK

Gli esempi seguenti abilitano la registrazione di log in un bucket. Devi creare due bucket, uno di origine e uno di destinazione (target). Gli esempi aggiornano prima l'ACL del bucket sul bucket di destinazione. Quindi concedono al gruppo di consegna di log le autorizzazioni necessarie per scrivere i log sul bucket di destinazione e poi abilitano la registrazione di log sul bucket di origine.

Questi esempi non funzionano sui bucket di destinazione che utilizzano l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto.

Se il bucket di destinazione (target) utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, non sarà possibile impostare le ACL di bucket o di oggetti. Inoltre, non puoi includere le concessioni di destinazione (target) nella tua configurazione. [PutBucketLogging](#)

È necessario utilizzare una policy di bucket per concedere l'accesso al principale del servizio di registrazione (`logging.s3.amazonaws.com`). Per ulteriori informazioni, consulta [Autorizzazioni per la distribuzione dei registri](#).

.NET

SDK per .NET

Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
using System;
using System.IO;
using System.Threading.Tasks;
using Amazon.S3;
using Amazon.S3.Model;
using Microsoft.Extensions.Configuration;

/// <summary>
/// This example shows how to enable logging on an Amazon Simple Storage
/// Service (Amazon S3) bucket. You need to have two Amazon S3 buckets for
/// this example. The first is the bucket for which you wish to enable
/// logging, and the second is the location where you want to store the
/// logs.
/// </summary>
public class ServerAccessLogging
{
    private static IConfiguration _configuration = null!;

    public static async Task Main()
    {
        LoadConfig();

        string bucketName = _configuration["BucketName"];
        string logBucketName = _configuration["LogBucketName"];
        string logObjectKeyPrefix = _configuration["LogObjectKeyPrefix"];
        string accountId = _configuration["AccountId"];

        // If the AWS Region defined for your default user is different
```

```

        // from the Region where your Amazon S3 bucket is located,
        // pass the Region name to the Amazon S3 client object's constructor.
        // For example: RegionEndpoint.USWest2 or RegionEndpoint.USEast2.
        IAmazonS3 client = new AmazonS3Client();

        try
        {
            // Update bucket policy for target bucket to allow delivery of
logs to it.
            await SetBucketPolicyToAllowLogDelivery(
                client,
                bucketName,
                logBucketName,
                logObjectKeyPrefix,
                accountId);

            // Enable logging on the source bucket.
            await EnableLoggingAsync(
                client,
                bucketName,
                logBucketName,
                logObjectKeyPrefix);
        }
        catch (AmazonS3Exception e)
        {
            Console.WriteLine($"Error: {e.Message}");
        }
    }

    /// <summary>
    /// This method grants appropriate permissions for logging to the
    /// Amazon S3 bucket where the logs will be stored.
    /// </summary>
    /// <param name="client">The initialized Amazon S3 client which will be
used
    /// to apply the bucket policy.</param>
    /// <param name="sourceBucketName">The name of the source bucket.</param>
    /// <param name="logBucketName">The name of the bucket where logging
    /// information will be stored.</param>
    /// <param name="logPrefix">The logging prefix where the logs should be
delivered.</param>
    /// <param name="accountId">The account id of the account where the
source bucket exists.</param>
    /// <returns>Async task.</returns>

```

```

    public static async Task SetBucketPolicyToAllowLogDelivery(
        IAmazonS3 client,
        string sourceBucketName,
        string logBucketName,
        string logPrefix,
        string accountId)
    {
        var resourceArn = @"""arn:aws:s3:::" + logBucketName + "/" +
logPrefix + @"""";

        var newPolicy = @"{
            ""Statement"": [{
                ""Sid"": ""S3ServerAccessLogsPolicy"",
                ""Effect"": ""Allow"",
                ""Principal"": { ""Service"":
""logging.s3.amazonaws.com"" },
                ""Action"": [""s3:PutObject""],
                ""Resource"": ["" + resourceArn + @""],
                ""Condition"": {
                    ""ArnLike"": { ""aws:SourceArn"":
""arn:aws:s3:::" + sourceBucketName + @"""" },
                    ""StringEquals"": { ""aws:SourceAccount"": """" +
accountId + @"""" }
                }
            }]
        }";

        Console.WriteLine($"The policy to apply to bucket {logBucketName} to
enable logging:");
        Console.WriteLine(newPolicy);

        PutBucketPolicyRequest putRequest = new PutBucketPolicyRequest
        {
            BucketName = logBucketName,
            Policy = newPolicy,
        };
        await client.PutBucketPolicyAsync(putRequest);
        Console.WriteLine("Policy applied.");
    }

    /// <summary>
    /// This method enables logging for an Amazon S3 bucket. Logs will be
    stored
    /// in the bucket you selected for logging. Selected prefix
    /// will be prepended to each log object.

```

```

    /// </summary>
    /// <param name="client">The initialized Amazon S3 client which will be
used
    /// to configure and apply logging to the selected Amazon S3 bucket.</
param>
    /// <param name="bucketName">The name of the Amazon S3 bucket for which
you
    /// wish to enable logging.</param>
    /// <param name="logBucketName">The name of the Amazon S3 bucket where
logging
    /// information will be stored.</param>
    /// <param name="logObjectKeyPrefix">The prefix to prepend to each
    /// object key.</param>
    /// <returns>Async task.</returns>
    public static async Task EnableLoggingAsync(
        IAmazonS3 client,
        string bucketName,
        string logBucketName,
        string logObjectKeyPrefix)
    {
        Console.WriteLine($"Enabling logging for bucket {bucketName}.");
        var loggingConfig = new S3BucketLoggingConfig
        {
            TargetBucketName = logBucketName,
            TargetPrefix = logObjectKeyPrefix,
        };

        var putBucketLoggingRequest = new PutBucketLoggingRequest
        {
            BucketName = bucketName,
            LoggingConfig = loggingConfig,
        };
        await client.PutBucketLoggingAsync(putBucketLoggingRequest);
        Console.WriteLine($"Logging enabled.");
    }

    /// <summary>
    /// Loads configuration from settings files.
    /// </summary>
    public static void LoadConfig()
    {
        _configuration = new ConfigurationBuilder()
            .SetBasePath(Directory.GetCurrentDirectory())
            .AddJsonFile("settings.json") // Load settings from .json file.
    }

```

```
        .AddJsonFile("settings.local.json", true) // Optionally, load
local settings.
        .Build();
    }
}
```

- Per i dettagli sulle API, consulta la [PutBucketLogging](#) sezione AWS SDK per .NET API Reference.

Java

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.BucketLoggingStatus;
import software.amazon.awssdk.services.s3.model.LoggingEnabled;
import software.amazon.awssdk.services.s3.model.PartitionedPrefix;
import software.amazon.awssdk.services.s3.model.PutBucketLoggingRequest;
import software.amazon.awssdk.services.s3.model.TargetObjectKeyFormat;

// Class to set a bucket policy on a target S3 bucket and enable server access
// logging on a source S3 bucket.
public class ServerAccessLogging {
    private static S3Client s3Client;

    public static void main(String[] args) {
        String sourceBucketName = "SOURCE-BUCKET";
        String targetBucketName = "TARGET-BUCKET";
        String sourceAccountId = "123456789012";
        String targetPrefix = "logs/";

        // Create S3 Client.
        s3Client = S3Client.builder().
            region(Region.US_EAST_2)
            .build();

        // Set a bucket policy on the target S3 bucket to enable server access
        // logging by granting the
        // logging.s3.amazonaws.com principal permission to use the PutObject
        // operation.
        ServerAccessLogging serverAccessLogging = new ServerAccessLogging();
```

```

        serverAccessLogging.setTargetBucketPolicy(sourceAccountId, sourceBucketName,
targetBucketName);

        // Enable server access logging on the source S3 bucket.
        serverAccessLogging.enableServerAccessLogging(sourceBucketName,
targetBucketName,
            targetPrefix);

    }

    // Function to set a bucket policy on the target S3 bucket to enable server
access logging by granting the
// logging.s3.amazonaws.com principal permission to use the PutObject operation.
    public void setTargetBucketPolicy(String sourceAccountId, String
sourceBucketName, String targetBucketName) {
        String policy = "{\n" +
            "    \"Version\": \"2012-10-17\",\n" +
            "    \"Statement\": [\n" +
            "        {\n" +
            "            \"Sid\": \"S3ServerAccessLogsPolicy\",\n" +
            "            \"Effect\": \"Allow\",\n" +
            "            \"Principal\": {\"Service\": \"logging.s3.amazonaws.com
\n\"},\n" +
            "            \"Action\": [\n" +
            "                \"s3:PutObject\"\n" +
            "            ],\n" +
            "            \"Resource\": \"arn:aws:s3::\" + targetBucketName + "/*
\n\", \n" +
            "            \"Condition\": {\n" +
            "                \"ArnLike\": {\n" +
            "                    \"aws:SourceArn\": \"arn:aws:s3::\" +
sourceBucketName + "\"\n" +
            "                },\n" +
            "                \"StringEquals\": {\n" +
            "                    \"aws:SourceAccount\": \"\" + sourceAccountId +
"\n" +
            "                }\n" +
            "            }\n" +
            "        }\n" +
            "    ]\n" +
            "}";
        s3Client.putBucketPolicy(b -> b.bucket(targetBucketName).policy(policy));
    }

```



```
// Function to enable server access logging on the source S3 bucket.
public void enableServerAccessLogging(String sourceBucketName, String
targetBucketName,
    String targetPrefix) {
    TargetObjectKeyFormat targetObjectKeyFormat =
TargetObjectKeyFormat.builder()

.partitionedPrefix(PartitionedPrefix.builder().partitionDateSource("EventTime").build())
    .build();
    LoggingEnabled loggingEnabled = LoggingEnabled.builder()
        .targetBucket(targetBucketName)
        .targetPrefix(targetPrefix)
        .targetObjectKeyFormat(targetObjectKeyFormat)
        .build();
    BucketLoggingStatus bucketLoggingStatus = BucketLoggingStatus.builder()
        .loggingEnabled(loggingEnabled)
        .build();
    s3Client.putBucketLogging(PutBucketLoggingRequest.builder()
        .bucket(sourceBucketName)
        .bucketLoggingStatus(bucketLoggingStatus)
        .build());
}
}
```

Utilizzo di AWS CLI

Ti consigliamo di creare un bucket di registrazione dedicato in ogni bucket in Regione AWS cui hai bucket S3. Quindi, fare in modo che i log degli accessi Amazon S3 vengano recapitati al bucket S3. Per ulteriori informazioni ed esempi, consulta l'esempio [put-bucket-logging](#) in Riferimento ai comandi della AWS CLI .

Se il bucket di destinazione (target) utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, non sarà possibile impostare le ACL di bucket o di oggetti. Inoltre, non puoi includere le concessioni di destinazione (target) nella tua configurazione. [PutBucketLogging](#) È necessario utilizzare una policy di bucket per concedere l'accesso al principale del servizio di registrazione (logging.s3.amazonaws.com). Per ulteriori informazioni, consulta [Autorizzazioni per la distribuzione dei registri](#).

Example- Abilitare i log degli accessi con cinque bucket in due regioni

In questo esempio, sono presenti i cinque bucket seguenti:

- *amzn-s3-demo-source-bucket*-us-east-1
- *amzn-s3-demo-source-bucket1*-us-east-1
- *amzn-s3-demo-source-bucket2*-us-east-1
- *amzn-s3-demo-bucket1*-us-west-2
- *amzn-s3-demo-bucket2*-us-west-2

Note

Il passaggio finale della procedura seguente fornisce esempi di script bash che è possibile utilizzare per creare i bucket di registrazione di log e abilitare la registrazione di log degli accessi al server su questi bucket. Per utilizzare questi script, devi creare i file `policy.json` e `logging.json`, come descritto nella procedura seguente.

1. Crea due bucket di destinazione per la registrazione di log nelle regioni Stati Uniti occidentali (Oregon) e Stati Uniti orientali (N. Virginia) e assegna loro i nomi elencati di seguito:
 - *amzn-s3-demo-destination-bucket*-logs-us-east-1
 - *amzn-s3-demo-destination-bucket1*-logs-us-west-2
2. Più avanti in questi passaggi, abiliterai la registrazione di log degli accessi al server come segue:
 - *amzn-s3-demo-source-bucket*-us-east-1 accede al bucket S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 con prefisso *amzn-s3-demo-source-bucket*-us-east-1
 - *amzn-s3-demo-source-bucket1*-us-east-1 accede al bucket S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 con prefisso *amzn-s3-demo-source-bucket1*-us-east-1
 - *amzn-s3-demo-source-bucket2*-us-east-1 accede al bucket S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 con prefisso *amzn-s3-demo-source-bucket2*-us-east-1
 - *amzn-s3-demo-bucket1*-us-west-2 accede al bucket S3 *amzn-s3-demo-destination-bucket1*-logs-us-west-2 con prefisso *amzn-s3-demo-bucket1*-us-west-2

- *amzn-s3-demo-bucket2*-us-west-2 accede al bucket S3 *amzn-s3-demo-destination-bucket1*-logs-us-west-2 con prefisso *amzn-s3-demo-bucket2*-us-west-2
3. Per ogni bucket di registrazione di log di destinazione, concedi le autorizzazioni per la consegna di log di accesso al server utilizzando una ACL di bucket o una policy del bucket:
- Aggiorna la policy del bucket (consigliato): per concedere autorizzazioni al principale del servizio di registrazione di log, utilizza il comando `put-bucket-policy` seguente. Sostituisci *amzn-s3-demo-destination-bucket*-logs con il nome del tuo bucket di destinazione.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-destination-bucket-logs --
policy file://policy.json
```

`Policy.json` è un documento JSON nella cartella corrente che contiene la policy del bucket seguente. Per utilizzare questa policy del bucket, sostituisci *user input placeholders* con le tue informazioni. Nella policy seguente, *amzn-s3-demo-destination-bucket-logs* è il bucket di destinazione in cui verranno distribuiti i log degli accessi al server e *amzn-s3-demo-source-bucket* è il bucket di origine. *SOURCE-ACCOUNT-ID* è l'Account AWS proprietario del bucket di origine.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3ServerAccessLogsPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
      },
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket-logs/*",
      "Condition": {
        "ArnLike": {
```

```

        "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-
bucket"
      },
      "StringEquals": {
        "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
      }
    }
  ]
}

```

- Aggiorna l'ACL bucket: per concedere le autorizzazioni al gruppo di distribuzione dei log S3, utilizza il comando `put-bucket-acl` seguente. Sostituisci **amzn-s3-demo-destination-bucket-logs** con il nome del tuo bucket di destinazione (target).

```

aws s3api put-bucket-acl --bucket amzn-s3-demo-destination-bucket-logs --
grant-write URI=http://acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp
URI=http://acs.amazonaws.com/groups/s3/LogDelivery

```

4. Quindi, crea un file `logging.json` che contenga la configurazione di registrazione di log (in base a uno dei tre esempi che seguono). Dopo aver creato il file `logging.json`, puoi applicare la configurazione di registrazione di log utilizzando il comando `put-bucket-logging` seguente. Sostituisci **amzn-s3-demo-destination-bucket-logs** con il nome del tuo bucket di destinazione (target).

```

aws s3api put-bucket-logging --bucket amzn-s3-demo-destination-bucket-logs --
bucket-logging-status file://logging.json

```

Note

Invece di usare questo comando `put-bucket-logging` per applicare la configurazione di registrazione di log su ogni bucket di destinazione, puoi usare uno degli script bash forniti nel passaggio successivo. Per utilizzare questi script, devi creare i file `policy.json` e `logging.json`, come descritto in questa procedura.

Il file `logging.json` è un documento JSON nella cartella corrente che contiene la configurazione della registrazione di log. Se un bucket di destinazione utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, la configurazione di registrazione di log non può contenere concessioni di destinazione (target). Per ulteriori informazioni, consulta [Autorizzazioni per la distribuzione dei registri](#).

Example– `logging.json` senza sovvenzioni di destinazione (obiettivo)

Il seguente file di esempio `logging.json` contiene concessioni di destinazione (target). Pertanto, puoi applicare questa configurazione a un bucket di destinazione (target) che utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto.

```
{
  "LoggingEnabled": {
    "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
    "TargetPrefix": "amzn-s3-demo-destination-bucket/"
  }
}
```

Example– `logging.json` con sovvenzioni di destinazione (obiettivo)

Il seguente file di esempio `logging.json` contiene concessioni di destinazione (target).

Se un bucket di destinazione utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, non sarà possibile includere concessioni di destinazione (target) nella configurazione [PutBucketLogging](#). Per ulteriori informazioni, consulta [Autorizzazioni per la distribuzione dei registri](#).

```
{
  "LoggingEnabled": {
    "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
    "TargetPrefix": "amzn-s3-demo-destination-bucket/",
    "TargetGrants": [
      {
        "Grantee": {
          "Type": "CanonicalUser",
```

```

        "ID":
        "79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be"
      },
      "Permission": "FULL_CONTROL"
    }
  ]
}

```

Valori dell'assegnatario

È possibile specificare la persona (assegnatario) a cui si assegnano i diritti di accesso (utilizzando gli elementi della richiesta) nei seguenti modi:

- In base all'ID della persona:

```

{
  "Grantee": {
    "Type": "CanonicalUser",
    "ID": "ID"
  }
}

```

- In base all'URI:

```

{
  "Grantee": {
    "Type": "Group",
    "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
  }
}

```

Example– logging.json con il formato della chiave dell'oggetto di registro impostato sull'ora dell'evento S3

Il file logging.json seguente modifica il formato della chiave dell'oggetto di log in Ora evento S3.

```

{

```

```

    "LoggingEnabled": {
      "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
      "TargetPrefix": "amzn-s3-demo-destination-bucket/",
      "TargetObjectKeyFormat": {
        "PartitionedPrefix": {
          "PartitionDateSource": "EventTime"
        }
      }
    }
  }
}

```

5. Utilizza uno dei seguenti script bash per aggiungere la registrazione di log degli accessi per tutti i bucket nel tuo account. Sostituisci *amzn-s3-demo-destination-bucket-logs* con il nome del bucket di destinazione (target) e sostituisci *us-west-2* con il nome della regione in cui si trovano i bucket.

Note

Questo script funziona solo se tutti i bucket si trovano nella stessa regione. Se ci sono bucket in più regioni, è necessario modificare lo script.

Example– Concedi l'accesso con le policy del bucket e aggiungi la registrazione per i bucket nel tuo account

```

loggingBucket='amzn-s3-demo-destination-bucket-logs'
region='us-west-2'

# Create the logging bucket.
aws s3 mb s3://$loggingBucket --region $region

aws s3api put-bucket-policy --bucket $loggingBucket --policy file://policy.json

# List the buckets in this account.
buckets="$(aws s3 ls | awk '{print $3}')"

# Put a bucket logging configuration on each bucket.
for bucket in $buckets
do

```

```

    # This if statement excludes the logging bucket.
    if [ "$bucket" == "$loggingBucket" ] ; then
        continue;
    fi
    printf '{
        "LoggingEnabled": {
            "TargetBucket": "%s",
            "TargetPrefix": "%s/"
        }
    }' "$loggingBucket" "$bucket" > logging.json
    aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
    echo "$bucket done"
done

rm logging.json

echo "Complete"

```

Example– Concedi l'accesso con ACL di bucket e aggiungi la registrazione per i bucket nel tuo account

```

loggingBucket='amzn-s3-demo-destination-bucket-logs'
region='us-west-2'

# Create the logging bucket.
aws s3 mb s3://$loggingBucket --region $region

aws s3api put-bucket-acl --bucket $loggingBucket --grant-write URI=http://
acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp URI=http://
acs.amazonaws.com/groups/s3/LogDelivery

# List the buckets in this account.
buckets="$(aws s3 ls | awk '{print $3}')"

# Put a bucket logging configuration on each bucket.
for bucket in $buckets
do
    # This if statement excludes the logging bucket.
    if [ "$bucket" == "$loggingBucket" ] ; then
        continue;
    fi

```



```
fi
printf '{
  "LoggingEnabled": {
    "TargetBucket": "%s",
    "TargetPrefix": "%s/"
  }
}' "$loggingBucket" "$bucket" > logging.json
aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
echo "$bucket done"
done

rm logging.json

echo "Complete"
```

Verifica della configurazione dei log degli accessi al server

Dopo aver abilitato la registrazione degli accessi al server, completa la procedura riportata di seguito:

- Accedi al bucket di destinazione e verifica che i file di log vengano distribuiti. Una volta impostati i log di accesso, Amazon S3 inizia immediatamente ad acquisire le richieste e a registrarle. Tuttavia, potrebbero essere necessarie alcune ore prima che i log vengano consegnati al bucket di destinazione. Per ulteriori informazioni, consulta [the section called “Tempo richiesto per l'applicazione delle modifiche dello stato di registrazione del bucket”](#) e [the section called “Best-effort consegna dei log del server”](#).

Puoi anche verificare automaticamente la consegna dei log utilizzando le metriche di richiesta di Amazon S3 e impostando gli CloudWatch allarmi Amazon per queste metriche. Per ulteriori informazioni, consulta [Metriche di monitoraggio con Amazon CloudWatch](#).

- Verifica di essere in grado di aprire e leggere il contenuto dei file di log.

Per informazioni sulla risoluzione dei problemi relativi alla registrazione degli accessi al server, consultare [Risoluzione dei problemi di registrazione degli accessi al server](#).

Formato del log di accesso al server Amazon S3

La registrazione degli accessi al server fornisce record dettagliati per le richieste che sono effettuate a un bucket Amazon S3. È possibile utilizzare i log degli accessi al server per i seguenti scopi:

- Esecuzione di controlli di sicurezza e degli accessi
- Informazioni sulla base di clienti
- Informazioni sulla fatturazione Amazon S3

In questa sezione viene descritto il formato e altri dettagli sui file di log di accesso al server Amazon S3.

Note

Questa pagina illustra il formato di testo delimitato da spazi utilizzato per i log inviati a un bucket Amazon S3 per uso generico. Per il formato JSON strutturato utilizzato in Amazon Logs, consulta. CloudWatch [Formato del registro in CloudWatch Logs](#)

I file dei log di accesso al server sono composti da una sequenza di record dei log delimitati da una nuova riga. Ogni record di log rappresenta una richiesta ed è composto da campi delimitati da spazio.

Di seguito è riportato un esempio di log composto da cinque record di log.

Note

Qualsiasi campo può essere impostato su - per indicare che i dati sono sconosciuti o non disponibili, oppure che il campo non è applicabile a questa richiesta.

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 - 113 - 7 -
"- " "S3Console/0.4" - s91zHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-demo-bucket1.s3.us-
west-1.amazonaws.com TLSV1.2 arn:aws:s3:us-west-1:123456789012:accesspoint/example-AP
Yes us-east-1
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
REST.GET.LOGGING_STATUS - "GET /amzn-s3-demo-bucket1?logging HTTP/1.1" 200 -
242 - 11 - "- " "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mX0cqPGzQ0I5XLnCtZNPxev+Hf
```

```
+7tpT6sxDwDty4LHBU0ZJG96N1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - - us-east-1
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
REST.GET.BUCKETPOLICY - "GET /amzn-s3-demo-bucket1?policy HTTP/1.1" 404
NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLEmC78iwEIWxs99CRUrbS4n11234= SigV4 ECDHE-RSA-AES128-GCM-SHA256
AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - Yes us-east-1
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket1 [06/Feb/2019:00:01:00 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 -
113 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuULPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpbybfEseEME/u7ME1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - - us-east-1
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket1 [06/Feb/2019:00:01:57 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /amzn-s3-demo-bucket1/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
10S62Zv81kBW7BB6SX4XJ48o6kpc16LPwEoizZQxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
ECDHE-RSA-AES128-SHA AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com
TLSV1.2 - Yes us-east-1
```

Di seguito è riportato un esempio di record di log per l'operazione Calcola il checksum:

```
7cd47ef2be amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be e5042925-b524-4b3b-
a869-f3881e78ff3a S3.COMPUTE.OBJECT.CHECKSUM example-object - - - 1048576 - -
- - - bPf7qjG4XwYdPgDQT172GW/uotRhdpZ2UryEyAFLDSRmKrakUkJCYLTAw6fdANCrsUYc1M/
kIu1XM1u5vZQT5g== - - - - - - - -
```

Argomenti

- [Campi del record di log](#)
- [Registrazione aggiuntiva per operazioni di copia](#)
- [Informazioni sui log di accesso personalizzati](#)
- [Considerazioni in materia di programmazione per il formato esteso dei log di accesso al server](#)

Campi del record di log

L'elenco di seguito descrive i campi dei record di log.

Proprietario del bucket

L'ID utente canonico del proprietario del bucket di origine. L'ID utente canonico è un'altra forma di ID. Account AWS Per ulteriori informazioni sull'ID utente canonico, consulta la sezione relativa agli [identificatori Account AWS](#) nella Riferimenti generali di AWS. Per informazioni su come trovare l'ID utente canonico per il tuo account, consulta [Ricerca dell'ID utente canonico per l' Account AWS](#).

Esempio di inserimento

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

Il nome del bucket riguardo al quale è stata elaborata la richiesta. Se il sistema riceve una richiesta non corretta e non riesce a determinare il bucket, tale richiesta non apparirà in alcun log di accesso al server.

Esempio di inserimento

```
amzn-s3-demo-bucket1
```

Orario

L'ora di ricezione della richiesta; queste date e ore sono in formato UTC. Il formato, utilizzando la terminologia `strftime()`, è il seguente: [%d/%b/%Y:%H:%M:%S %z]

Esempio di inserimento

```
[06/Feb/2019:00:00:38 +0000]
```

IP remoto

Indirizzo IP apparente del richiedente. Dei proxy e firewall intermedi potrebbero oscurare l'indirizzo IP effettivo della macchina che effettua la richiesta.

Esempio di inserimento

```
192.0.2.3
```

Richiedente

L'ID utente canonico del richiedente o - per richieste non autenticate. Se il richiedente era un utente IAM, questo campo restituisce il nome utente IAM del richiedente insieme al nome a Account AWS cui appartiene l'utente IAM. Questo identificatore è lo stesso che viene usato per accedere a scopi di controllo.

Esempio di inserimento

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Se il richiedente utilizza un ruolo assunto, questo campo restituisce il ruolo IAM assunto.

Esempio di inserimento

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

ID di richiesta

Una stringa generata da Amazon S3 per identificare in maniera univoca ogni richiesta. Per le richieste del processo Calcola il checksum, il campo ID richiesta visualizza l'ID del processo associato. Per ulteriori informazioni, consulta [Calcolo dei checksum](#).

Esempio di inserimento

```
3E57427F33A59F07
```

Operazione

L'operazione elencata qui viene dichiarata come SOAP.*operation*, REST.*HTTP_method.resource_type*, WEBSITE.*HTTP_method.resource_type*, oppure BATCH.DELETE.OBJECT, oppure S3.action.resource_type per [Ciclo di vita S3 e registrazione](#). Per le richieste del processo [Compute checksum](#), l'operazione è elencata come S3.COMPUTE.OBJECT.CHECKSUM.

Esempio di inserimento

```
REST.PUT.OBJECT
```

```
S3.COMPUTE.OBJECT.CHECKSUM
```

Chiave

La parte chiave (nome dell'oggetto) della richiesta.

Esempio di inserimento

```
/photos/2019/08/puppy.jpg
```

Request-URI

La parte Request-URI del messaggio di richiesta HTTP. Questo campo può includere virgolette senza escape inserite dall'utente.

Esempio di inserimento

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

Stato HTTP

Il codice di stato HTTP numerico della risposta.

Esempio di inserimento

```
200
```

Codice di errore

Le [risposte di errore](#) di Amazon S3 o - se non si è verificato alcun errore.

Esempio di inserimento

```
NoSuchBucket
```

Byte inviati

Il numero di byte della risposta inviati, a esclusione di overhead di protocollo HTTP, o - se uguale a zero.

Esempio di inserimento

2662992

Dimensione oggetto

La dimensione totale dell'oggetto in questione.

Esempio di inserimento

3462992

Tempo totale

Il numero di millisecondi durante i quali la richiesta è stata in transito dalla prospettiva del server. Questo valore viene misurato dal momento in cui si riceve la richiesta al momento in cui viene inviato l'ultimo byte di risposta. Le misurazioni effettuate dalla prospettiva del cliente potrebbero essere più lunghe in ragione della latenza di rete.

Esempio di inserimento

70

Turn-Around Ora

Il numero di millisecondi che sono stati necessari ad Amazon S3 per elaborare la richiesta. Questo valore viene misurato dal momento in cui si riceve l'ultimo byte della richiesta al momento in cui viene inviato il primo byte di risposta.

Esempio di inserimento

10

Referer

Il valore dell'intestazione HTTP Referer, se presente. Gli utenti-agenti HTTP (ad esempio, i browser) generalmente impostano questa intestazione sull'URL della pagina di collegamento o incorporazione quando viene effettuata una richiesta. Questo campo può includere virgolette senza escape inserite dall'utente.

Esempio di inserimento

"http://www.example.com/webservices"

User-Agent

Il valore dell'intestazione HTTP User-Agent. Questo campo può includere virgolette senza escape tratte dall'input dell'utente.

Esempio di inserimento

```
"curl/7.15.1"
```

Versione ID

L'ID della versione nella richiesta oppure - se l'operazione non prevede un parametro `versionId`.

Esempio di inserimento

```
3HL4kqtJvjVBH40NrjfkD
```

ID host

`x-amz-id-2` o ID richiesta esteso Amazon S3.

Esempio di inserimento

```
s9lzhYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Signature Version

La versione della firma, `SigV2` o `SigV4`, utilizzata per autenticare la richiesta o un - per richieste non autenticate.

Esempio di inserimento

```
SigV2
```

Pacchetti di crittografia

La crittografia Transport Layer Security (TLS) negoziata per richieste HTTPS o - per HTTP.

Esempio di inserimento

```
ECDHE-RSA-AES128-GCM-SHA256
```


Tipo di autenticazione

Il tipo di autenticazione della richiesta utilizzato: AuthHeader per intestazioni autenticate, QueryString per stringa di query (URL prefirmato) o - per richieste non autenticate.

Esempio di inserimento

```
AuthHeader
```

Intestazione dell'host

L'endpoint utilizzato per connettersi ad Amazon S3.

Esempio di inserimento

```
s3.us-west-2.amazonaws.com
```

Alcune Regioni meno recenti supportano gli endpoint legacy. Potresti vedere questi endpoint nei log o nei log di accesso al server. AWS CloudTrail Per ulteriori informazioni, consulta [Endpoint legacy](#). Per un elenco completo degli endpoint e delle regioni Amazon S3, consultare la sezione relativa a [endpoint e quote di Amazon S3](#) nella Riferimenti generali di Amazon Web Services.

Versione TLS

La versione di Transport Layer Security (TLS) negoziata dal client. Il valore è uno dei seguenti: TLSv1.1, TLSv1.2, TLSv1.3 o - se non è stato utilizzato TLS.

Esempio di inserimento

```
TLSv1.2
```

Nome della risorsa Amazon (ARN) del punto di accesso

Il nome della risorsa Amazon (ARN) del punto di accesso della richiesta. Se il nome della risorsa Amazon (ARN) del punto di accesso ha un formato non valido oppure non viene utilizzato, il campo conterrà -. Per ulteriori informazioni sui punti di accesso, consulta [Utilizzo dei punti di accesso Amazon S3 per bucket per uso generico](#). Per maggiori informazioni sui nomi delle risorse Amazon (ARN), consulta [Nome della risorsa Amazon \(ARN\)](#) in Riferimenti generali di AWS .

Esempio di inserimento

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

Una stringa che indica se la richiesta richiede una lista di controllo degli accessi (ACL) per l'autorizzazione. Se la richiesta richiede una ACL per l'autorizzazione, la stringa è Yes. Se non sono richieste ACL, la stringa è -. Per ulteriori informazioni sulle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#). Per ulteriori informazioni sull'utilizzo del campo aclRequired per disabilitare le ACL, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Esempio di inserimento

```
Yes
```

Regione di origine

La AWS regione da cui proviene la richiesta. Questo campo mostra un trattino (-) quando non è possibile determinare la regione di origine (ad esempio PrivateLink connessioni, connessioni Direct Connect, indirizzi IP Bring your own (BYOIP) o indirizzi non IP) o quando il registro viene generato da operazioni attivate in base a politiche o azioni impostate dal cliente, come il ciclo di vita e il checksum.AWS

Esempio di inserimento

```
us-east-1
```

Registrazione aggiuntiva per operazioni di copia

Un'operazione di copia implica un GET e un PUT. Per questa ragione, vengono registrati due report quando si effettua un'operazione di logging. La tabella precedente descrive i campi che si riferiscono alla parte PUT dell'operazione. L'elenco di seguito descrive i campi nel record che si riferiscono alla parte GET dell'operazione di copia.

Proprietario del bucket

L'ID utente canonico del bucket archivia l'oggetto che viene copiato. L'ID utente canonico è un'altra forma dell'ID. Account AWS Per ulteriori informazioni sull'ID utente canonico, consulta la sezione relativa agli [identificatori Account AWS](#) nella Riferimenti generali di AWS. Per informazioni

su come trovare l'ID utente canonico per il tuo account, consulta [Ricerca dell'ID utente canonico per l' Account AWS](#).

Esempio di inserimento

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

Nome del bucket che archivia l'oggetto che viene copiato.

Esempio di inserimento

```
amzn-s3-demo-bucket1
```

Orario

L'ora di ricezione della richiesta; queste date e ore sono in formato UTC. Il formato, utilizzando la terminologia `strftime()`, è il seguente: [%d/%B/%Y:%H:%M:%S %z]

Esempio di inserimento

```
[06/Feb/2019:00:00:38 +0000]
```

IP remoto

Indirizzo IP apparente del richiedente. Dei proxy e firewall intermedi potrebbero oscurare l'indirizzo IP effettivo della macchina che effettua la richiesta.

Esempio di inserimento

```
192.0.2.3
```

Richiedente

L'ID utente canonico del richiedente o - per richieste non autenticate. Se il richiedente era un utente IAM, questo campo restituirà il nome utente IAM del richiedente insieme al nome a Utente root dell'account AWS cui appartiene l'utente IAM. Questo identificatore è lo stesso che viene usato per accedere a scopi di controllo.

Esempio di inserimento

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Se il richiedente utilizza un ruolo assunto, questo campo restituisce il ruolo IAM assunto.

Esempio di inserimento

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

ID di richiesta

Una stringa generata da Amazon S3 per identificare in maniera univoca ogni richiesta. Per le richieste del processo Calcola il checksum, il campo ID richiesta visualizza l'ID del processo associato. Per ulteriori informazioni, consulta [Calcolo dei checksum](#).

Esempio di inserimento

```
3E57427F33A59F07
```

Operazioni

Le operazioni qui elencate vengono dichiarate come SOAP.*operation*, REST.*HTTP_method.resource_type*, WEBSITE.*HTTP_method.resource_type* oppure BATCH.DELETE.OBJECT.

Esempio di inserimento

```
REST.COPY.OBJECT_GET
```

Chiave

La "chiave" (nome oggetto) dell'oggetto che viene copiato o - se l'operazione non prevede un parametro chiave.

Esempio di inserimento

```
/photos/2019/08/puppy.jpg
```

Request-URI

La parte Request-URI del messaggio di richiesta HTTP. Questo campo può includere virgolette senza escape inserite dall'utente.

Esempio di inserimento

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar"
```

Stato HTTP

Il codice di stato HTTP numerico della porzione GET dell'operazione di copia.

Esempio di inserimento

```
200
```

Codice di errore

Le [risposte di errore](#) di Amazon S3 della porzione GET dell'operazione di copia oppure - se non si è verificato alcun errore.

Esempio di inserimento

```
NoSuchBucket
```

Byte inviati

Numero di byte della risposta inviati, a esclusione di overhead di protocollo HTTP, o - se uguale a zero.

Esempio di inserimento

```
2662992
```

Dimensione oggetto

La dimensione totale dell'oggetto in questione.

Esempio di inserimento

```
3462992
```

Tempo totale

Il numero di millisecondi durante i quali la richiesta è stata in transito dalla prospettiva del server. Questo valore viene misurato dal momento in cui si riceve la richiesta al momento in cui viene

inviato l'ultimo byte di risposta. Le misurazioni effettuate dalla prospettiva del cliente potrebbero essere più lunghe in ragione della latenza di rete.

Esempio di inserimento

```
70
```

Turn-Around Ora

Il numero di millisecondi che sono stati necessari ad Amazon S3 per elaborare la richiesta. Questo valore viene misurato dal momento in cui si riceve l'ultimo byte della richiesta al momento in cui viene inviato il primo byte di risposta.

Esempio di inserimento

```
10
```

Referer

Il valore dell'intestazione HTTP `Referer`, se presente. Gli utenti-agenti HTTP (ad esempio, i browser) generalmente impostano questa intestazione sull'URL della pagina di collegamento o incorporazione quando viene effettuata una richiesta. Questo campo può includere virgolette senza escape inserite dall'utente.

Esempio di inserimento

```
"http://www.example.com/webservices"
```

User-Agent

Il valore dell'intestazione HTTP `User-Agent`. Questo campo può includere virgolette senza escape tratte dall'input dell'utente.

Esempio di inserimento

```
"curl/7.15.1"
```

Versione ID

ID versione dell'oggetto che viene copiato oppure - se l'intestazione `x-amz-copy-source` non specificava un parametro `versionId` come parte dell'origine della copia.

Esempio di inserimento

```
3HL4kqtJvjVBH40N1jfkD
```

ID host

x-amz-id-2 o ID richiesta esteso Amazon S3.

Esempio di inserimento

```
s91zHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Signature Version

Versione della firma, SigV2 o SigV4, utilizzata per autenticare la richiesta o - per richieste non autenticate.

Esempio di inserimento

```
SigV4
```

Pacchetti di crittografia

La crittografia Transport Layer Security (TLS) negoziata per richieste HTTPS o - per HTTP.

Esempio di inserimento

```
ECDHE-RSA-AES128-GCM-SHA256
```

Tipo di autenticazione

Tipo di autenticazione della richiesta utilizzato: AuthHeader per intestazioni autenticate, QueryString per stringa di query (URL prefirmati) o - per richieste non autenticate.

Esempio di inserimento

```
AuthHeader
```

Intestazione dell'host

L'endpoint utilizzato per connettersi ad Amazon S3.

Esempio di inserimento

```
s3.us-west-2.amazonaws.com
```

Alcune Regioni meno recenti supportano gli endpoint legacy. Potresti vedere questi endpoint nei log o nei log di accesso al server. AWS CloudTrail Per ulteriori informazioni, consulta [Endpoint legacy](#). Per un elenco completo degli endpoint e delle regioni Amazon S3, consultare la sezione relativa a [endpoint e quote di Amazon S3](#) nella Riferimenti generali di Amazon Web Services.

Versione TLS

La versione di Transport Layer Security (TLS) negoziata dal client. Il valore è uno dei seguenti: TLSv1.1, TLSv1.2, TLSv1.3 o - se non è stato utilizzato TLS.

Esempio di inserimento

```
TLSv1.2
```

Nome della risorsa Amazon (ARN) del punto di accesso

Il nome della risorsa Amazon (ARN) del punto di accesso della richiesta. Se il nome della risorsa Amazon (ARN) del punto di accesso ha un formato non valido oppure non viene utilizzato, il campo conterrà -. Per ulteriori informazioni sui punti di accesso, consulta [Utilizzo dei punti di accesso Amazon S3 per bucket per uso generico](#). Per maggiori informazioni sui nomi delle risorse Amazon (ARN), consulta [Nome della risorsa Amazon \(ARN\)](#) in Riferimenti generali di AWS .

Esempio di inserimento

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

Una stringa che indica se la richiesta richiede una lista di controllo degli accessi (ACL) per l'autorizzazione. Se la richiesta richiede una ACL per l'autorizzazione, la stringa è Yes. Se non sono richieste ACL, la stringa è -. Per ulteriori informazioni sulle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#). Per ulteriori informazioni sull'utilizzo del campo aclRequired per disabilitare le ACL, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Esempio di inserimento

```
Yes
```


Regione di origine

La AWS regione da cui proviene la richiesta. Questo campo mostra un trattino (-) quando non è possibile determinare la regione di origine (ad esempio PrivateLink connessioni, connessioni Direct Connect, indirizzi IP Bring your own (BYOIP) o indirizzi non IP) o quando il registro viene generato da operazioni attivate in base a politiche o azioni impostate dal cliente, come il ciclo di vita e il checksum.AWS

Esempio di inserimento

```
us-east-1
```

Informazioni sui log di accesso personalizzati

È possibile includere informazioni personalizzate da memorizzare nel record del log di accesso per una richiesta. A tale scopo, aggiungere un parametro di stringa query personalizzato all'URL per la richiesta. Amazon S3 ignora i parametri di stringa di query che iniziano con x-, ma include quelli nel record del log degli accessi per la richiesta, come parte del campo Request-URI del record del log.

Ad esempio, una richiesta GET per "s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-user=johndoe" funziona come la richiesta "s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg", ad eccezione del fatto che la stringa "x-user=johndoe" è inclusa nel campo Request-URI per il record di log associato. Questa funzionalità è disponibile solo nell'interfaccia REST.

Considerazioni in materia di programmazione per il formato esteso dei log di accesso al server

Occasionalmente è possibile estendere il formato del report del log degli accessi aggiungendo nuovi campi alla fine di ogni linea. Pertanto, è necessario che il codice che analizza i log degli accessi al server sia in grado di gestire i campi che potrebbero non essere riconosciuti.

Gestione della conservazione dei log

Un bucket Amazon S3 con la registrazione degli accessi al server abilitata può accumulare nel tempo molti oggetti del log del server. Puoi utilizzare la configurazione del ciclo di vita di Amazon S3 per impostare regole in modo che Amazon S3 elimini automaticamente gli oggetti di log dopo un periodo specificato. Se hai specificato un prefisso nella tua configurazione di registrazione, puoi adattare la regola del ciclo di vita a quel prefisso. Ad esempio, se gli oggetti di log hanno il prefisso logs/, è possibile creare una regola del ciclo di vita per eliminare tutti gli oggetti con quel prefisso dopo

un determinato numero di giorni. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#).

Per i log inviati a Logs, vedere. CloudWatch [Gestione della conservazione dei log](#)

Utilizzo dei log degli accessi al server Amazon S3 per identificare le richieste

Puoi identificare le richieste Amazon S3 con i log degli accessi al server Amazon S3.

Note

- Per identificare le richieste di Amazon S3, ti consigliamo di utilizzare eventi di AWS CloudTrail dati anziché i log di accesso al server Amazon S3. CloudTrail gli eventi di dati sono più facili da configurare e contengono più informazioni. Per ulteriori informazioni, consulta [Identificazione delle richieste Amazon S3 utilizzando CloudTrail](#).
- A seconda del numero di richieste di accesso ricevute, l'analisi dei registri potrebbe richiedere più risorse o più tempo rispetto all'utilizzo di eventi di CloudTrail dati.

Argomenti

- [Esecuzione di query sui log degli accessi per le richieste tramite Amazon Athena](#)
- [Identificazione delle richieste di Signature Version 2](#)
- [Identificazione delle richieste di accesso agli oggetti](#)

Esecuzione di query sui log degli accessi per le richieste tramite Amazon Athena

Puoi identificare le richieste ad Amazon S3 con i log degli accessi ad Amazon S3 utilizzando Amazon Athena.

Amazon S3 archivia i log degli accessi al server come oggetti in un bucket S3. Spesso è più facile utilizzare uno strumento in grado di analizzare i log in Amazon S3. Athena supporta l'analisi di oggetti S3 e può essere utilizzato per eseguire query sui log degli accessi Amazon S3.

Example

L'esempio seguente mostra come eseguire query sui log degli accessi al server Amazon S3 in Amazon Athena. Sostituisci *user input placeholders* che trovi nei seguenti esempi con le tue informazioni.

 Note

Per specificare una posizione Amazon S3 in una query Athena, devi fornire un URI S3 per il bucket in cui vengono distribuiti i log. Questo URI deve includere il nome e il prefisso del bucket nel seguente formato: `s3://amzn-s3-demo-bucket1-logs/prefix/`

1. Apri la console Athena all'indirizzo <https://console.aws.amazon.com/athena/>.
2. Nel Query Editor esegui un comando simile al seguente. Sostituisci `s3_access_logs_db` con il nome che desideri assegnare al database.

```
CREATE DATABASE s3_access_logs_db
```

 Note

È consigliabile creare il database nello stesso bucket Regione AWS S3.

3. Nel Query Editor eseguire un comando simile al seguente per creare uno schema di tabella nel database creato nella fase 2. Sostituisci `s3_access_logs_db.mybucket_logs` con il nome che desideri assegnare alla tabella. I valori dei tipi di dati STRING e BIGINT sono le proprietà del log di accesso. È possibile eseguire query su queste proprietà in Athena. Per LOCATION, immettere il percorso del prefisso e il bucket S3 come indicato in precedenza.

Date-based partitioning

```
CREATE EXTERNAL TABLE s3_access_logs_db.mybucket_logs(  
  `bucketowner` STRING,  
  `bucket_name` STRING,  
  `requestdatetime` STRING,  
  `remoteip` STRING,  
  `requester` STRING,  
  `requestid` STRING,  
  `operation` STRING,  
  `key` STRING,  
  `request_uri` STRING,  
  `httpstatus` STRING,  
  `errorcode` STRING,  
  `bytessent` BIGINT,  
  `objectsize` BIGINT,
```

```

`totaltime` STRING,
`turnaroundtime` STRING,
`referrer` STRING,
`useragent` STRING,
`versionid` STRING,
`hostid` STRING,
`sigv` STRING,
`ciphersuite` STRING,
`authtype` STRING,
`endpoint` STRING,
`tlsversion` STRING,
`accesspointarn` STRING,
`aclrequired` STRING,
`sourceregion` STRING)
PARTITIONED BY (
    `timestamp` string)
ROW FORMAT SERDE
    'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
    'input.regex'='([^\ ]*) ([^\ ]*) \\[(.\\?)\\] ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) (\\\"[^\"]*\\\"|-) (-|[0-9]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) (\\\"[^\"]*\\\"|-) ([^\ ]*)(?: ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*))?.*\\$')
STORED AS INPUTFORMAT
    'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
    'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
    's3://bucket-name/prefix-name/account-id/region/source-bucket-name/'
TBLPROPERTIES (
    'projection.enabled'='true',
    'projection.timestamp.format'='yyyy/MM/dd',
    'projection.timestamp.interval'='1',
    'projection.timestamp.interval.unit'='DAYS',
    'projection.timestamp.range'='2024/01/01,NOW',
    'projection.timestamp.type'='date',
    'storage.location.template'='s3://bucket-name/prefix-name/account-id/region/  

source-bucket-name/${timestamp}')

```

Non-date-based partitioning

```
CREATE EXTERNAL TABLE `s3_access_logs_db.mybucket_logs`(  
  `bucketowner` STRING,
```

```

    `bucket_name` STRING,
    `requestdatetime` STRING,
    `remoteip` STRING,
    `requester` STRING,
    `requestid` STRING,
    `operation` STRING,
    `key` STRING,
    `request_uri` STRING,
    `httpstatus` STRING,
    `errorcode` STRING,
    `bytessent` BIGINT,
    `objectsize` BIGINT,
    `totaltime` STRING,
    `turnaroundtime` STRING,
    `referrer` STRING,
    `useragent` STRING,
    `versionid` STRING,
    `hostid` STRING,
    `sigv` STRING,
    `ciphersuite` STRING,
    `authtype` STRING,
    `endpoint` STRING,
    `tlsversion` STRING,
    `accesspointarn` STRING,
    `aclrequired` STRING,
    `sourcereion` STRING)
ROW FORMAT SERDE
    'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
    'input.regex'= '([^\ ]*) ([^\ ]*) \\[(.??)\\] ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*)
    ([^\ ]*) (\\\"[^\"]*\\\"|-) (-|[0-9]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*)
    ([^\ ]*) (\\\"[^\"]*\\\"|-) ([^\ ]*)(?: ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*)
    ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*))?.*$',
    'output.regex'= '([^\ ]*) ([^\ ]*) \\[(.??)\\] ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*)
    ([^\ ]*) (\\\"[^\"]*\\\"|-) (-|[0-9]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*)
    ([^\ ]*) (\\\"[^\"]*\\\"|-) ([^\ ]*)(?: ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*)
    ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*))?.*$',
    'serialization.format'= '1'
)
STORED AS INPUTFORMAT
    'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
    'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
    's3://amzn-s3-demo-bucket1-logs/prefix/'

```

4. Nel riquadro di navigazione, in Database, scegliere il database.
5. In Tables (Tabelle), scegliere Preview table (Anteprima tabella) accanto al nome della tabella.

Nel pannello Results (Risultati), dovrebbero essere visualizzati i dati dai log di accesso al server, come bucketowner, bucket, requestdatetime e così via. Questo indica che la tabella Athena è stata creata correttamente. È ora possibile eseguire query sui log degli accessi al server Amazon S3.

Example- Visualizza chi ha eliminato un oggetto e quando (timestamp, indirizzo IP e utente IAM)

```
SELECT requestdatetime, remoteip, requester, key
FROM s3_access_logs_db.mybucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Example- Visualizza tutte le operazioni eseguite da un utente IAM

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

Example- Visualizza tutte le operazioni eseguite su un oggetto in un periodo di tempo specifico

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE Key='prefix/images/picture.jpg'
AND parse_datetime(requestdatetime, 'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2017-02-18:07:00:00', 'yyyy-MM-dd:HH:mm:ss')
AND parse_datetime('2017-02-18:08:00:00', 'yyyy-MM-dd:HH:mm:ss');
```

Example: visualizza la quantità di dati trasferiti da un indirizzo IP specifico in un determinato periodo di tempo

```
SELECT coalesce(SUM(bytesent), 0) AS bytesenttotal
FROM s3_access_logs_db.mybucket_logs
WHERE remoteip='192.0.2.1'
AND parse_datetime(requestdatetime, 'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-06-01', 'yyyy-MM-dd')
AND parse_datetime('2022-07-01', 'yyyy-MM-dd');
```

Example- Trova gli ID delle richieste per gli errori HTTP 5xx in un periodo di tempo specifico

```
SELECT requestdatetime, key, httpstatus, errorcode, requestid, hostid
```

```
FROM s3_access_logs_db.mybucket_logs
WHERE httpstatus like '5%' AND timestamp
BETWEEN '2024/01/29'
AND '2024/01/30'
```

Identificazione delle richieste di Signature Version 2

È possibile utilizzare i log di accesso al server per identificare le richieste di Signature Version 2. Per informazioni dettagliate sull'interrogazione dei log con Amazon Athena, consulta la sezione sulle interrogazioni di Athena in: [Invio di log a un bucket Amazon S3 per uso generico](#)

Identificazione delle richieste di accesso agli oggetti

È possibile utilizzare i log di accesso al server per identificare i modelli di accesso agli oggetti. Per informazioni dettagliate sull'interrogazione dei log con Amazon Athena, consulta la sezione sulle interrogazioni di Athena in: [Invio di log a un bucket Amazon S3 per uso generico](#)

Risoluzione dei problemi di registrazione degli accessi al server

Gli argomenti seguenti possono essere utili per risolvere i problemi che possono verificarsi durante la configurazione della registrazione con Amazon S3.

Argomenti

- [Messaggi di errore comuni durante la configurazione della registrazione](#)
- [Risoluzione dei problemi di consegna](#)

Messaggi di errore comuni durante la configurazione della registrazione

I seguenti messaggi di errore comuni possono apparire quando abiliti la registrazione tramite () e SDK: AWS Command Line Interface AWS CLI AWS

Errore: Registrazione multi-posizione S3 non consentita

Se il bucket di destinazione (noto anche come bucket target) si trova in una regione diversa da quella del bucket di origine, si verifica l'errore Registrazione multi-posizione S3 non consentita. Per risolvere questo errore, assicurati che il bucket di destinazione configurato per ricevere i log di accesso sia nello stesso Regione AWS e nel bucket di Account AWS origine.

Errore: Il proprietario del bucket da registrare e quello del bucket di destinazione devono coincidere

Quando si abilita la registrazione degli accessi al server, questo errore si verifica se il bucket di destinazione specificato appartiene a un account diverso. Per risolvere questo errore, assicurati che il bucket di destinazione sia nello stesso bucket di Account AWS origine.

Note

Ti consigliamo di scegliere un bucket di destinazione diverso dal bucket di origine. Quando il bucket di origine e il bucket di destinazione coincidono, vengono creati log aggiuntivi per i log scritti nel bucket. Questa situazione può causare l'aumento delle spese di archiviazione. La registrazione di questi log aggiuntivi può rendere difficile la ricerca di log specifici. Tuttavia, per una gestione più semplice dei log, si consiglia di salvare i log degli accessi in un bucket diverso.

Errore: Il bucket di destinazione per la registrazione non esiste

Il bucket di destinazione deve esistere prima di impostare la configurazione. Questo errore indica che il bucket di destinazione non esiste o non può essere trovato. Verifica che il nome del bucket sia stato digitato correttamente, quindi riprova.

Errore: Concessioni di destinazione non consentite per i bucket con l'opzione Bucket owner enforced abilitata

Questo errore indica che il bucket di destinazione utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3. L'impostazione Proprietario del bucket applicato non supporta le concessioni di destinazione (target). Per ulteriori informazioni, consulta [Autorizzazioni per la distribuzione dei registri](#).

Risoluzione dei problemi di consegna

Per evitare problemi di registrazione degli accessi al server, assicurati di seguire queste best practice:

- Il gruppo di distribuzione dei log S3 dispone dell'accesso in scrittura al bucket di destinazione: il gruppo di distribuzione dei log S3 fornisce i log degli accessi al server al bucket di destinazione. Puoi usare una policy del bucket o una lista di controllo degli accessi (ACL) di un bucket per concedere l'accesso in scrittura al bucket di destinazione. Invece di una lista di controllo degli accessi (ACL) consigliamo di utilizzare una policy di bucket. Per ulteriori informazioni su come concedere l'accesso in scrittura al bucket di destinazione, consulta [Autorizzazioni per la distribuzione dei registri](#).

 Note

Se il bucket di destinazione utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto, tieni presente quanto segue:

- Le ACL sono disabilitate e non hanno più alcuna ripercussione sulle autorizzazioni. Ciò significa che non è possibile aggiornare l'ACL del bucket per concedere l'accesso al gruppo di distribuzione dei log S3. Invece, è necessario aggiornare la policy del bucket per il bucket di destinazione per concedere l'accesso al principale del servizio di registrazione.
- Non puoi includere concessioni di destinazione nella configurazione PutBucketLogging.

- La policy del bucket per il bucket di destinazione consente l'accesso ai log: controlla la policy del bucket del bucket di destinazione. Nella policy di bucket cerca tutte le istruzioni contenenti "Effect": "Deny". Verifica quindi che l'istruzione Deny non impedisca la scrittura dei log di accesso nel bucket.
- S3 Object Lock non è abilitato sul bucket di destinazione: controlla se per il bucket di destinazione è stata abilitata l'opzione Object Lock. L'opzione Blocco oggetti blocca la consegna del log degli accessi al server. È necessario scegliere un bucket di destinazione in cui non sia abilitata l'opzione Object Lock.
- Il bucket di destinazione deve utilizzare le chiavi gestite di Amazon S3 (SSE-S3): se il bucket di destinazione utilizza la crittografia SSE-KMS predefinita, gli oggetti di log potrebbero essere creati ma crittografati con una chiave a cui non puoi accedere.
- Nel bucket di destinazione l'opzione Pagamento a carico del richiedente non è abilitata: non è supportato l'uso di un bucket con pagamento a carico del richiedente come bucket di destinazione per la registrazione degli accessi al server. Per consentire la consegna dei log di accesso ai server, disabilita l'opzione Pagamento a carico del richiedente nel bucket di destinazione.
- Rivedi le politiche di controllo dei AWS Organizations servizi (SCP) e le politiche di controllo delle risorse (RCP): durante l'utilizzo AWS Organizations, controlla le politiche di controllo dei servizi e le politiche di controllo delle risorse per assicurarti che l'accesso ad Amazon S3 sia consentito. Queste policy specificano le autorizzazioni massime per i principali e le risorse negli account interessati. Cerca nelle policy tutte le istruzioni che contengono "Effect": "Deny" e verificare che le istruzioni Deny non impediscano la scrittura dei log degli accessi nel bucket. Per ulteriori informazioni, consulta le [policy di autorizzazione in AWS Organizations](#) nella Guida all'utente AWS Organizations .

- Attendi qualche minuto affinché le modifiche recenti alla configurazione dei log siano effettive: l'abilitazione della registrazione di accesso ai server per la prima volta o la modifica del bucket di destinazione per i log richiede tempo per essere pienamente effettiva. Potrebbe essere necessaria più di un'ora prima che tutte le richieste vengano registrate e consegnate correttamente.

Per verificare eventuali errori di consegna dei log, abilita le metriche delle richieste in Amazon CloudWatch. Se i log non vengono consegnati entro poche ore, cerca la metrica `4xxErrors`, che può indicare gli errori di consegna dei log. Per ulteriori informazioni sull'abilitazione delle metriche delle richieste, consulta [the section called “Creazione di una configurazione di parametri per tutti gli oggetti”](#).

Metriche di monitoraggio con Amazon CloudWatch

CloudWatch Le metriche di Amazon per Amazon S3 possono aiutarti a comprendere e migliorare le prestazioni delle applicazioni che utilizzano Amazon S3. Esistono diversi modi per utilizzarlo CloudWatch con Amazon S3.

Daily storage metrics for buckets (Parametri di archiviazione giornalieri per i bucket)

Monitora il bucket storage utilizzando CloudWatch, che raccoglie ed elabora i dati di storage da Amazon S3 in metriche giornaliere leggibili. Questi parametri di storage per Amazon S3 vengono indicati una volta al giorno e sono disponibili per tutti i clienti senza costi aggiuntivi.

Request metrics (Parametri di richiesta)

Puoi monitorare le richieste di Amazon S3 per identificare rapidamente i problemi operativi e intraprendere le operazioni appropriate. I parametri sono disponibili a intervalli di 1 minuto dopo una determinata latenza di elaborazione. Queste CloudWatch metriche vengono fatturate alla stessa tariffa delle metriche personalizzate di Amazon CloudWatch. Per informazioni sui prezzi, consulta [i prezzi di Amazon CloudWatch](#). Per informazioni su come ottenere questi parametri, consulta [CloudWatch configurazioni delle metriche](#).

Quando sono abilitati, i parametri della richiesta vengono indicati per tutte le operazioni sull'oggetto. Per default, questi parametri da 1 minuto sono disponibili a livello di bucket di Amazon S3. Puoi anche definire un filtro per i parametri usando un prefisso condiviso, un tag oggetto o un punto di accesso:

- Punto di accesso: i punti di accesso sono endpoint di rete denominati e allegati a bucket che semplificano la gestione degli accessi ai dati su vasta scala per set di dati condivisi in S3. Con il filtro del punto di accesso, puoi ottenere informazioni dettagliate sull'utilizzo del punto

di accesso. Per ulteriori informazioni sui punti di accesso, consulta la sezione [Monitoraggio e registrazione degli access point](#).

- **Prefisso:** sebbene il modello di dati Amazon S3 abbia una struttura orizzontale, puoi applicare una gerarchia utilizzando i prefissi. Un prefisso è simile a un nome di directory che consente di raggruppare oggetti simili in un bucket. La console S3 supporta i prefissi con il concetto delle cartelle. Se si applica un filtro basato sul prefisso, gli oggetti con lo stesso prefisso verranno inclusi nella configurazione del parametro. Per ulteriori informazioni sui prefissi, consulta [Organizzazione degli oggetti utilizzando i prefissi](#).
- **Tag:** puoi aggiungere tag, che sono coppie di nomi chiave-valore, agli oggetti. I tag consentono di trovare e organizzare gli oggetti in modo semplice. Puoi inoltre possibile utilizzare i tag come filtro per le configurazioni dei parametri, in modo che nella configurazione vengano inclusi solo gli oggetti con tali tag. Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#).

Per allineare questi parametri a specifiche applicazioni business, flussi di lavoro o organizzazioni interne, puoi applicare un filtro in base a un prefisso condiviso, un tag oggetto o un punto di accesso.

Replication metrics (Parametri di replica)

Monitorare il numero totale di operazioni API S3 in attesa di replica, la dimensione totale degli oggetti in attesa di replica, il tempo massimo di replica alla destinazione Regione AWS e il numero totale di operazioni che non sono riuscite ad essere replicate. Le regole di replica con il controllo del tempo di replica di S3 (S3 RTC) o le metriche di replica S3 abilitati pubblicheranno le metriche di replica.

Per ulteriori informazioni, consulta [Monitoraggio della replica con parametri, notifiche di eventi e stati](#) o [Soddisfazione dei requisiti di conformità con il controllo del tempo di replica di Amazon S3](#).

Parametri di Amazon S3 Storage Lens

Puoi pubblicare le metriche di utilizzo e attività di S3 Storage Lens su Amazon CloudWatch per creare una visione unificata dello stato operativo nelle dashboard. CloudWatch https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html

I parametri di S3 Storage Lens sono disponibili nello spazio dei nomi AWS/S3/Storage-Lens. L'opzione di CloudWatch pubblicazione è disponibile per i dashboard di S3 Storage Lens aggiornati a metriche e raccomandazioni avanzate. Puoi abilitare l'opzione di CloudWatch pubblicazione per una configurazione del dashboard nuova o esistente in S3 Storage Lens.

Per ulteriori informazioni, consulta [Monitora le metriche di S3 Storage Lens in CloudWatch](#).

Tutte le CloudWatch statistiche vengono conservate per un periodo di 15 mesi in modo da poter accedere alle informazioni storiche e ottenere una prospettiva migliore sulle prestazioni dell'applicazione o del servizio web. Per ulteriori informazioni CloudWatch, consulta [Cos'è Amazon CloudWatch?](#) nella Guida per CloudWatch l'utente di Amazon. Potresti aver bisogno di alcune configurazioni aggiuntive per i tuoi CloudWatch allarmi, a seconda dei casi d'uso. Ad esempio, puoi utilizzare un'espressione matematica metrica per creare un allarme. Per ulteriori informazioni, consulta [Use CloudWatch metrics](#), [Use metric math](#), [Using Amazon CloudWatch alarms](#) e [Create a CloudWatch alarm based on a metric math expression nella Amazon User Guide](#). CloudWatch

Best-effort CloudWatch consegna delle metriche

CloudWatch le metriche vengono fornite con il massimo impegno possibile. La maggior parte delle richieste per un oggetto Amazon S3 con metriche di richiesta comportano l'invio di un punto dati a CloudWatch

La completezza e la tempestività dei parametri non è garantita. È possibile che il data point per una richiesta specifica venga restituito con un timestamp successivo a quello del momento effettivo di elaborazione della richiesta. Il data point potrebbe subire un ritardo di un minuto prima di essere disponibile oppure potrebbe non essere consegnato affatto. CloudWatch CloudWatch le metriche relative alle richieste ti danno un'idea della natura del traffico diretto verso il tuo bucket in tempo quasi reale, ma non intendono essere un resoconto completo di tutte le richieste.

Dalla natura best-effort di questa funzione deriva che i report disponibili nella [dashboard di gestione dei costi e della fatturazione](#) potrebbero includere una o più richieste di accesso che non compaiono nelle metriche del bucket.

Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

- [Metriche e dimensioni](#)
- [Accesso alle CloudWatch metriche](#)
- [CloudWatch configurazioni delle metriche](#)

Metriche e dimensioni

Le metriche e le dimensioni di storage che Amazon S3 invia ad Amazon CloudWatch sono elencate nelle tabelle seguenti.

Best-effort CloudWatch consegna delle metriche

CloudWatch le metriche vengono fornite con il massimo impegno possibile. La maggior parte delle richieste per un oggetto Amazon S3 con metriche di richiesta comportano l'invio di un punto dati a CloudWatch.

La completezza e la tempestività dei parametri non è garantita. È possibile che il data point per una richiesta specifica venga restituito con un timestamp successivo a quello del momento effettivo di elaborazione della richiesta. Il data point potrebbe subire un ritardo di un minuto prima di essere disponibile oppure potrebbe non essere consegnato affatto. CloudWatch le metriche relative alle richieste ti danno un'idea della natura del traffico diretto verso il tuo bucket in tempo quasi reale, ma non intendono essere un resoconto completo di tutte le richieste.

Dalla natura best-effort di questa funzione deriva che i report disponibili nella [dashboard di gestione dei costi e della fatturazione](#) potrebbero includere una o più richieste di accesso che non compaiono nelle metriche del bucket.

Argomenti

- [Metriche di storage giornaliere di Amazon S3 per i bucket in CloudWatch](#)
- [Metriche delle richieste di Amazon S3 in CloudWatch](#)
- [Metriche di replica S3 in CloudWatch](#)
- [Metriche di S3 Storage Lens in CloudWatch](#)
- [Metriche di richiesta S3 Object Lambda in CloudWatch](#)
- [Dimensioni di Amazon S3 in CloudWatch](#)
- [Dimensioni di replica S3 in CloudWatch](#)
- [Dimensioni dell'obiettivo di archiviazione S3 in CloudWatch](#)
- [Dimensioni della richiesta S3 Object Lambda in CloudWatch](#)
- [Metriche di utilizzo di Amazon S3](#)

Metriche di storage giornaliere di Amazon S3 per i bucket in CloudWatch

Il namespace AWS/S3 include i seguenti parametri di storage giornalieri per i bucket.

Parametro	Description
BucketSizeBytes	La quantità di dati in byte archiviati in un bucket nelle seguenti classi di archiviazione:

Parametro	Description
	<div><ul style="list-style-type: none">Reduced Redundancy Storage (RRS) (REDUCED_REDUNDANCY)S3 Express One Zone (EXPRESS_ONEZONE)Deep Archive Amazon S3 Glacier (DEEP_ARCHIVE)Recupero flessibile Amazon S3 Glacier (GLACIER)Recupero istantaneo Amazon S3 Glacier (GLACIER_IR)S3 () Intelligent-Tiering INTELLIGENT_TIERINGS3 One Zone-Infrequent Access () ONEZONE_IAAmazon S3 Standard (STANDARD)Standard-Infrequent Accesso S3 () STANDARD_IA</div> <p>Questo valore è calcolato sommando le dimensioni di tutti gli oggetti e i metadati (come i nomi dei bucket) nel bucket (sia gli oggetti correnti che quelli non correnti), comprese le dimensioni di tutte le parti per tutti i caricamenti multiparte incompleti nel bucket.</p> <div><div> Note</div><div>La classe di storage S3 Express One Zone è disponibile solo per i bucket di directory.</div></div> <p>Filtri di tipo storage validi (consulta la dimensione StorageType):</p> <ul style="list-style-type: none">Reduced Redundancy Storage (RRS): ReducedRedundancyStorageS3 Express One Zone: ExpressOneZoneStorageS3 Glacier Deep Archive: DeepArchiveObjectOverhead , DeepArchiveS3ObjectOverhead , DeepArchiveStagingStorage , DeepArchiveStorageRecupero flessibile S3 Glacier: GlacierObjectOverhead , GlacierS3ObjectOverhead , GlacierStagingStorage , GlacierStorage

Parametro	Description
	<ul style="list-style-type: none"> Recupero istantaneo S3 Glacier: <code>GlacierInstantRetrievalStorage</code> , <code>GlacierIRSizeOverhead</code> S3 Intelligent-Tiering: <code>IntelligentTieringAAStorage</code> , <code>IntelligentTieringAIStorage</code> , <code>IntelligentTieringDAStorage</code> , <code>IntelligentTieringFAStorage</code> , <code>IntelligentTieringIAStorage</code> Zone-Infrequent Accesso S3 One: <code>OneZoneIASizeOverhead</code> , <code>OneZoneIAStorage</code> Standard S3: <code>StandardStorage</code> Standard-Infrequent Accesso S3: <code>StandardIAObjectOverhead</code> , <code>StandardIASizeOverhead</code> , <code>StandardIAStorage</code> <p>Unità: byte</p> <p>Statistiche valide: media</p> <p>Per ulteriori informazioni sulle dimensioni di <code>StorageType</code> , consulta the section called “Dimensioni di Amazon S3 in CloudWatch”.</p>
<code>NumberOfObjects</code>	<p>Il numero totale di oggetti archiviati in un bucket a uso generico per tutte le classi di archiviazione. Questo valore è calcolato contando tutti gli oggetti nel bucket (sia oggetti correnti che non correnti), elimina marcatori e il numero totale di parti dei caricamenti in più parti incompleti nel bucket. Per i bucket di directory con oggetti nella classe di archiviazione S3 Express One Zone, questo valore viene calcolato contando tutti gli oggetti nel bucket, ma non include i caricamenti in più parti incompleti nel bucket.</p> <p>Filtri validi per il tipo di storage: <code>AllStorageTypes</code> (vedi la dimensione <code>StorageType</code>)</p> <p>Unità: numero</p> <p>Statistiche valide: media</p>

Metriche delle richieste di Amazon S3 in CloudWatch

Il namespace `AWS/S3` include i seguenti parametri di richiesta. Queste metriche includono le richieste non fatturabili (nel caso delle richieste di GET da `CopyObject` e `Replication`).

Metrica	Descrizione
<code>AllRequests</code>	<p>Numero totale di richieste HTTP effettuate a un bucket Amazon S3, indipendentemente dal tipo. Se utilizzi la configurazione di una metrica con un filtro, questa metrica restituisce solo le richieste HTTP che soddisfano i requisiti del filtro.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
<code>GetRequests</code>	<p>Numero totale di richieste HTTP GET effettuate per gli oggetti in un bucket Amazon S3. Non sono incluse le operazioni LIST. Questa metrica viene incrementata per l'origine di ogni richiesta <code>CopyObject</code>.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p> <div> Note Richieste paginate orientate all'elenco, come ListMultipartUploads, ListParts, ListObjectVersions, e altre, non sono incluse in questa metrica.</div>
<code>PutRequests</code>	<p>Numero totale di richieste HTTP PUT effettuate per gli oggetti in un bucket Amazon S3. Questa metrica viene incrementata per la destinazione di ogni richiesta <code>CopyObject</code>.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>

Metrica	Descrizione
DeleteRequests	<p>Numero totale di richieste HTTP DELETE effettuate per gli oggetti in un bucket Amazon S3. Questa metrica include anche DeleteObjects richieste. Questa metrica mostra il numero di richieste effettuate e non il numero di oggetti eliminati.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
HeadRequests	<p>Numero di richieste HTTP HEAD effettuate su un bucket Amazon S3.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
PostRequests	<p>Numero di richieste HTTP POST effettuate su un bucket Amazon S3.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p> <div> Note DeleteObjects e SelectObjectContent le richieste non sono incluse in questa metrica.</div>
SelectRequests	<p>Il numero di richieste Amazon S3 SelectObjectContent effettuate per gli oggetti in un bucket Amazon S3.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>

Metrica	Descrizione
SelectBytesScanned	<p>Il numero di byte di dati scansionati con le richieste di Amazon S3 SelectObjectContent in un bucket Amazon S3.</p> <p>Unità: byte</p> <p>Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo, massimo (come p100), qualsiasi percentile tra p0,0 e p99,9</p>
SelectBytesReturned	<p>Il numero di byte di dati restituiti con le richieste Amazon S3 SelectObjectContent in un bucket Amazon S3.</p> <p>Unità: byte</p> <p>Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo, massimo (come p100), qualsiasi percentile tra p0,0 e p99,9</p>
ListRequests	<p>Il numero di richieste HTTP che visualizzano l'elenco del contenuto di un bucket.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
BytesDownloaded	<p>Il numero di byte scaricati per le richieste effettuate a un bucket Amazon S3, in cui la risposta include un corpo.</p> <p>Unità: byte</p> <p>Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo, massimo (come p100), qualsiasi percentile tra p0,0 e p99,9</p>

Metrica	Descrizione
BytesUploaded	<p>Numero di byte caricati per le richieste effettuate su un bucket Amazon S3, in cui la richiesta include un corpo.</p> <p>Unità: byte</p> <p>Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo, massimo (come p100), qualsiasi percentile tra p0,0 e p99,9</p>
4xxErrors	<p>Il numero di richieste con codice di stato di errore client HTTP 4xx effettuate a un bucket Amazon S3 con un valore di 0 o 1. La statistica Average (Media) mostra la frequenza degli errori, mentre la statistica Sum (Somma) mostra il conteggio per un tipo specifico di errore, per ogni periodo.</p> <p>Unità: numero</p> <p>Statistiche valide: media (report per richiesta), somma (report per periodo), minimo, massimo, numero di esempi</p>
5xxErrors	<p>Il numero di richieste con codice di stato di errore del server HTTP 5xx effettuate su un bucket Amazon S3 con valore 0 o 1. La statistica Average (Media) mostra la frequenza degli errori, mentre la statistica Sum (Somma) mostra il conteggio per un tipo specifico di errore, per ogni periodo.</p> <p>Unità: numero</p> <p>Statistiche valide: media (report per richiesta), somma (report per periodo), minimo, massimo, numero di esempi</p>

Metrica	Descrizione
FirstByteLatency	<p>Per ogni richiesta, il tempo dalla ricezione della richiesta completa da parte di un bucket Amazon S3 all'inizio della restituzione della risposta.</p> <p>Unità: millisecondi</p> <p>Statistiche valide: Average (Media), Sum (Somma), Min (Minimo), Max (Massimo) (come p100), Sample Count (Numero di esempi), qualsiasi percentile tra p0,0 e p100</p>
TotalRequestLatency	<p>Per ogni richiesta, il tempo trascorso dalla ricezione del primo byte all'invio dell'ultimo byte a un bucket Amazon S3. Questa metrica include il tempo necessario per ricevere il corpo della richiesta e inviare il corpo della risposta, non incluso in FirstByteLatency.</p> <p>Unità: millisecondi</p> <p>Statistiche valide: Average (Media), Sum (Somma), Min (Minimo), Max (Massimo) (come p100), Sample Count (Numero di esempi), qualsiasi percentile tra p0,0 e p100</p>

Metriche di replica S3 in CloudWatch

Puoi monitorare l'avanzamento della replica con le metriche di replica S3 tramite il tracciamento dei byte in sospeso, delle operazioni in sospeso e della latenza di replica. Per ulteriori informazioni, consulta [Monitoraggio dell'avanzamento con i parametri di replica](#).

Note

Puoi abilitare gli allarmi per le tue metriche di replica in Amazon CloudWatch. Quando configuri gli allarmi per i parametri di replica, imposta il campo Missing data treatment (Trattamento dati persi) su Treat missing data as ignore (maintain the alarm state) (Ignora i dati mancanti (stesso stato allarme)).

Parametro	Description
ReplicationLatency	<p>Il numero massimo di secondi entro il quale la destinazione della replica Regione AWS si trova dietro l'origine Regione AWS per una determinata regola di replica.</p> <p>Unità: secondi</p> <p>Statistiche valide: Max</p>
BytesPendingReplication	<p>Numero totale di byte di oggetti in attesa di replica per una determinata regola di replica.</p> <p>Unità: byte</p> <p>Statistiche valide: Max</p>
OperationsPendingReplication	<p>Numero di operazioni in attesa di replica per una determinata regola di replica.</p> <p>Unità: numero</p> <p>Statistiche valide: Max</p>
OperationsFailedReplication	<p>Numero di operazioni che non sono state replicate per una determinata regola di replica.</p> <p>Unità: numero</p> <p>Statistiche valide: Sum (numero totale di operazioni non riuscite), Average (percentuale di errori), Sample Count (numero totale di operazioni di replica)</p>

Metriche di S3 Storage Lens in CloudWatch

Puoi pubblicare le metriche di utilizzo e attività di S3 Storage Lens su Amazon per CloudWatch creare una visione unificata dello stato operativo nelle dashboard. [CloudWatch](#) Le metriche di S3 Storage Lens vengono pubblicate nel namespace in. `AWS/S3/Storage-Lens` CloudWatch

L'opzione di CloudWatch pubblicazione è disponibile per i dashboard di S3 Storage Lens che sono stati aggiornati con metriche e consigli avanzati.

Per un elenco delle metriche di S3 Storage Lens pubblicate su, consulta. CloudWatch [Glossario dei parametri di Amazon S3 Storage Lens](#) Per un elenco completo delle dimensioni, consulta [Dimensioni](#).

Metriche di richiesta S3 Object Lambda in CloudWatch

S3 Object Lambda include le seguenti metriche di richiesta.

Metrica	Description
AllRequests	<p>Numero totale di richieste HTTP effettuate su un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
GetRequests	<p>Numero totale di richieste HTTP GET effettuate per gli oggetti utilizzando un punto di accesso Lambda per oggetti. Questa metrica non include le operazioni LIST.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
BytesUploaded	<p>Numero totale di byte caricati in un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti, in cui la richiesta include un corpo.</p> <p>Unità: byte</p> <p>Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo, massimo (come p100), qualsiasi percentile tra p0,0 e p99,9</p>
PostRequests	<p>Numero di richieste HTTP POST effettuate in un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti.</p> <p>Unità: numero</p>

Metrica	Description
	Statistiche valide: somma
PutRequests	<p>Numero di richieste HTTP PUT di oggetti effettuate in un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
DeleteRequests	<p>Numero di richieste HTTP DELETE di oggetti effettuate in un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti. Questa metrica include DeleteObjects richieste. Questa metrica mostra il numero di richieste effettuate e non il numero di oggetti eliminati.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
BytesDownloaded	<p>Numero di byte scaricati per le richieste effettuate su un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti, in cui la risposta include un corpo.</p> <p>Unità: byte</p> <p>Statistiche valide: media (byte per richiesta), somma (byte per periodo), numero di esempi, minimo, massimo (come p100), qualsiasi percentile tra p0,0 e p99,9</p>

Metrica	Description
FirstByte Latency	<p>Per ogni richiesta, il tempo dalla ricezione della richiesta completa da parte di un bucket Amazon S3 mediante il punto di accesso Lambda per oggetti all'inizio della restituzione della risposta. Questa metrica dipende dal tempo di esecuzione della funzione AWS Lambda per trasformare l'oggetto prima che la funzione restituisca i byte al punto di accesso Lambda per oggetti.</p> <p>Unità: millisecondi</p> <p>Statistiche valide: Average (Media), Sum (Somma), Min (Minimo), Max (Massimo) (come p100), Sample Count (Numero di esempi), qualsiasi percentile tra p0,0 e p100</p>
TotalRequestLatency	<p>Per ogni richiesta, il tempo trascorso dalla ricezione del primo byte all'invio dell'ultimo byte a un punto di accesso Lambda per oggetti. Questa metrica include il tempo necessario per ricevere il corpo della richiesta e inviare il corpo della risposta, non incluso in FirstByte Latency.</p> <p>Unità: millisecondi</p> <p>Statistiche valide: Average (Media), Sum (Somma), Min (Minimo), Max (Massimo) (come p100), Sample Count (Numero di esempi), qualsiasi percentile tra p0,0 e p100</p>
HeadRequests	<p>Numero di richieste HTTP HEAD effettuate in un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>

Metrica	Description
ListRequests	<p>Numero di richieste HTTP GET che visualizzano l'elenco del contenuto di un bucket Amazon S3. Questa metrica include i byte delle operazioni <code>ListObjects</code> e <code>ListObjectsV2</code>.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
4xxErrors	<p>Il numero di richieste con codice di stato di errore client HTTP 4xx effettuate a un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti con un valore di 0 o 1. La statistica Average (Media) mostra la frequenza degli errori, mentre la statistica Sum (Somma) mostra il conteggio per un tipo specifico di errore, per ogni periodo.</p> <p>Unità: numero</p> <p>Statistiche valide: media (report per richiesta), somma (report per periodo), minimo, massimo, numero di esempi</p>
5xxErrors	<p>Il numero di richieste con codice di stato di errore del server HTTP 5xx effettuate a un bucket Amazon S3 utilizzando un punto di accesso Lambda per oggetti con un valore di 0 o 1. La statistica Average (Media) mostra la frequenza degli errori, mentre la statistica Sum (Somma) mostra il conteggio per un tipo specifico di errore, per ogni periodo.</p> <p>Unità: numero</p> <p>Statistiche valide: media (report per richiesta), somma (report per periodo), minimo, massimo, numero di esempi</p>
ProxiedRequests	<p>Numero di richieste HTTP in un punto di accesso Lambda per oggetti che restituiscono la risposta standard dell'API Amazon S3. Tali richieste non hanno una funzione Lambda configurata.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>

Metrica	Description
InvokedLambda	<p>Numero di richieste HTTP a un oggetto S3 in cui è stata richiamata una funzione Lambda.</p> <p>Unità: numero</p> <p>Statistiche valide: somma</p>
LambdaResponseRequests	Numero totale di richieste <code>WriteGetObjectResponse</code> effettuate dalla funzione Lambda. Questa metrica si applica solo alle richieste <code>GetObject</code> .
LambdaResponse4xx	Il numero di errori HTTP 4xx del client che si verificano quando si chiama <code>WriteGetObjectResponse</code> da una funzione Lambda. Questo parametro fornisce le stesse informazioni di <code>4xxErrors</code> , ma solo per le chiamate <code>WriteGetObjectResponse</code> .
LambdaResponse5xx	Il numero di errori del server HTTP 5xx che si verificano quando si chiama <code>WriteGetObjectResponse</code> da una funzione Lambda. Questo parametro fornisce le stesse informazioni di <code>5xxErrors</code> , ma solo per le chiamate <code>WriteGetObjectResponse</code> .

Dimensioni di Amazon S3 in CloudWatch

Le dimensioni elencate di seguito vengono utilizzate per filtrare i parametri Amazon S3.

Dimensione	Description
BucketName	Questa dimensione filtra i dati richiesti solo per il bucket identificato.
StorageType	<p>Questa dimensione filtra i dati archiviati in un bucket in base ai seguenti tipi di storage:</p> <ul style="list-style-type: none">• <code>DeepArchiveObjectOverhead</code>: per ogni oggetto archiviato, S3 Glacier aggiunge 32 KB di spazio di archiviazione per l'indice e i metadati correlati. Questi dati aggiuntivi

Dimensione	Description
	<p>i sono necessari per identificare e ripristinare l'oggetto desiderato. Questo storage aggiuntivo viene addebitato secondo le tariffe di S3 Glacier Deep Archive.</p> <ul style="list-style-type: none"> • <code>DeepArchiveS3ObjectOverhead</code> : per ogni oggetto archiviato in S3 Glacier Deep Archive, Amazon S3 utilizza 8 KB di spazio di archiviazione per il nome dell'oggetto e gli altri metadati. Questo spazio di archiviazione aggiuntivo viene addebitato secondo le tariffe di S3 Standard. • <code>DeepArchiveStagingStorage</code> - Il numero di byte utilizzati per parti di oggetti di caricamento multipart prima che la richiesta <code>CompleteMultipartUpload</code> sia completata sugli oggetti della classe di storage S3 Glacier Deep Archive. • <code>DeepArchiveStorage</code> : il numero di byte utilizzati per gli oggetti nella classe di archiviazione S3 Glacier Deep Archive. • <code>ExpressOneZoneStorage</code> : numero di byte utilizzati per gli oggetti nella classe di archiviazione S3 Express One Zone. • <code>GlacierInstantRetrievalStorage</code> : il numero di byte utilizzati per gli oggetti nella classe di archiviazione S3 Glacier Instant Retrieval. • <code>GlacierIRSizeOverhead</code> : per gli oggetti di dimensione e inferiore a 128 KB archiviati nella classe di archiviazione S3 Glacier Instant Retrieval, questo tipo di archiviazione rappresenta i byte aggiuntivi addebitati per soddisfare i requisiti di dimensione minima dell'oggetto. • <code>GlacierObjectOverhead</code> : per ogni oggetto archiviato, S3 Glacier aggiunge 32 KB di spazio di archiviazione per l'indice e i metadati correlati. Questi dati aggiuntivi sono necessari per identificare e ripristinare l'oggetto desiderato. Questo spazio di archiviazione aggiuntivo viene addebitato secondo le tariffe di S3 Glacier Flexible Retrieval. • <code>GlacierS3ObjectOverhead</code> : per ogni oggetto archiviato in S3 Glacier Flexible Retrieval, Amazon S3 utilizza 8 KB

Dimensione	Description
	<p>di spazio di archiviazione per il nome dell'oggetto e gli altri metadati. Questo spazio di archiviazione aggiuntivo viene addebitato secondo le tariffe di S3 Standard.</p> <ul style="list-style-type: none"> • <code>GlacierStagingStorage</code> - Il numero di byte utilizzati per parti di oggetti di caricamento multipart prima che la richiesta <code>CompleteMultipartUpload</code> sia completata sugli oggetti della classe di storage Recupero flessibile S3 Glacier. • <code>GlacierStorage</code> : il numero di byte utilizzati per gli oggetti nella classe di archiviazione S3 Glacier Flexible Retrieval. • <code>IntAAObjectOverhead</code> : per ogni oggetto nella classe di archiviazione <code>INTELLIGENT_TIERING</code> nel livello Archive Access (Accesso archiviazione), S3 Glacier aggiunge 32 KB di spazio di archiviazione per l'indice e i metadati correlati. Questi dati aggiuntivi sono necessari per identificare e ripristinare l'oggetto desiderato. Per questa archiviazione aggiuntiva vengono addebitate le tariffe di Recupero flessibile S3 Glacier. • <code>IntAAS3ObjectOverhead</code> : per ogni oggetto nella classe di archiviazione <code>INTELLIGENT_TIERING</code> nel livello Archive Access (Accesso archiviazione), Amazon S3 utilizza 8 KB di spazio di archiviazione per il nome dell'oggetto e altri metadati. Questo spazio di archiviazione aggiuntivo viene addebitato secondo le tariffe di S3 Standard. • <code>IntDAAObjectOverhead</code> : per ogni oggetto nella classe di archiviazione <code>INTELLIGENT_TIERING</code> nel livello Deep Archive Access (Accesso archiviazione profonda), S3 Glacier aggiunge 32 KB di spazio di archiviazione per l'indice e i metadati correlati. Questi dati aggiuntivi sono necessari per identificare e ripristinare l'oggetto desiderato. Questo storage aggiuntivo viene addebitato secondo le tariffe di storage di S3 Glacier Deep Archive. • <code>IntDAAS3ObjectOverhead</code> : per ogni oggetto nella classe di archiviazione <code>INTELLIGENT_TIERING</code> nel livello Deep Archive Access (Accesso archiviazione profonda), Amazon

Dimensione	Description
	<p>S3 aggiunge 8 KB di spazio di archiviazione per l'indice e i metadati correlati. Questi dati aggiuntivi sono necessari per identificare e ripristinare l'oggetto desiderato. Questo spazio di archiviazione aggiuntivo viene addebitato secondo le tariffe di S3 Standard.</p> <ul style="list-style-type: none"> • <code>IntelligentTieringAAStorage</code> : numero di byte utilizzati per gli oggetti nel livello Archive Access (Accesso archiviazione) della classe di archiviazione <code>INTELLIGENT_TIERING</code> . • <code>IntelligentTieringAIAStorage</code> : numero di byte utilizzati per gli oggetti nel livello Archive Instant Access (Accesso di archiviazione immediato) della classe di archiviazione <code>INTELLIGENT_TIERING</code> . • <code>IntelligentTieringDAASStorage</code> : numero di byte utilizzati per gli oggetti nel livello Deep Archive Access (Accesso di archiviazione profonda) della classe di archiviazione <code>INTELLIGENT_TIERING</code> . • <code>IntelligentTieringFAStorage</code> : numero di byte utilizzati per gli oggetti nel livello Frequent Access (Accesso frequente) della classe di archiviazione <code>INTELLIGENT_TIERING</code> . • <code>IntelligentTieringIASStorage</code> : numero di byte utilizzati per gli oggetti nel livello Infrequent Access (Accesso infrequente) della classe di archiviazione <code>INTELLIGENT_TIERING</code> . • <code>OneZoneIASizeOverhead</code> — Per gli oggetti di dimensioni inferiori a 128 KB archiviati nella classe di storage S3 One Zone-Infrequent Access (<code>ONEZONE_IA</code>), questo tipo di storage rappresenta i byte aggiuntivi addebitati per soddisfare i requisiti di dimensione minima degli oggetti. • <code>OneZoneIASStorage</code> — Il numero di byte utilizzati per gli oggetti nella classe di storage S3 One Zone-Infrequent Access (<code>ONEZONE_IA</code>) .

Dimensione	Description
	<ul style="list-style-type: none"> • <code>ReducedRedundancyStorage</code> : il numero di byte utilizzati per gli oggetti nella classe Reduced Redundancy Storage (RRS). • <code>StandardIASizeOverhead</code> : per gli oggetti di dimensioni inferiori a 128 KB archiviati nella classe di archiviazione <code>STANDARD_IA</code>, questo tipo di archiviazione rappresenta i byte aggiuntivi addebitati per soddisfare il requisito di dimensione minima dell'oggetto. • <code>StandardIAStorage</code> — Il numero di byte utilizzati per gli oggetti nella classe di storage S3 Standard-Infrequent Access (<code>STANDARD_IA</code>). • <code>StandardStorage</code> : numero di byte utilizzati per gli oggetti nella classe di archiviazione <code>STANDARD</code>.
<code>FilterId</code>	Questa dimensione filtra le configurazioni delle metriche specificate per le metriche delle richieste in un bucket. Quando crei una configurazione delle metriche, specifichi un ID filtro (ad esempio, un prefisso, un tag o un punto di accesso). Per ulteriori informazioni, consulta la sezione Creazione di una configurazione dei parametri .

Dimensioni di replica S3 in CloudWatch

Le seguenti dimensioni vengono utilizzate per filtrare le metriche di S3 Replication.

Dimensione	Description
<code>SourceBucket</code>	Il nome del bucket da cui vengono replicati gli oggetti.
<code>DestinationBucket</code>	Il nome del bucket in cui vengono replicati gli oggetti.
<code>RuleId</code>	Identificatore univoco della regola che ha attivato l'aggiornamento della metrica di replica.

Dimensioni dell'obiettivo di archiviazione S3 in CloudWatch

Per un elenco delle dimensioni utilizzate per filtrare le metriche di S3 Storage Lens, vedi [CloudWatch Dimensioni](#).

Dimensioni della richiesta S3 Object Lambda in CloudWatch

Le dimensioni riportate di seguito vengono utilizzate per filtrare i dati in un punto di accesso Lambda per oggetti.

Dimensione	Description
AccessPointName	Nome del punto di accesso a cui vengono effettuate le richieste.
DataSourceARN	Origine da cui il punto di accesso Lambda per oggetti sta recuperando i dati. Se la richiesta invoca una funzione Lambda, si riferisce al nome della risorsa Amazon (ARN) Lambda. Altrimenti si riferisce all'ARN del punto di accesso.

Metriche di utilizzo di Amazon S3

Puoi utilizzare le metriche CloudWatch di utilizzo per fornire visibilità sull'utilizzo delle risorse da parte del tuo account. Utilizza queste metriche per visualizzare l'attuale utilizzo del servizio su CloudWatch grafici e dashboard.

Le metriche di utilizzo di Amazon S3 corrispondono alle quote di servizio. AWS È possibile configurare gli allarmi che avvisano quando l'uso si avvicina a una quota di servizio. Per ulteriori informazioni sull' CloudWatchintegrazione con le quote di servizio, consulta le metriche di [AWS utilizzo](#) nella Amazon User Guide. CloudWatch

Amazon S3 pubblica le seguenti metriche nello spazio dei nomi AWS/Usage.

Metrica	Descrizione
ResourceCount	Il numero delle risorse specificate in esecuzione nell'account. Le risorse sono definite dalle dimensioni associate al parametro.

Le seguenti dimensioni sono utilizzate per affinare le metriche di utilizzo pubblicate da Amazon S3.

Dimensione	Description
Service	Il nome del AWS servizio che contiene la risorsa. Per le metriche di utilizzo di Amazon S3, il valore di questa dimensione è S3.
Type	Il tipo di entità che viene segnalato. Attualmente, l'unico valore valido per le metriche di utilizzo di Amazon S3 è Resource.
Resource	Il tipo di risorsa in esecuzione. Attualmente, l'unico valore valido per le metriche di utilizzo di Amazon S3 è GeneralPurposeBuckets , che restituisce il numero di bucket per uso generico in un Account AWS. I bucket per uso generico consentono di archiviare oggetti in tutte le classi di storage, ad eccezione di S3 Express One Zone.

Accesso alle CloudWatch metriche

È possibile utilizzare le seguenti procedure per visualizzare le metriche di archiviazione per Amazon S3. Per includere i parametri di Amazon S3, è necessario impostare un timestamp di inizio e uno di fine. Per i parametri relativi a un periodo specifico di 24 ore, impostare il periodo di tempo su 86400 secondi, ovvero il numero di secondi in un giorno. Ricordare anche di impostare le dimensioni BucketName e StorageType.

Utilizzo di AWS CLI

Ad esempio, se desideri utilizzare il per AWS CLI ottenere la media della dimensione di un bucket specifico in byte, puoi usare il seguente comando:

```
aws cloudwatch get-metric-statistics --metric-name BucketSizeBytes --namespace AWS/S3
--start-time 2016-10-19T00:00:00Z --end-time 2016-10-20T00:00:00Z --statistics Average
--unit Bytes --region us-west-2 --dimensions Name=BucketName,Value=amzn-s3-demo-bucket
Name=StorageType,Value=StandardStorage --period 86400 --output json
```

Questo esempio produce il seguente output.

```
{
  "Datapoints": [
    {
```



```
        "Timestamp": "2016-10-19T00:00:00Z",
        "Average": 1025328.0,
        "Unit": "Bytes"
    }
],
"Label": "BucketSizeBytes"
}
```

Utilizzo della console S3

Per visualizzare le metriche utilizzando la console Amazon CloudWatch

1. Apri la CloudWatch console all'indirizzo. <https://console.aws.amazon.com/cloudwatch/>
2. Nel pannello di navigazione a sinistra scegli Metrics (Parametri).
3. Scegliere il namespace S3.
4. (Facoltativo) Per visualizzare un parametro, immettere il nome parametro nella casella di ricerca.
5. (Facoltativo) Per filtrare in base alla `StorageType` dimensione, inserisci il nome della classe di archiviazione nella casella di ricerca.

Per visualizzare un elenco di metriche valide archiviate per il tuo Account AWS utilizzando il AWS CLI

- Al prompt dei comandi utilizza il comando seguente.

```
aws cloudwatch list-metrics --namespace "AWS/S3"
```

Per ulteriori informazioni sulle autorizzazioni richieste per accedere alle CloudWatch dashboard, consulta le autorizzazioni delle CloudWatch dashboard di [Amazon](#) nella Amazon CloudWatch User Guide.

CloudWatch configurazioni delle metriche

Con Amazon CloudWatch Request Metrics per Amazon S3, puoi ricevere parametri in 1 minuto, impostare CloudWatch allarmi e accedere a CloudWatch dashboard per CloudWatch visualizzare le operazioni e le prestazioni quasi in tempo reale del tuo storage Amazon S3. Per le applicazioni che dipendono dallo storage nel cloud, questi parametri consentono di identificare rapidamente i problemi operativi e intraprendere le azioni appropriate. Quando sono abilitati, questi parametri da 1 minuto sono disponibili a livello di bucket Amazon S3 per default.

Se desideri ottenere le metriche delle CloudWatch richieste per gli oggetti in un bucket, devi creare una configurazione delle metriche per il bucket. Per ulteriori informazioni, consulta [Creazione di una configurazione CloudWatch delle metriche per tutti gli oggetti nel bucket](#).

Puoi anche definire un filtro per i parametri raccolti usando un prefisso condiviso, tag di oggetto o un punto di accesso. Questo metodo di definizione di un filtro consente di allineare i filtri dei parametri a determinati flussi di lavoro, applicazioni business o organizzazioni interne. Per ulteriori informazioni, consulta [Creazione di una configurazione dei parametri che filtra in base al prefisso, al tag oggetto o al punto di accesso](#). Per ulteriori informazioni sui parametri di CloudWatch disponibili e sulle differenze tra parametri di storage e di richiesta, consulta [Metriche di monitoraggio con Amazon CloudWatch](#).

Quando si usano le configurazioni dei parametri, tenere presente quanto indicato di seguito:

- È possibile definire un massimo di 1.000 configurazioni dei parametri per ciascun bucket.
- È possibile scegliere quali oggetti di un bucket includere nelle configurazioni dei parametri utilizzando i filtri. L'applicazione di un filtro utilizzando un prefisso condiviso, un tag di oggetto o un punto di accesso consente di allineare i filtri dei parametri a determinati flussi di lavoro, applicazioni business o organizzazioni interne. Per richiedere i parametri per l'intero bucket, creare una configurazione di parametro senza filtri.
- Le configurazioni delle metriche sono necessarie solo per abilitare le metriche delle richieste. Bucket-level le metriche di archiviazione giornaliere sono sempre attive e vengono fornite senza costi aggiuntivi. Attualmente, non è possibile ottenere parametri di storage giornalieri per un sottoinsieme filtrato di oggetti.
- Ogni configurazione delle metriche abilita il set completo di metriche di richiesta [disponibili](#). Operation-specific le metriche (ad esempio `PostRequests`) vengono segnalate solo se sono presenti richieste di quel tipo per il bucket o il filtro.
- I parametri della richiesta vengono indicati per le operazioni a livello di oggetto. Vengono indicati anche per le operazioni che elencano i contenuti del bucket, come [GET Bucket \(List Objects\) \(Elenca oggetti GET Bucket\)](#), [GET Bucket Object Versions \(Versioni dell'oggetto GET Bucket\)](#) e [List Multipart Uploads \(Elenca caricamenti in più parti\)](#), ma non vengono indicati per altre operazioni sui bucket.
- I parametri di richiesta supportano i filtri in base al prefisso, al tag oggetto o al punto di accesso, diversamente dai parametri di storage.

Best-effort CloudWatch consegna delle metriche

CloudWatch le metriche vengono fornite con il massimo impegno possibile. La maggior parte delle richieste per un oggetto Amazon S3 con metriche di richiesta comportano l'invio di un punto dati a CloudWatch.

La completezza e la tempestività dei parametri non è garantita. È possibile che il data point per una richiesta specifica venga restituito con un timestamp successivo a quello del momento effettivo di elaborazione della richiesta. Il data point potrebbe subire un ritardo di un minuto prima di essere disponibile oppure potrebbe non essere consegnato affatto. CloudWatch le metriche relative alle richieste ti danno un'idea della natura del traffico diretto verso il tuo bucket in tempo quasi reale, ma non intendono essere un resoconto completo di tutte le richieste.

Dalla natura best-effort di questa funzione deriva che i report disponibili nella [dashboard di gestione dei costi e della fatturazione](#) potrebbero includere una o più richieste di accesso che non compaiono nelle metriche del bucket.

Per ulteriori informazioni sull'utilizzo delle CloudWatch metriche in Amazon S3, consulta i seguenti argomenti.

Argomenti

- [Creazione di una configurazione CloudWatch delle metriche per tutti gli oggetti nel bucket](#)
- [Creazione di una configurazione dei parametri che filtra in base al prefisso, al tag oggetto o al punto di accesso](#)
- [Eliminazione di un filtro dei parametri](#)

Creazione di una configurazione CloudWatch delle metriche per tutti gli oggetti nel bucket

Quando configuri le metriche delle richieste, puoi creare una configurazione CloudWatch delle metriche per tutti gli oggetti del bucket oppure puoi filtrare per prefisso, tag dell'oggetto o punto di accesso. Nelle procedure descritte in questo argomento viene illustrato come creare una configurazione per tutti gli oggetti nel bucket. Per creare una configurazione che filtri in base al tag oggetto, al prefisso o al punto di accesso, consulta [Creazione di una configurazione dei parametri che filtra in base al prefisso, al tag oggetto o al punto di accesso](#).

Esistono tre tipi di metriche Amazon per Amazon S3: CloudWatch metriche di storage, metriche di richiesta e metriche di replica. I parametri di storage vengono indicati una volta al giorno e sono disponibili per tutti i clienti senza costi aggiuntivi. I parametri di richiesta sono disponibili a intervalli di 1 minuto dopo una determinata latenza per l'elaborazione. Le metriche delle richieste vengono

fatturate alla tariffa standard. CloudWatch È necessario acconsentire esplicitamente ai parametri di richiesta configurandoli nella console o utilizzando l'API Amazon S3. Le [metriche di replica S3](#) forniscono metriche dettagliate per le regole nella configurazione di replica. Con le metriche di replica, puoi monitorare l'avanzamento della replica minuto per minuto controllando i byte in attesa di replica, le operazioni in attesa di replica, le operazioni con replica non riuscita e la latenza di replica.

Per ulteriori informazioni sulle CloudWatch metriche per Amazon S3, consulta [Metriche di monitoraggio con Amazon CloudWatch](#)

Puoi aggiungere configurazioni dei parametri a un bucket utilizzando la console di Amazon S3, la AWS Command Line Interface (AWS CLI) o REST API di Amazon S3.

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket seleziona il nome del bucket contenente gli oggetti di cui desideri ottenere i parametri.
4. Seleziona la scheda Parametri.
5. In Bucket metrics (Parametri bucket) scegli View additional charts (Visualizza grafici aggiuntivi).
6. Scegli la scheda Request metrics (Parametri di richiesta).
7. Scegli Create Filter (Crea filtro).
8. Nella casella Filter name (Nome filtro) immettere il nome del filtro.

I nomi possono contenere solo lettere, numeri, punti, trattini e caratteri di sottolineatura. Si consiglia di utilizzare il nome EntireBucket per un filtro che si applica a tutti gli oggetti.

9. In Filter scope (Ambito del filtro) seleziona This filter applies to all objects in the bucket (Questo filtro si applica a tutti gli oggetti del bucket).

È anche possibile definire un filtro in modo che i parametri vengano acquisiti e indicati solo per un sottoinsieme di oggetti del bucket. Per ulteriori informazioni, consulta [Creazione di una configurazione dei parametri che filtra in base al prefisso, al tag oggetto o al punto di accesso](#).

10. Scegli Salva modifiche.
11. Nella scheda Request metrics (Parametri di richiesta), in Filters (Filtri), scegliere il filtro appena creato.

Dopo circa 15 minuti, CloudWatch inizia a tracciare queste metriche di richiesta. Puoi visualizzarli nella scheda Request metrics (Parametri di richiesta) . Puoi visualizzare i grafici delle metriche su Amazon S3 o sulla console. CloudWatch Le metriche delle richieste vengono fatturate alla tariffa standard. CloudWatch Per ulteriori informazioni, consulta i prezzi di [Amazon CloudWatch](#) .

Utilizzo della REST API

È anche possibile aggiungere configurazioni di parametri in modo programmatico con REST API di Amazon S3. Per ulteriori informazioni sull'aggiunta e sull'utilizzo delle configurazioni dei parametri, consulta i seguenti argomenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [Configurazione del parametro PUT Bucket](#)
- [Configurazione del parametro GET Bucket](#)
- [Configurazione del parametro LIST Bucket](#)
- [Configurazione del parametro DELETE Bucket](#)

Utilizzo di AWS CLI

1. Installa e configura il AWS CLI. Per le istruzioni, consulta [Installazione, aggiornamento e disinstallazione della AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface .
2. Aprire un terminale.
3. Eseguire il comando riportato di seguito per aggiungere una configurazione di parametro.

```
aws s3api put-bucket-metrics-configuration --endpoint https://s3.us-west-2.amazonaws.com --bucket bucket-name --id metrics-config-id --metrics-configuration '{"Id": "metrics-config-id"}'
```

Creazione di una configurazione dei parametri che filtra in base al prefisso, al tag oggetto o al punto di accesso

Esistono tre tipi di CloudWatch metriche Amazon per Amazon S3: metriche di storage, metriche di richiesta e metriche di replica. I parametri di storage vengono indicati una volta al giorno e sono disponibili per tutti i clienti senza costi aggiuntivi. I parametri di richiesta sono disponibili a intervalli di 1 minuto dopo una determinata latenza per l'elaborazione. Le metriche delle richieste vengono

fatturate alla tariffa standard. CloudWatch È necessario acconsentire esplicitamente ai parametri di richiesta configurandoli nella console o utilizzando l'API Amazon S3. Le [metriche di replica S3](#) forniscono metriche dettagliate per le regole nella configurazione di replica. Con le metriche di replica, puoi monitorare l'avanzamento della replica minuto per minuto controllando i byte in attesa di replica, le operazioni in attesa di replica, le operazioni con replica non riuscita e la latenza di replica.

Per ulteriori informazioni sulle CloudWatch metriche per Amazon S3, consulta [Metriche di monitoraggio con Amazon CloudWatch](#)

Quando configuri le CloudWatch metriche, puoi creare un filtro per tutti gli oggetti del bucket oppure puoi filtrare la configurazione in gruppi di oggetti correlati all'interno di un singolo bucket. Puoi filtrare gli oggetti in un bucket da includere in una configurazione di parametro in base a uno o più dei tipi di filtro elencati di seguito.

- Prefisso del nome della chiave dell'oggetto: sebbene il modello di dati Amazon S3 abbia una struttura orizzontale, è possibile applicare una gerarchia utilizzando un prefisso. La console di Amazon S3 supporta questi prefissi con il concetto di cartelle. Se si applica un filtro basato sul prefisso, gli oggetti con lo stesso prefisso verranno inclusi nella configurazione del parametro. Per ulteriori informazioni sui prefissi, consulta [Organizzazione degli oggetti utilizzando i prefissi](#).
- Tag - È possibile aggiungere tag, che sono coppie di nomi chiave-valore, agli oggetti. I tag consentono di trovare e organizzare gli oggetti in modo semplice. È possibile utilizzare i tag anche come filtri per le configurazioni dei parametri. Per ulteriori informazioni sui tag degli oggetti, consulta [Etichettare i tuoi oggetti](#).
- Punto di accesso: i punti di accesso S3 sono endpoint di rete denominati e allegati a bucket che semplificano la gestione degli accessi ai dati su vasta scala per set di dati condivisi in S3. Quando crei un filtro in base al punto di accesso, Amazon S3 include le richieste al punto di accesso specificato nella configurazione dei parametri. Per ulteriori informazioni, consulta [Monitoraggio e registrazione degli access point](#).

Note

Quando crei una configurazione di parametri che filtra in base al punto di accesso, devi utilizzare l'Amazon Resource Name (ARN) del punto di accesso e non l'alias del punto di accesso. Assicurati di utilizzare l'ARN del punto di accesso e non l'ARN di un oggetto specifico. Per ulteriori informazioni sugli ARN dei punti di accesso, consulta la sezione [Utilizzo dei punti di accesso Amazon S3 per bucket per uso generico](#).

Se si specifica un filtro, solo le richieste che agiscono su oggetti singoli possono corrispondere al filtro ed essere incluse nei parametri dichiarati. Richieste come [DeleteObjects](#) e `ListObjects` non restituiscono alcuna metrica per le configurazioni con filtri.

Per richiedere un'applicazione più complessa di filtri, scegliere due o più elementi. Nella configurazione del parametro verranno inclusi solo gli oggetti con tutti questi elementi. Se non si impostano i filtri, tutti gli oggetti nel bucket vengono inclusi nella configurazione del parametro.

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Bucket per uso generico.
3. Nell'elenco dei bucket seleziona il nome del bucket contenente gli oggetti di cui desideri ottenere i parametri.
4. Seleziona la scheda Parametri.
5. In Bucket metrics (Parametri bucket) scegli View additional charts (Visualizza grafici aggiuntivi).
6. Scegli la scheda Request metrics (Parametri di richiesta).
7. Scegli Create Filter (Crea filtro).
8. Nella casella Filter name (Nome filtro) immettere il nome del filtro.

I nomi possono contenere solo lettere, numeri, punti, trattini e caratteri di sottolineatura.

9. In Filter scope (Ambito del filtro), scegli Limit the scope of this filter using a prefix, object tags, and an S3 Access Point, or a combination of all three (Limita l'ambito di questo filtro utilizzando un prefisso, tag oggetto e un punto di accesso S3 o una combinazione dei tre).
10. In Filter type (Tipo di filtro), scegli almeno un tipo di filtro: Prefix (Prefisso), Object tags (Tag oggetto) oppure Access point (Punto di accesso).
11. Nella casella Prefix (Prefisso) inserisci un prefisso per definire un filtro in base al prefisso e limitare l'ambito del filtro a un singolo percorso.
12. Per definire un filtro in base ai tag oggetto, in Object tags (Tag oggetto), scegli Add tag (Aggiungi tag), quindi inserisci un tag Key (Chiave) e Value (Valore).
13. Per definire un filtro in base al punto di accesso, nel campo S3 Access point (Punto di accesso S3), inserisci l'ARN del punto di accesso o scegli Browse S3 (Sfoggia S3) per passare al punto di accesso.

⚠ Important

Non puoi inserire l'alias del punto di accesso. Devi inserire l'ARN del punto di accesso stesso e non l'ARN di un oggetto specifico.

14. Scegli Save changes (Salva modifiche).

Amazon S3 crea un filtro che utilizza il prefisso, i tag o il punto di accesso specificati.

15. Nella scheda Request metrics (Parametri di richiesta), in Filters (Filtri), scegliere il filtro appena creato.

Hai creato un filtro che limita l'ambito dei parametri di richiesta in base al prefisso, ai tag oggetto o al punto di accesso. Circa 15 minuti dopo l'inizio del monitoraggio di queste metriche delle richieste, puoi visualizzare i grafici delle metriche sia su Amazon S3 che sulle console. CloudWatch Le metriche delle richieste vengono fatturate alla tariffa standard. CloudWatch Per ulteriori informazioni, consulta i prezzi di [Amazon CloudWatch](#).

È anche possibile richiedere i parametri a livello di bucket. Per informazioni, consulta [Creazione di una configurazione CloudWatch delle metriche per tutti gli oggetti nel bucket](#).

Utilizzo di AWS CLI

1. Installa e configura il AWS CLI. Per le istruzioni, consulta [Installazione, aggiornamento e disinstallazione della AWS CLI](#) nella Guida per l'utente di AWS Command Line Interface.
2. Aprire un terminale.
3. Esegui uno dei comandi riportati di seguito per aggiungere una configurazione di parametri.

Example: per filtrare in base al prefisso

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --  
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":  
{"Prefix":"prefix1"}} '
```


Example: per filtrare in base ai tag

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"Tag": {"Key": "string", "Value": "string"}} '
```

Example: per filtrare in base al punto di accesso

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"AccessPointArn":"arn:aws:s3:Region:account-id:accesspoint/access-point-name"}} '
```

Example: per filtrare in base al prefisso, ai tag e al punto di accesso

```
aws s3api put-bucket-metrics-configuration --endpoint https://
s3.Region.amazonaws.com --bucket amzn-s3-demo-bucket --id metrics-config-id --
metrics-configuration '
{
  "Id": "metrics-config-id",
  "Filter": {
    "And": {
      "Prefix": "string",
      "Tags": [
        {
          "Key": "string",
          "Value": "string"
        }
      ],
      "AccessPointArn": "arn:aws:s3:Region:account-id:accesspoint/access-
point-name"
    }
  }
}'
```

Utilizzo della REST API

È anche possibile aggiungere configurazioni di parametri in modo programmatico con REST API di Amazon S3. Per ulteriori informazioni sull'aggiunta e sull'utilizzo delle configurazioni dei parametri,

consulta i seguenti argomenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [Configurazione del parametro PUT Bucket](#)
- [Configurazione del parametro GET Bucket](#)
- [Configurazione del parametro LIST Bucket](#)
- [Configurazione del parametro DELETE Bucket](#)

Eliminazione di un filtro dei parametri

Puoi eliminare un filtro delle metriche delle CloudWatch richieste Amazon se non ti serve più. Quando elimini un filtro, non ti vengono più addebitati i costi per le metriche delle richieste che utilizzano quel filtro specifico. Tuttavia, gli addebiti si applicano comunque per tutti gli altri filtri rimasti.

Non è possibile annullare l'eliminazione di un filtro. Dopo aver eliminato un filtro, non puoi più utilizzarlo per le metriche delle richieste.

Per creare un filtro per le metriche delle richieste, consulta i seguenti argomenti:

- [Creazione di una configurazione CloudWatch delle metriche per tutti gli oggetti nel bucket](#)
- [Creazione di una configurazione dei parametri che filtra in base al prefisso, al tag oggetto o al punto di accesso](#)

Utilizzo della console S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket per il quale desideri eliminare un filtro delle metriche di richiesta.
4. Seleziona la scheda Parametri.
5. In Bucket metrics (Parametri bucket) scegli View additional charts (Visualizza grafici aggiuntivi).
6. Scegliere la scheda Request metrics (Parametri di richiesta).
7. Scegliere Manage filters (Gestisci filtri).
8. Scegliere il filtro.

 Important

L'eliminazione di un filtro non può essere annullata.

9. Scegliere Delete (Elimina).

Amazon S3 elimina il filtro.

Utilizzo di REST API

È anche possibile aggiungere configurazioni di parametri in modo programmatico con REST API di Amazon S3. Per ulteriori informazioni sull'aggiunta e sull'utilizzo delle configurazioni dei parametri, consulta i seguenti argomenti nella Documentazione di riferimento delle API di Amazon Simple Storage Service:

- [Configurazione del parametro PUT Bucket](#)
- [Configurazione del parametro GET Bucket](#)
- [Configurazione del parametro LIST Bucket](#)
- [Configurazione del parametro DELETE Bucket](#)

Notifiche di eventi Amazon S3

Puoi utilizzare la funzionalità Notifiche di eventi Amazon S3 per ricevere le notifiche relative a quando si verificano determinati eventi nel bucket S3. Per abilitare le notifiche, aggiungi una configurazione di notifica che identifichi gli eventi che Amazon S3 deve pubblicare. Assicurati inoltre che identifichi le destinazioni a cui Amazon S3 deve inviare le notifiche. Questa configurazione viene archiviata nella risorsa secondaria notifica associata a un bucket. Per ulteriori informazioni, consulta [Opzioni di configurazione dei bucket per uso generico](#). Amazon S3 fornisce un'API per la gestione di questa risorsa secondaria.

 Important

Le notifiche degli eventi di Amazon S3 sono progettate per essere distribuite almeno una volta. Le notifiche di eventi in genere vengono distribuite in pochi secondi, ma a volte può essere necessario un minuto o più.

Panoramica delle notifiche eventi di Amazon S3.

Attualmente, Amazon S3 può pubblicare notifiche per i seguenti eventi:

- Eventi di creazione nuovo oggetto
- Eventi di rimozione di oggetti
- Eventi di ripristino di oggetti
- Un evento di perdita oggetto Reduced Redundancy Storage (RRS)
- Eventi di replica
- Eventi di scadenza del ciclo di vita S3
- Eventi di transizione del ciclo di vita S3
- Eventi di archiviazione Intelligent-Tiering automatica S3
- Eventi di assegnazione di tag agli oggetti
- Eventi di ACL PUT di oggetto
- Eventi di annotazione degli oggetti

Per una descrizione completa dei tipi di evento, consulta [Tipi di eventi supportati per SQS, SNS e Lambda](#).

Amazon S3 può inviare messaggi di notifica degli eventi alle seguenti destinazioni. Il valore dell'Amazon Resource Name (ARN) di queste destinazioni viene specificato nella configurazione della notifica.

- Argomenti su Amazon Simple Notification Service (Amazon SNS)
- Code di Amazon Simple Queue Service (Amazon SQS)
- AWS Lambda funzione
- Amazon EventBridge

Per ulteriori informazioni, consulta [Destinazioni eventi supportate](#).

Note

Le code FIFO (First-In-First-Out) di Amazon Simple Queue Service non sono supportate come destinazione di notifica degli eventi di Amazon S3. Per inviare una notifica per un

evento Amazon S3 a una coda FIFO di Amazon SQS, puoi utilizzare Amazon EventBridge. Per ulteriori informazioni, consulta [Abilitare Amazon EventBridge](#).

Note

AWS Lambda le funzioni durevoli non sono supportate come destinazione di notifica degli eventi di Amazon S3.

Warning

Se la notifica scrive nello stesso bucket che attiva la notifica, potrebbe causare un loop di esecuzione. Ad esempio, se il bucket attiva una funzione Lambda ogni volta che un oggetto viene caricato e la funzione carica un oggetto nel bucket, allora la funzione indirettamente lo attiva. Per evitare questo, utilizzare due bucket, oppure configurare il trigger in modo che venga applicato solo a un prefisso utilizzato per gli oggetti in entrata.

Per ulteriori informazioni e un esempio di utilizzo delle notifiche Amazon S3 con AWS Lambda, consulta [Using AWS Lambda with Amazon S3](#) nella Developer Guide. AWS Lambda

Per ulteriori informazioni sul numero di configurazioni di notifica degli eventi che è possibile creare per bucket, consulta [Quote di servizio Amazon S3](#) in Riferimenti generali di AWS .

Per ulteriori informazioni sulle notifiche degli eventi, consulta le sezioni seguenti.

Argomenti

- [Tipi di notifiche eventi e destinazioni](#)
- [Utilizzo di Amazon SQS, Amazon SNS e Lambda](#)
- [Usando EventBridge](#)

Tipi di notifiche eventi e destinazioni

Amazon S3 supporta diversi tipi di notifiche di eventi e destinazioni in cui è possibile pubblicare le notifiche. Puoi specificare il tipo di evento e la destinazione durante la configurazione delle notifiche.

degli eventi. È possibile specificare una sola destinazione per ogni notifica di evento. Le notifiche degli eventi di Amazon S3 inviano una voce di evento per ogni messaggio di notifica.

Argomenti

- [Destinazioni eventi supportate](#)
- [Tipi di eventi supportati per SQS, SNS e Lambda](#)
- [Tipi di eventi supportati per Amazon EventBridge](#)
- [Ordinamento degli eventi e duplicazione degli eventi](#)

Destinazioni eventi supportate

Amazon S3 può inviare messaggi di notifica degli eventi alle seguenti destinazioni.

- Argomenti su Amazon Simple Notification Service (Amazon SNS)
- Code di Amazon Simple Queue Service (Amazon SQS)
- AWS Lambda
- Amazon EventBridge

Tuttavia, è possibile specificare un solo tipo di destinazione per ogni notifica di evento.

Note

È necessario concedere ad Amazon S3; le autorizzazioni per pubblicare i messaggi in un argomento Amazon SNS o in una coda Amazon SQS. Devi inoltre concedere ad Amazon S3 l'autorizzazione a richiamare una AWS Lambda funzione per tuo conto. Per istruzioni su come concedere queste autorizzazioni, consulta [Concessione di autorizzazioni per pubblicare messaggi di notifica eventi in una destinazione](#).

Argomento Amazon SNS

Amazon SNS è un servizio di messaggistica push completamente gestito e flessibile. Tramite questo servizio, è possibile inviare messaggi push a dispositivi mobili o servizi distribuiti. Con SNS puoi pubblicare un messaggio e inviarlo una o più volte. Al momento, l'SNS standard è consentito solo come destinazione di notifica di eventi S3, mentre l'SNS FIFO non è consentito.

Amazon SNS coordina e gestisce la consegna o l'invio di messaggi agli endpoint o ai client abbonati. È possibile utilizzare la console Amazon SNS per creare un argomento Amazon SNS a cui inviare le notifiche.

L'argomento deve essere nello Regione AWS stesso bucket Amazon S3. Per informazioni sulla creazione di un argomento Amazon SNS, consulta [Nozioni di base](#) nella Guida per sviluppatori di Amazon Simple Notification Service e [Domande frequenti su Amazon SNS](#).

Per poter utilizzare l'argomento Amazon SNS creato come destinazione della notifica di eventi, è necessario disporre di quanto segue:

- L'Amazon Resource Name (ARN) per l'argomento Amazon SNS
- Un'iscrizione valida a un argomento di Amazon SNS. Con esso, gli iscritti agli argomenti vengono informati quando un messaggio viene pubblicato sul tuo argomento Amazon SNS.

Coda Amazon SQS

Amazon SQS offre code ospitate affidabili e scalabili per lo storage dei messaggi mentre transitano tra computer. Tramite Amazon SQS è possibile trasmettere qualsiasi volume di dati senza richiedere la disponibilità costante di altri servizi. È possibile utilizzare la console Amazon SQS per creare una coda Amazon SQS a cui inviare le notifiche.

La coda Amazon SQS deve essere nella stessa Regione AWS del bucket Amazon S3. Per informazioni sulla creazione di una coda di Amazon SQS, consulta [Cos'è Amazon Simple Queue Service?](#) e [Nozioni di base su Amazon SQS](#) nella Guida per sviluppatori di Amazon Simple Queue Service.

Per poter utilizzare la coda Amazon SQS come destinazione della notifica eventi, devi disporre di quanto segue:

- L'Amazon Resource Name (ARN) per la coda di Amazon SQS

Note

Le code FIFO (First-In-First-Out) di Amazon Simple Queue Service non sono supportate come destinazione di notifica degli eventi di Amazon S3. Per inviare una notifica per un evento Amazon S3 a una coda FIFO di Amazon SQS, puoi utilizzare Amazon EventBridge. Per ulteriori informazioni, consulta [Abilitare Amazon EventBridge](#).

Dimensioni del messaggio Amazon SQS

I messaggi di notifica degli eventi di Amazon S3 possono pesare fino a 64 KB. Ti consigliamo di impostare l'`MaximumMessageSize` attributo della coda su almeno 64 KB. Se la notifica di un evento supera la coda configurata `MaximumMessageSize`, Amazon SQS rifiuta la notifica e non consegna l'evento.

funzione Lambda

Puoi utilizzarlo AWS Lambda per estendere altri AWS servizi con logica personalizzata o creare un backend personalizzato che funzioni su AWS scala, prestazioni e sicurezza. Con Lambda, è possibile creare applicazioni separate e basate su eventi che vengono eseguite solo quando necessario. È inoltre possibile utilizzarlo per dimensionare automaticamente queste applicazioni da poche richieste al giorno a migliaia al secondo.

Lambda esegue codice personalizzato in risposta agli eventi dei bucket Amazon S3. Il codice personalizzato viene caricato su Lambda e quindi viene creata quella che si chiama funzione Lambda. Quando Amazon S3 rileva un evento di un tipo specifico, può pubblicare l'evento AWS Lambda e richiamare la tua funzione in Lambda. In risposta, Lambda esegue la tua funzione. Un tipo di evento che potrebbe rilevare, ad esempio, è un evento di creazione oggetto.

Puoi utilizzare la AWS Lambda console per creare una funzione Lambda che utilizza l'AWS infrastruttura per eseguire il codice per tuo conto. La funzione Lambda deve trovarsi nella stessa regione del bucket S3. Per impostare la funzione Lambda come destinazione di notifica eventi, è inoltre necessario disporre del nome o dell'ARN di una funzione Lambda.

Warning

Se la notifica scrive nello stesso bucket che attiva la notifica, potrebbe causare un loop di esecuzione. Ad esempio, se il bucket attiva una funzione Lambda ogni volta che un oggetto viene caricato e la funzione carica un oggetto nel bucket, allora la funzione indirettamente lo attiva. Per evitare questo, utilizzare due bucket, oppure configurare il trigger in modo che venga applicato solo a un prefisso utilizzato per gli oggetti in entrata.

Per ulteriori informazioni e un esempio di utilizzo delle notifiche Amazon S3 con AWS Lambda, consulta [Using AWS Lambda with Amazon S3](#) nella Developer Guide. AWS Lambda

Amazon EventBridge

Amazon EventBridge è un bus di eventi serverless, che riceve eventi dai AWS servizi. Puoi impostare regole per abbinare gli eventi e distribuirli ai target, come ad esempio un servizio AWS o un endpoint HTTP. Per ulteriori informazioni, consulta [What is EventBridge](#) in the Amazon EventBridge User Guide.

A differenza di altre destinazioni, puoi abilitare o disabilitare gli eventi a cui inviare EventBridge un bucket. Se abiliti la consegna, tutti gli eventi vengono inviati a EventBridge. Inoltre, puoi utilizzare EventBridge le regole per indirizzare gli eventi verso obiettivi aggiuntivi.

Tipi di eventi supportati per SQS, SNS e Lambda

Amazon S3 pubblica i tipi di eventi riportati di seguito. Questi tipi di eventi devono essere specificati nella configurazione delle notifiche.

Tipi di eventi	Description
<code>s3:TestEvent</code>	Quando una notifica è abilitata, Amazon S3 pubblica una notifica di prova. Questo serve a garantire che l'argomento esista e che il proprietario del bucket abbia l'autorizzazione a pubblicare l'argomento specificato. Se l'attivazione della notifica ha esito negativo, non verrà ricevuta alcuna notifica di prova.
<code>s3:ObjectCreated:*</code> <code>s3:ObjectCreated:Put</code> <code>s3:ObjectCreated:Post</code> <code>s3:ObjectCreated:Copy</code> <code>s3:ObjectCreated:CompleteMultipartUpload</code>	Le operazioni API di Amazon S3, come PUT, POST e COPY, possono creare un oggetto. Con questi tipi di eventi, puoi abilitare le notifiche quando un oggetto viene creato tramite un'API specifica. In alternativa, puoi utilizzare il tipo di evento <code>s3:ObjectCreated:*</code> per richiedere la notifica indipendentemente dall'API utilizzata per creare un oggetto. <code>s3:ObjectCreated:CompleteMultipartUpload</code> include gli oggetti creati con UploadPartCopy per le operazioni di copia.
<code>s3:ObjectRemoved:*</code> <code>s3:ObjectRemoved:Delete</code>	Utilizzando i tipi di evento <code>ObjectRemoved</code> , è possibile attivare la notifica quando un oggetto o un gruppo di oggetti viene rimosso da un bucket.

Tipi di eventi	Description
<p><code>s3:ObjectRemoved:DeleteMarkerCreated</code></p>	<p>È possibile richiedere una notifica quando viene eliminato un oggetto o quando viene eliminato in modo permanent e un oggetto con versione utilizzando il tipo di evento <code>s3:ObjectRemoved:Delete</code> . In alternativa, è possibile richiedere una notifica quando viene creato un contrassegno di eliminazione per un oggetto con versione utilizzando <code>s3:ObjectRemoved:DeleteMarkerCreated</code> . Per istruzioni su come eliminare gli oggetti con versione, consulta Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata . Inoltre, è possibile utilizzare un carattere jolly <code>s3:ObjectRemoved:*</code> per richiedere la notifica ogni volta che viene eliminato un oggetto.</p> <p>Queste notifiche di eventi non provvedono alcun avviso per le eliminazioni automatiche dalle configurazioni del ciclo di vita o dalle operazioni che hanno avuto esito negativo.</p>
<p><code>s3:ObjectRestore:*</code></p> <p><code>s3:ObjectRestore:Post</code></p> <p><code>s3:ObjectRestore:Completed</code></p> <p><code>s3:ObjectRestore:Delete</code></p>	<p>Utilizzando i tipi di <code>ObjectRestore</code> evento, è possibile ricevere notifiche per l'avvio e il completamento degli eventi durante il ripristino di oggetti dalla classe di storage S3 Glacier Flexible Retrieval, dalla classe di storage S3 Glacier Deep Archive, dal livello S3 Archive Access e dal livello S3 Deep Intelligent-Tiering Archive Access. Intelligent-Tiering</p> <p>È inoltre possibile ricevere notifiche per la scadenza della copia ripristinata di un oggetto.</p> <p>Il tipo di evento <code>s3:ObjectRestore:Post</code> notifica l'avvio del ripristino degli oggetti. Il tipo di evento <code>s3:ObjectRestore:Completed</code> notifica il completamento del ripristino. Il tipo di evento <code>s3:ObjectRestore:Delete</code> notifica la scadenza della copia temporanea di un oggetto ripristinato.</p>

Tipi di eventi	Description
s3:ReducedRedundancyLostObject	Puoi ricevere questo evento di notifica quando Amazon S3 rileva che un oggetto della classe di archiviazione RRS è andato perso.
s3:Replication:* s3:Replication:OperationFailedReplication s3:Replication:OperationMissedThreshold s3:Replication:OperationReplicatedAfterThreshold s3:Replication:OperationNotTracked	<p>Utilizzando i tipi di evento <code>Replication</code>, è possibile ricevere notifiche per le configurazioni di replica con metriche di replica S3 o controllo del tempo di replica di S3 (S3 RTC) abilitate. È possibile monitorare l'avanzamento della replica minuto per minuto controllando i byte in sospeso, le operazioni in sospeso e la latenza di replica. Per informazioni sui parametri di replica, consulta Monitoraggio della replica con parametri, notifiche di eventi e stati.</p> <ul style="list-style-type: none"> • Il tipo di evento <code>s3:Replication:OperationFailedReplication</code> notifica quando un oggetto idoneo per la replica non è stato replicato. • Il tipo di evento <code>s3:Replication:OperationMissedThreshold</code> notifica quando un oggetto idoneo per la replica che utilizza S3 RTC supera la soglia di 15 minuti per la replica. • Il tipo di evento <code>s3:Replication:OperationReplicatedAfterThreshold</code> notifica quando un oggetto idoneo per la replica che utilizza S3 RTC viene replicato dopo la soglia di 15 minuti. • Il tipo di <code>s3:Replication:OperationNotTracked</code> evento ti avvisa quando un oggetto idoneo per la replica in tempo reale (Same-Region Replication [SRR] o Cross-Region Replication [CRR]) non viene più tracciato dalle metriche di replica.

Tipi di eventi	Description
<code>s3:LifecycleExpiration:*</code> <code>s3:LifecycleExpiration:Delete</code> <code>s3:LifecycleExpiration:DeleteMarkerCreated</code>	<p>Utilizzando i tipi di evento <code>LifecycleExpiration</code> , è possibile ricevere una notifica quando Amazon S3 elimina un oggetto in base alla configurazione del ciclo di vita S3.</p> <p>Il tipo di evento <code>s3:LifecycleExpiration:Delete</code> avvisa quando viene eliminato un oggetto in un bucket senza versione. Notifica inoltre quando una versione dell'oggetto viene eliminata definitivamente da una configurazione del ciclo di vita S3. Il tipo di evento <code>s3:LifecycleExpiration:DeleteMarkerCreated</code> notifica quando il ciclo di vita S3 crea un contrassegno di eliminazione quando viene eliminata una versione corrente di un oggetto in un bucket con versione.</p>
<code>s3:LifecycleTransition</code>	<p>Puoi ricevere questo evento di notifica quando un oggetto viene trasferito a un'altra classe di archiviazione Amazon S3 mediante una configurazione di S3 Lifecycle.</p>
<code>s3:IntelligentTiering</code>	<p>Si riceve questo evento di notifica quando un oggetto all'interno della classe di storage S3 viene spostato al livello Archive Access o al livello Intelligent-Tiering Deep Archive Access.</p>
<code>s3:ObjectTagging:*</code> <code>s3:ObjectTagging:Put</code> <code>s3:ObjectTagging:Delete</code>	<p>Utilizzando i tipi di evento <code>ObjectTagging</code> , è possibile attivare la notifica quando un tag oggetto viene aggiunto o eliminato da un oggetto.</p> <p>Il tipo di evento <code>s3:ObjectTagging:Put</code> notifica quando un tag viene inserito su un oggetto tramite richiesta PUT o quando viene aggiornato un tag esistente. Il tipo di evento <code>s3:ObjectTagging:Delete</code> notifica quando un tag viene rimosso da un oggetto.</p>

Tipi di eventi	Description
<code>s3:ObjectAnnotation:*</code> <code>s3:ObjectAnnotation:Put</code> <code>s3:ObjectAnnotation:Delete</code>	Utilizzando i tipi di <code>ObjectAnnotation</code> evento, è possibile abilitare la notifica quando un'annotazione viene creata, aggiornata o eliminata su un oggetto. Il tipo di <code>s3:ObjectAnnotation:Put</code> evento ti avvisa quando un'annotazione viene creata o aggiornata tramite. <code>PutObjectAnnotation</code> Il tipo di <code>s3:ObjectAnnotation:Delete</code> evento avvisa l'utente quando un'annotazione viene eliminata. <code>DeleteObjectAnnotation</code>
<code>s3:ObjectAcl:Put</code>	Puoi ricevere questo evento di notifica quando un'ACL viene inserita su un oggetto tramite richiesta PUT o quando viene modificata un'ACL esistente. Un evento non viene generato quando una richiesta non comporta alcuna modifica all'ACL di un oggetto.

Note

Nota il seguente comportamento per le notifiche degli eventi di annotazione:

- `PutObjectAnnotation DeleteObjectAnnotation` invia solo eventi specifici dell'annotazione. Non inviano eventi a livello di oggetto come. `s3:ObjectCreated:*`
- `GetObjectAnnotation ListObjectAnnotations` non inviano notifiche di eventi.
- `CopyObject` invia l'`s3:ObjectCreated:Copy` evento standard. Se l'oggetto copiato contiene annotazioni, l'evento include un `hasObjectAnnotation` campo impostato su `true`
- `DeleteObject` non include i campi relativi alle annotazioni nel payload dell'evento.
- I filtri di prefisso e suffisso si applicano solo alle chiavi degli oggetti, non ai nomi delle annotazioni.

Tipi di eventi supportati per Amazon EventBridge

Per un elenco dei tipi di eventi che Amazon S3 invierà ad Amazon EventBridge, consulta [Usando EventBridge](#).

Ordinamento degli eventi e duplicazione degli eventi

Amazon S3 Event Notifications è progettato per inviare notifiche almeno una volta, ma non è garantito che arrivino nello stesso ordine in cui si sono verificati gli eventi. In rare occasioni, il meccanismo di riprova di Amazon S3 potrebbe causare notifiche di eventi S3 duplicate per lo stesso evento oggetto. Per ulteriori informazioni sulla gestione degli eventi duplicati o fuori ordine, consulta la sezione [Gestire l'ordine degli eventi e gli eventi duplicati con le notifiche degli eventi di Amazon S3](#) su AWS Storage Blog.

Utilizzo di Amazon SQS, Amazon SNS e Lambda

L'abilitazione delle notifiche è un'operazione a livello di bucket. Le informazioni di configurazione delle notifiche vengono memorizzate nella risorsa secondaria di notifica associata a un bucket. Dopo avere creato o modificato la configurazione di notifica del bucket, in genere è necessario attendere 5 minuti affinché le modifiche abbiano effetto. Si verificherà un `s3:TestEvent` quando la notifica viene attivata per la prima volta. Per gestire la configurazione delle notifiche, è possibile utilizzare i metodi indicati di seguito:

- Utilizzo della console di Amazon S3 — E' possibile utilizzare l'interfaccia utente della console per impostare una configurazione di notifiche su un bucket senza dover scrivere alcun codice. Per ulteriori informazioni, consulta [Attivazione e configurazione delle notifiche di eventi tramite la console di Amazon S3](#).
- Utilizzo programmatico degli SDK: internamente, sia la console che AWS gli SDK richiamano l'API REST di Amazon S3 per gestire le risorse secondarie di notifica associate al bucket. Per esempi di configurazione di notifiche che utilizzano gli SDK di AWS, consulta [Spiegazione passo per passo: configurare un bucket per le notifiche \(argomento SNS o coda SQS\)](#).

Note

Puoi effettuare le chiamate a REST API di Amazon S3 anche direttamente dal codice. Tuttavia, ciò può risultare scomodo in quanto richiede la scrittura di codice per autenticare le richieste.

Indipendentemente dal metodo utilizzato, Amazon S3 archivia la configurazione delle notifiche in formato XML nella risorsa secondaria notifica associata a un bucket. Per informazioni sulle risorse secondarie del bucket, consulta la sezione [Opzioni di configurazione dei bucket per uso generico](#).

Note

Se si verificano più notifiche di eventi falliti a causa di destinazioni eliminate, è possibile che si riceva il messaggio Impossibile convalidare le seguenti configurazioni di destinazione quando si cerca di eliminarle. È possibile risolvere il problema nella console S3 eliminando contemporaneamente tutte le notifiche non riuscite.

Argomenti

- [Concessione di autorizzazioni per pubblicare messaggi di notifica eventi in una destinazione](#)
- [Attivazione e configurazione delle notifiche di eventi tramite la console di Amazon S3](#)
- [Configurazione delle notifiche degli eventi a livello di programmazione](#)
- [Spiegazione passo per passo: configurare un bucket per le notifiche \(argomento SNS o coda SQS\)](#)
- [Configurazione delle notifiche di eventi mediante il filtro dei nomi delle chiavi oggetto](#)
- [Struttura del messaggio di evento](#)

Concessione di autorizzazioni per pubblicare messaggi di notifica eventi in una destinazione

È necessario concedere al principale di Amazon S3 le autorizzazioni necessarie per richiamare l'API pertinente per pubblicare i messaggi in un argomento SNS, una coda SQS o una funzione Lambda. In questo modo Amazon S3 può pubblicare messaggi di notifica di eventi in una destinazione.

Per risolvere i problemi relativi alla pubblicazione dei messaggi di notifica di eventi su una destinazione, consulta [Risoluzione dei problemi relativi alla pubblicazione delle notifiche di eventi di Amazon S3 in un argomento di Servizio di notifica semplice Amazon](#).

Argomenti

- [Concessione delle autorizzazioni per richiamare un AWS Lambda funzione](#)
- [Concessione di autorizzazioni per pubblicare messaggi in un argomento SNS o una coda SQS](#)

Concessione delle autorizzazioni per richiamare un AWS Lambda funzione

Amazon S3 pubblica messaggi di evento richiamando una funzione AWS Lambda e fornendo il messaggio dell'evento come argomento.

Quando si utilizza la console di Amazon S3 per configurare le notifiche eventi in un bucket di Amazon S3 per una funzione Lambda, la console configura le autorizzazioni necessarie sulla funzione Lambda. In questo modo Amazon S3 dispone delle autorizzazioni per richiamare la funzione dal bucket. Per ulteriori informazioni, consulta [Attivazione e configurazione delle notifiche di eventi tramite la console di Amazon S3](#).

Puoi anche concedere ad Amazon S3 le autorizzazioni per richiamare la tua funzione Lambda AWS Lambda . Per ulteriori informazioni, consulta [Tutorial: Using AWS Lambda with Amazon S3](#) nella Developer Guide. AWS Lambda

Concessione di autorizzazioni per pubblicare messaggi in un argomento SNS o una coda SQS

Per concedere ad Amazon S3 le autorizzazioni per pubblicare messaggi sull'argomento SNS o sulla coda SQS, allega una policy AWS Identity and Access Management (IAM) all'argomento SNS o alla coda SQS di destinazione.

Per un esempio di come collegare una policy a un argomento SNS o a una coda SQS, consulta la sezione [Spiegazione passo per passo: configurare un bucket per le notifiche \(argomento SNS o coda SQS\)](#). Per ulteriori informazioni sulle autorizzazioni, consulta i seguenti argomenti:

- [Casi di esempio per il controllo degli accessi ad Amazon SNS](#) nella Guida per sviluppatori di Amazon Simple Notification Service
- [Identity and Access Management in Amazon SQS](#) nella Guida per gli sviluppatori di Amazon Simple Queue Service

Policy IAM per un argomento SNS di destinazione

Di seguito è riportato un esempio di policy AWS Identity and Access Management (IAM) da allegare all'argomento SNS di destinazione. Per maggiori informazioni su come utilizzare questa policy per configurare un argomento Amazon SNS di destinazione per le notifiche degli eventi, consulta [Spiegazione passo per passo: configurare un bucket per le notifiche \(argomento SNS o coda SQS\)](#).

JSON

```
{
  "Version": "2012-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "Example SNS topic policy",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": [
        "SNS:Publish"
      ],
      "Resource": "arn:aws:sns:us-east-1:111122223333:example-sns-topic",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        "StringEquals": {
          "aws:SourceAccount": "bucket-owner-123456789012"
        }
      }
    }
  ]
}
```

Policy IAM per una coda SQS di destinazione

Di seguito è riportato un esempio di policy IAM collegata alla coda SQS di destinazione. Per maggiori informazioni su come utilizzare questa policy per impostare una coda Amazon SQS di destinazione per le notifiche degli eventi, consulta [Spiegazione passo per passo: configurare un bucket per le notifiche \(argomento SNS o coda SQS\)](#).

Per utilizzare questa policy, devi aggiornare l'ARN della coda Amazon SQS, il nome del bucket e l'ID del proprietario del bucket. Account AWS

JSON

```
{
  "Version": "2012-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": [
        "SQS:SendMessage"
      ],
      "Resource": "arn:aws:sqs:us-east-1:111122223333:queue-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket"
        },
        "StringEquals": {
          "aws:SourceAccount": "bucket-owner-123456789012"
        }
      }
    }
  ]
}
```

Per entrambe le policy IAM di Amazon SNS e Amazon SQS, è possibile specificare la condizione `StringLike` nella policy anziché la condizione `ArnLike`.

Quando si utilizza `ArnLike`, le partizioni, il servizio, l'ID dell'account, il tipo di risorsa e l'ID della risorsa parziale dell'ARN devono corrispondere esattamente all'ARN nel contesto della richiesta. La corrispondenza parziale è consentita solo per la Regione e il percorso della risorsa.

Quando al posto di `ArnLike` viene utilizzato `StringLike`, la corrispondenza ignora la struttura dell'ARN e consente una corrispondenza parziale, indipendentemente dalla parte sostituita dal carattere jolly. Per ulteriori informazioni, consulta [Elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

```
"Condition": {  
  "StringLike": { "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket" }  
}
```

AWS KMS politica chiave

Se la coda SQS o gli argomenti SNS sono crittografati con una chiave AWS Key Management Service (AWS KMS) gestita dal cliente, è necessario concedere l'autorizzazione principale del servizio Amazon S3 per lavorare con gli argomenti o la coda crittografati. Per concedere al servizio Amazon S3 l'autorizzazione principale, aggiungi l'istruzione seguente alla policy delle chiavi per la chiave gestita dal cliente.

JSON

```
{  
  "Version": "2012-10-17",  
  "Id": "example-ID",  
  "Statement": [  
    {  
      "Sid": "example-statement-ID",  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "s3.amazonaws.com"  
      },  
      "Action": [  
        "kms:GenerateDataKey",  
        "kms:Decrypt"  
      ],  
      "Resource": "*"   
    }  
  ]  
}
```

Per ulteriori informazioni sulle policy chiave, consulta [AWS KMS Using key policy](#) in nella [Developer Guide. AWS KMS](#) AWS Key Management Service

Per ulteriori informazioni sull'utilizzo della crittografia lato server con AWS KMS Amazon SQS e Amazon SNS, consulta quanto segue:

- [Gestione delle chiavi](#) nella Guida per sviluppatori di Amazon Simple Notification Service.

- [Gestione delle chiavi](#) nella Guida per sviluppatori di Amazon Simple Queue Service.
- [Crittografia dei messaggi pubblicati su Amazon SNS con AWS KMS](#) nel Blog di calcolo di AWS .

Attivazione e configurazione delle notifiche di eventi tramite la console di Amazon S3

È possibile abilitare determinati eventi del bucket per uso generico Amazon S3 per inviare un messaggio di notifica a una destinazione ogni volta che si verificano gli eventi. In questa sezione viene descritto come utilizzare la console di Amazon S3 per abilitare le notifiche di evento. Per informazioni su come utilizzare le notifiche degli eventi con gli AWS SDK e le API REST di Amazon S3, consulta [Configurazione delle notifiche degli eventi a livello di programmazione](#)

Prerequisiti: prima di abilitare le notifiche di eventi per il bucket, è necessario impostare uno dei tipi di destinazione e quindi configurare le autorizzazioni. Per ulteriori informazioni, consulta [Destinazioni eventi supportate](#) e [Concessione di autorizzazioni per pubblicare messaggi di notifica eventi in una destinazione](#).

Note

Le code FIFO (First-In-First-Out) di Amazon Simple Queue Service non sono supportate come destinazione di notifica degli eventi di Amazon S3. Per inviare una notifica per un evento Amazon S3 a una coda FIFO di Amazon SQS, puoi utilizzare Amazon EventBridge. Per ulteriori informazioni, consulta [Abilitare Amazon EventBridge](#).

Argomenti

- [Attivazione delle notifiche di Amazon SNS, Amazon SQS o Lambda tramite la console di Amazon S3](#)

Attivazione delle notifiche di Amazon SNS, Amazon SQS o Lambda tramite la console di Amazon S3

Per abilitare e configurare le notifiche di evento per un bucket S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket per il quale desideri abilitare gli eventi.

4. Scegliere Properties (Proprietà).
5. Passare alla sezione Event Notifications (Notifiche evento) e scegliere Create event notification (Crea notifica evento).
6. Nella sezione General configuration (Configurazione generale) specificare il nome dell'evento descrittivo per la notifica dell'evento. Facoltativamente, è anche possibile specificare un prefisso e un suffisso per limitare le notifiche agli oggetti con chiavi che terminano con i caratteri specificati.

- a. Immettere una descrizione per Event name (Nome evento).

Se non specifichi un nome, viene generato e utilizzato un GUID (Globally Unique Identifier).

- b. (Facoltativo) Per filtrare le notifiche degli eventi in base al prefisso, immettere Prefix.

Ad esempio, è possibile impostare un filtro prefisso in modo da ricevere notifiche solo quando i file vengono aggiunti a una cartella specifica `co, images/`.

- c. (Facoltativo) Per filtrare le notifiche degli eventi in base al suffisso, immettere Suffix.

Per ulteriori informazioni, consulta [Configurazione delle notifiche di eventi mediante il filtro dei nomi delle chiavi oggetto](#).

7. Nella sezione Tipi di evento, selezionare uno o più tipi di evento per i quali si desidera ricevere notifiche.

Per un elenco dei vari tipi di evento, consulta [Tipi di eventi supportati per SQS, SNS e Lambda](#).

8. Nella sezione Destination (Destinazione), scegliere la destinazione della notifica dell'evento.

Note

Prima di poter pubblicare le notifiche di eventi, è necessario concedere al principale di Amazon S3 le autorizzazioni necessarie per richiamare l'API pertinente. In questo modo è possibile pubblicare le notifiche su una funzione Lambda, un argomento SNS o una coda SQS.

- a. Selezionare il tipo di destinazione: Lambda Function (Funzione Lambda), SNS Topic (Argomento SNS) o SQS Queue (Coda SQS).
- b. Dopo aver scelto il tipo di destinazione, scegliere una funzione, un argomento o una coda dall'elenco.

- c. In alternativa, se preferisci specificare un Amazon Resource Name (ARN), seleziona Inserisci ARN e specifica l'ARN.

Per ulteriori informazioni, consulta [Destinazioni eventi supportate](#).

9. Seleziona Salva modifiche e Amazon S3 invia un messaggio di prova alla destinazione della notifica dell'evento.

Configurazione delle notifiche degli eventi a livello di programmazione

Per impostazione predefinita, le notifiche sono disattivate per tutti i tipi di evento. Pertanto, inizialmente la risorsa secondaria notifica archivia una configurazione vuota.

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</NotificationConfiguration>
```

Per abilitare le notifiche per tipi di eventi specifici, sostituisci il file XML con la configurazione appropriata che identifica i tipi di evento che Amazon S3 deve pubblicare e la destinazione in cui gli eventi devono essere pubblicati. Per ciascuna destinazione, si aggiunge una configurazione XML corrispondente.

Per pubblicare messaggi di eventi in una coda SQS

Per impostare una coda SQS come destinazione di notifica per uno o più tipi di evento, aggiungi la `QueueConfiguration`.

```
<NotificationConfiguration>
  <QueueConfiguration>
    <Id>optional-id-string</Id>
    <Queue>sqs-queue-arn</Queue>
    <Event>event-type</Event>
    <Event>event-type</Event>
    ...
  </QueueConfiguration>
  ...
</NotificationConfiguration>
```

Per pubblicare i messaggi di eventi in un argomento SNS

Per impostare un argomento SNS come destinazione di notifica per tipi di eventi specifici, aggiungi la `TopicConfiguration`.

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>optional-id-string</Id>
    <Topic>sns-topic-arn</Topic>
    <Event>event-type</Event>
    <Event>event-type</Event>
    ...
  </TopicConfiguration>
  ...
</NotificationConfiguration>
```

Per richiamare il AWS Lambda funziona e fornisce un messaggio di evento come argomento

Per impostare una funzione Lambda come destinazione di notifica per tipi di eventi specifici, aggiungi la `CloudFunctionConfiguration`.

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
    <Id>optional-id-string</Id>
    <CloudFunction>cloud-function-arn</CloudFunction>
    <Event>event-type</Event>
    <Event>event-type</Event>
    ...
  </CloudFunctionConfiguration>
  ...
</NotificationConfiguration>
```

Per rimuovere tutte le notifiche configurate su un bucket

Per rimuovere tutte le notifiche configurate in un bucket, salva un elemento `<NotificationConfiguration/>` vuoto nella risorsa secondaria di notifica.

Quando Amazon S3 rileva un evento di tipo specifico, pubblica un messaggio con le informazioni sull'evento. Per ulteriori informazioni, consulta [Struttura del messaggio di evento](#).

Per ulteriori informazioni sulla configurazione delle notifiche di eventi, consulta i seguenti argomenti:

- [Spiegazione passo per passo: configurare un bucket per le notifiche \(argomento SNS o coda SQS\)](#).

- [Configurazione delle notifiche di eventi mediante il filtro dei nomi delle chiavi oggetto](#)

Spiegazione passo per passo: configurare un bucket per le notifiche (argomento SNS o coda SQS)

Puoi ricevere notifiche Amazon S3 utilizzando Amazon Simple Notification Service (Amazon SNS) o Amazon Simple Queue Service (Amazon SQS). Nella spiegazione passo per passo seguente viene aggiunta una configurazione di notifica al bucket utilizzando un argomento Amazon SNS e una coda Amazon SQS.

Note

Le code FIFO (First-In-First-Out) di Amazon Simple Queue Service non sono supportate come destinazione di notifica degli eventi di Amazon S3. Per inviare una notifica per un evento Amazon S3 a una coda FIFO di Amazon SQS, puoi utilizzare Amazon EventBridge. Per ulteriori informazioni, consulta [Abilitare Amazon EventBridge](#).

Argomenti

- [Riepilogo della spiegazione passo per passo](#)
- [Fase 1: creare una coda Amazon SQS](#)
- [Fase 2: creare un argomento Amazon SNS](#)
- [Fase 3: aggiungere una configurazione delle notifiche al bucket](#)
- [Fase 4: eseguire il test della configurazione](#)

Riepilogo della spiegazione passo per passo

Questa spiegazione passo per passo aiuta a completare le seguenti operazioni:

- Pubblicare eventi di tipo `s3:ObjectCreated:*` in una coda Amazon SQS.
- Pubblicare eventi di tipo `s3:ReducedRedundancyLostObject` in un argomento Amazon SNS.

Per informazioni sulla configurazione delle notifiche, consulta [Utilizzo di Amazon SQS, Amazon SNS e Lambda](#).

È possibile eseguire tutte queste fasi utilizzando la console, senza scrivere alcun codice. Inoltre, vengono forniti anche esempi di codice che utilizzano AWS SDK per Java e .NET per aiutarti ad aggiungere configurazioni di notifica a livello di programmazione.

La procedura include le seguenti fasi:

1. Creare una coda Amazon SQS.

Attraverso la console di Amazon SQS, crea una coda SQS. È possibile accedere a qualsiasi messaggio che Amazon S3 invia alla coda in modo programmatico. Tuttavia, per questa procedura guidata, i messaggi di notifica si verificano nella console.

Collega una policy di accesso all'argomento per concedere ad Amazon S3 l'autorizzazione a pubblicare messaggi.

2. Creare un argomento Amazon SNS.

Utilizzando la console di Amazon SNS, crea un argomento SNS e iscriviti all'argomento. In questo modo, riceverai tutti gli eventi pubblicati. Si specifica l'e-mail come protocollo di comunicazione. Dopo aver creato un argomento, Amazon SNS invia un'e-mail. È necessario utilizzare il collegamento nell'e-mail per confermare la sottoscrizione all'argomento.

Collega una policy di accesso all'argomento per concedere ad Amazon S3 l'autorizzazione a pubblicare messaggi.

3. Aggiungere una configurazione delle notifiche a un bucket.

Fase 1: creare una coda Amazon SQS

Segui le fasi per creare una coda Amazon Simple Queue Service (Amazon SQS) ed effettuarvi la sottoscrizione.

1. Utilizzando la console di Amazon SQS, creare una coda. Per istruzioni, consulta la sezione [Nozioni di base su Amazon SQS](#) nella Guida per gli sviluppatori di Amazon Simple Queue Service.
2. Sostituire la policy di accesso allegata alla coda con la policy riportata di seguito.
 - a. Nella console di Amazon SQS, nell'elenco Code, seleziona il nome della coda.
 - b. Nella scheda Policy di accesso, seleziona Modifica.

- c. Sostituire la policy di accesso allegata alla coda. Fornisci l'ARN di Amazon SQS, il nome del bucket di origine e l'ID dell'account del proprietario del bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": [
        "SQS:SendMessage"
      ],
      "Resource": "arn:aws:sqs:us-west-2:111122223333:s3-  
notification-queue",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
        },
        "StringEquals": {
          "aws:SourceAccount": "bucket-owner-123456789012"
        }
      }
    }
  ]
}
```

- d. Selezionare Salva.
3. (Facoltativo) Se la coda Amazon SQS o l'argomento Amazon SNS è abilitata per la crittografia lato server con AWS Key Management Service (AWS KMS), aggiungi la seguente policy alla chiave gestita dal cliente con crittografia simmetrica associata.

Devi aggiungere la policy a una chiave gestita dal cliente perché non è possibile modificare la chiave gestita da AWS per Amazon SQS o Amazon SNS.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

Per ulteriori informazioni sull'utilizzo di SSE per Amazon SQS e Amazon SNS con, consulta quanto segue: AWS KMS

- [Gestione delle chiavi](#) nella Guida per sviluppatori di Amazon Simple Notification Service.
- [Gestione delle chiavi](#) nella Guida per sviluppatori di Amazon Simple Queue Service.

4. Prendere nota dell'ARN della coda.

La coda SQS creata è un'altra risorsa nel tuo Account AWS. Dispone di un Amazon Resource Name (ARN) univoco. Il presente ARN è necessario nella fase successiva. Il nome ARN presenta il formato seguente:

```
arn:aws:sqs:aws-region:account-id:queue-name
```

Fase 2: creare un argomento Amazon SNS

Completa la procedura per creare e sottoscrivere un argomento Amazon SNS.

1. Utilizzando la console di Amazon SNS, crea un argomento. Per le istruzioni, consulta la sezione [Creazione di un argomento Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.
2. Effettuare la sottoscrizione all'argomento. Per questo esercizio, utilizzare l'e-mail come protocollo di comunicazione. Per le istruzioni, consulta la sezione [Sottoscrizione a un argomento di Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Si riceverà un'e-mail in cui è richiesto di confermare la sottoscrizione all'argomento. Confermare la sottoscrizione.

3. Sostituire la policy di accesso collegata all'argomento con la policy riportata di seguito. Fornisci l'ARN dell'argomento SNS, il nome del bucket e l'ID dell'account del proprietario del bucket.

```
{
  "Version": "2012-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": [
        "SNS:Publish"
      ],
      "Resource": "arn:aws:sns:us-west-2:111122223333:s3-notification-topic",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
        },
        "StringEquals": {
          "aws:SourceAccount": "bucket-owner-123456789012"
        }
      }
    }
  ]
}
```

4. Prendere nota dell'ARN dell'argomento.

L'argomento SNS che hai creato è un'altra risorsa nella tua e ha un Account AWS ARN univoco. L'ARN è necessario nella fase successiva. L'ARN ha il formato seguente:

```
arn:aws:sns:aws-region:account-id:topic-name
```

Fase 3: aggiungere una configurazione delle notifiche al bucket

Puoi abilitare le notifiche bucket utilizzando la console Amazon S3 o a livello di codice utilizzando gli SDK. AWS Scegliere una delle opzioni per configurare le notifiche nel bucket. Questa sezione fornisce esempi di codice che utilizzano gli SDK AWS per Java e .NET.

Opzione A: abilitare le notifiche in un bucket utilizzando la console

Utilizzando la console di Amazon S3, aggiungi una configurazione di notifica che richiede ad Amazon S3 di:

- Pubblicare gli eventi di tipo Tutti gli eventi di creazione dell'oggetto nella coda Amazon SQS.
- Pubblica gli eventi di tipo Oggetto perso in RRS sul tuo argomento Amazon SNS.

Dopo aver salvato la configurazione delle notifiche, Amazon S3 pubblica un messaggio di prova, che ricevi tramite e-mail.

Per istruzioni, consulta l'argomento [Attivazione e configurazione delle notifiche di eventi tramite la console di Amazon S3](#).

Opzione B: abilita le notifiche su un bucket utilizzando AWS SDK

.NET

L'esempio di codice C# riportato di seguito include il codice completo che aggiunge una configurazione delle notifiche in un bucket. Occorre aggiornare il codice e fornire il nome del bucket e l'ARN dell'argomento SNS. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;  
using Amazon.S3;  
using Amazon.S3.Model;  
using System;
```

```
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class EnableNotificationsTest
    {
        private const string bucketName = "**** bucket name ****";
        private const string snsTopic = "**** SNS topic ARN ****";
        private const string sqsQueue = "**** SQS topic ARN ****";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            EnableNotificationAsync().Wait();
        }

        static async Task EnableNotificationAsync()
        {
            try
            {
                PutBucketNotificationRequest request = new
PutBucketNotificationRequest
                {
                    BucketName = bucketName
                };

                TopicConfiguration c = new TopicConfiguration
                {
                    Events = new List<EventType> { EventType.ObjectCreatedCopy },
                    Topic = snsTopic
                };
                request.TopicConfigurations = new List<TopicConfiguration>();
                request.TopicConfigurations.Add(c);
                request.QueueConfigurations = new List<QueueConfiguration>();
                request.QueueConfigurations.Add(new QueueConfiguration()
                {
                    Events = new List<EventType> { EventType.ObjectCreatedPut },
                    Queue = sqsQueue
                });
            }
        }
    }
}
```

```
        PutBucketNotificationResponse response = await
client.PutBucketNotificationAsync(request);
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered on server. Message:'{0}' ",
e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown error encountered on server.
Message:'{0}' ", e.Message);
    }
}
}
```

Java

Per esempi su come configurare le notifiche bucket con l' AWS SDK per Java, consulta le notifiche degli eventi [Process S3](#) nell'Amazon S3 API Reference.

Fase 4: eseguire il test della configurazione

Ora è possibile testare la configurazione caricando un oggetto nel bucket e verificando la notifica di eventi nella console di Amazon SQS. Per istruzioni, consulta la sezione [Ricezione di un messaggio](#) nella sezione "Nozioni di base" della Guida per gli sviluppatori di Amazon Simple Queue Service.

Configurazione delle notifiche di eventi mediante il filtro dei nomi delle chiavi oggetto

Quando configuri una notifica di eventi di Amazon S3, devi specificare quali tipi di eventi di Amazon S3 supportati fanno sì che Amazon S3 invii la notifica. Se nel bucket S3 si verifica un tipo di evento che non hai specificato, Amazon S3 non invia la notifica.

È possibile configurare le notifiche in modo da essere filtrate in base al prefisso e al suffisso del nome della chiave degli oggetti. Ad esempio, è possibile impostare una configurazione per ricevere una notifica solo quando i file di immagini con l'estensione del nome file ".jpg" vengono aggiunti a un bucket. In alternativa, puoi avere una configurazione che invii una notifica a un argomento di Amazon SNS quando un oggetto con il prefisso "images/" viene aggiunto al bucket, mentre le notifiche per gli oggetti con un prefisso "logs/" nello stesso bucket vengono inviate a una funzione. AWS Lambda

 Note

Un carattere jolly ("*") non può essere utilizzato nei filtri come prefisso o suffisso. Se il prefisso o il suffisso contiene uno spazio, è necessario sostituirlo con il carattere "+". Se utilizzi altri caratteri speciali nel valore del prefisso o del suffisso, devi inserirli in formato (codificato in percentuale). [URL-encoded](#) Per un elenco completo dei caratteri speciali che devono essere convertiti in URL-encoded formato se utilizzati in un prefisso o suffisso per le notifiche degli eventi, vedere. [Caratteri sicuri](#)

È possibile impostare configurazioni delle notifiche che utilizzano il filtraggio del nome della chiave oggetto nella console di Amazon S3. Puoi farlo utilizzando direttamente le API di Amazon S3 tramite gli AWS SDK o le API REST. Per informazioni sull'utilizzo dell'interfaccia utente della console per impostare una configurazione di notifica in un bucket, consulta la sezione [Attivazione e configurazione delle notifiche di eventi tramite la console di Amazon S3](#).

Amazon S3 archivia la configurazione delle notifiche in formato XML nella risorsa secondaria notification associata a un bucket, come descritto in [Utilizzo di Amazon SQS, Amazon SNS e Lambda](#). Si utilizza la struttura XML `Filter` per definire le regole per filtrare le notifiche in base al prefisso o al suffisso del nome della chiave oggetto. Per informazioni sulla struttura XML `Filter`, consulta [notifica PUT Bucket](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Le configurazioni delle notifiche che utilizzano `Filter` non possono definire regole di filtri con prefissi che si sovrappongono, suffissi che si sovrappongono o prefisso e suffisso che si sovrappongono. Nelle sezioni seguenti sono riportati esempi di configurazioni delle notifiche valide con il filtro del nome della chiave dell'oggetto. Contengono anche esempi di configurazioni delle notifiche non valide a causa della sovrapposizione di prefisso/suffisso.

Argomenti

- [Esempi di configurazioni di notifiche valide con il filtro del nome della chiave dell'oggetto](#)
- [Esempi di configurazioni di notifiche con sovrapposizione di prefisso/suffisso non valida](#)

Esempi di configurazioni di notifiche valide con il filtro del nome della chiave dell'oggetto

La configurazione delle notifiche seguente contiene una configurazione della coda che identifica una coda Amazon SQS dove Amazon S3 deve pubblicare gli eventi di tipo `s3:ObjectCreated:Put`.

Gli eventi vengono pubblicati ogni volta che un oggetto con prefisso `images/` e suffisso `jpg` viene aggiunto a un bucket tramite richiesta PUT.

```
<NotificationConfiguration>
  <QueueConfiguration>
    <Id>1</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
        <FilterRule>
          <Name>suffix</Name>
          <Value>jpg</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Queue>arn:aws:sqs:us-west-2:444455556666:s3notificationqueue</Queue>
    <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

La configurazione delle notifiche riportata di seguito include diversi prefissi che non si sovrappongono. La configurazione stabilisce che le notifiche delle richieste PUT nella cartella `images/` vanno nella coda A (queue-A) mentre le notifiche delle richieste PUT nella cartella `logs/` vanno nella coda B (queue-B).

```
<NotificationConfiguration>
  <QueueConfiguration>
    <Id>1</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-A</Queue>
    <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
```

```

<QueueConfiguration>
  <Id>2</Id>
  <Filter>
    <S3Key>
      <FilterRule>
        <Name>prefix</Name>
        <Value>logs</Value>
      </FilterRule>
    </S3Key>
  </Filter>
  <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-B</Queue>
  <Event>s3:ObjectCreated:Put</Event>
</QueueConfiguration>
</NotificationConfiguration>

```

La configurazione delle notifiche riportata di seguito include diversi suffissi che non si sovrappongono. La configurazione stabilisce che tutte le nuove immagini .jpg aggiunte al bucket verranno elaborate dalla funzione Lambda cloud-function-A, mentre tutte le nuove immagini .png verranno elaborate dalla funzione cloud-function-B. I suffissi .png e .jpg non si sovrappongono anche se hanno la stessa lettera finale. I due suffissi si considerano sovrapposti se una determinata stringa può terminare con entrambi. Una stringa non può terminare sia con .png che con .jpg, pertanto i suffissi nella configurazione di esempio non si sovrappongono.

```

<NotificationConfiguration>
  <CloudFunctionConfiguration>
    <Id>1</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>suffix</Name>
          <Value>.jpg</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
    <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
    <Id>2</Id>
    <Filter>
      <S3Key>

```

```

        <FilterRule>
            <Name>suffix</Name>
            <Value>.png</Value>
        </FilterRule>
    </S3Key>
</Filter>
<CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
    <Event>s3:ObjectCreated:Put</Event>
</CloudFunctionConfiguration>
</NotificationConfiguration>

```

Le configurazioni delle notifiche che utilizzano `Filter` non possono definire regole per filtrare i prefissi che si sovrappongono nello stesso tipo di evento. Possono farlo solo se i prefissi sovrapposti sono utilizzati con suffissi che non si sovrappongono. L'esempio di configurazione seguente mostra in che modo gli oggetti creati con un prefisso comune ma con suffissi che non si sovrappongono possono essere distribuiti in diverse destinazioni.

```

<NotificationConfiguration>
    <CloudFunctionConfiguration>
        <Id>1</Id>
        <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
        </Filter>
        <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
        <Event>s3:ObjectCreated:Put</Event>
    </CloudFunctionConfiguration>
    <CloudFunctionConfiguration>
        <Id>2</Id>
        <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>

```

```
        <Value>images</Value>
      </FilterRule>
      <FilterRule>
        <Name>suffix</Name>
        <Value>.png</Value>
      </FilterRule>
    </S3Key>
  </Filter>
  <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
  <Event>s3:ObjectCreated:Put</Event>
</CloudFunctionConfiguration>
</NotificationConfiguration>
```

Esempi di configurazioni di notifiche con sovrapposizione di prefisso/suffisso non valida

La maggior parte delle configurazioni delle notifiche che utilizzano `Filter` non possono definire regole per filtrare i prefissi che si sovrappongono, i suffissi che si sovrappongono o le combinazioni di prefissi e suffissi che si sovrappongono per gli stessi tipi di eventi. È possibile avere prefissi che si sovrappongono a condizione che non si sovrappongano i suffissi. Per un esempio, consulta [Configurazione delle notifiche di eventi mediante il filtro dei nomi delle chiavi oggetto](#).

È possibile utilizzare filtri di nomi delle chiavi degli oggetti che si sovrappongono con diversi tipi di eventi. Ad esempio, si potrebbe creare una configurazione delle notifiche che utilizza il prefisso `image/` per il tipo di evento `ObjectCreated:Put` e il prefisso `image/` per il tipo di evento `ObjectRemoved:*`.

Se cerchi di salvare una configurazione delle notifiche con filtri di nomi non validi che si sovrappongono per gli stessi tipi di eventi, durante l'utilizzo dell'API o della console di Amazon S3, si verifica un errore. Questa sezione mostra esempi di configurazioni delle notifiche non valide a causa della sovrapposizione dei filtri dei nomi.

Si presuppone che qualsiasi regola di configurazione delle notifiche esistente abbia prefisso e suffisso predefiniti che corrispondano rispettivamente a qualsiasi altro prefisso e suffisso. La configurazione delle notifiche riportata di seguito non è valida poiché include prefissi che si sovrappongono. In particolare, il prefisso `root` si sovrappone con qualsiasi altro prefisso. Lo stesso vale nel caso in cui in questo esempio si utilizzi un suffisso anziché il prefisso. Il suffisso `root` si sovrappone a qualsiasi altro suffisso.

```
<NotificationConfiguration>
```

```

<TopicConfiguration>
  <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-one</Topic>
  <Event>s3:ObjectCreated:*</Event>
</TopicConfiguration>
<TopicConfiguration>
  <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-two</Topic>
  <Event>s3:ObjectCreated:*</Event>
  <Filter>
    <S3Key>
      <FilterRule>
        <Name>prefix</Name>
        <Value>images</Value>
      </FilterRule>
    </S3Key>
  </Filter>
</TopicConfiguration>
</NotificationConfiguration>

```

La configurazione delle notifiche riportata di seguito non è valida in quanto include suffissi che si sovrappongono. I due suffissi si considerano sovrapposti se una determinata stringa può terminare con entrambi. Una stringa può terminare con jpg e pg. Quindi, i suffissi si sovrappongono. Lo stesso vale per i prefissi. Due prefissi sono considerati sovrapposti se una determinata stringa può iniziare con entrambi i prefissi.

```

<NotificationConfiguration>
  <TopicConfiguration>
    <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
    <Event>s3:ObjectCreated:*</Event>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>suffix</Name>
          <Value>jpg</Value>
        </FilterRule>
      </S3Key>
    </Filter>
  </TopicConfiguration>
  <TopicConfiguration>
    <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
    <Event>s3:ObjectCreated:Put</Event>
    <Filter>
      <S3Key>
        <FilterRule>

```

```

        <Name>suffix</Name>
        <Value>pg</Value>
      </FilterRule>
    </S3Key>
  </Filter>
</TopicConfiguration>
</NotificationConfiguration>

```

La configurazione delle notifiche riportata di seguito non è valida poiché include prefissi e suffissi che si sovrappongono.

```

<NotificationConfiguration>
  <TopicConfiguration>
    <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
    <Event>s3:ObjectCreated:*</Event>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images</Value>
        </FilterRule>
        <FilterRule>
          <Name>suffix</Name>
          <Value>jpg</Value>
        </FilterRule>
      </S3Key>
    </Filter>
  </TopicConfiguration>
  <TopicConfiguration>
    <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
    <Event>s3:ObjectCreated:Put</Event>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>suffix</Name>
          <Value>jpg</Value>
        </FilterRule>
      </S3Key>
    </Filter>
  </TopicConfiguration>
</NotificationConfiguration>

```

Struttura del messaggio di evento

Il messaggio di notifica inviato da Amazon S3 per pubblicare un evento è in formato JSON.

Per una panoramica generale e istruzioni sulla configurazione delle notifiche degli eventi, consulta [Notifiche di eventi Amazon S3](#).

Questo esempio mostra la versione 2.5 della struttura JSON di notifica degli eventi. In precedenza, Amazon S3 utilizzava versioni diverse per diversi tipi di eventi. Gli eventi generali utilizzavano la versione 2.1, gli eventi di replica tra regioni erano usati 2.2 e gli eventi di eliminazione di S3 Lifecycle, S3, object ACL Intelligent-Tiering, object Tagging e Object Restoration hanno utilizzato la versione 2.3.

A partire dalla versione 2.4, Amazon S3 utilizza un'unica versione unificata per tutti i tipi di eventi e la versione viene incrementata in modo coerente tra tutti i tipi di eventi ogni volta che lo schema si evolve. Ogni evento contiene informazioni aggiuntive specifiche sull'operazione.

La dimensione massima di un messaggio di notifica di un evento è 64 KB. Quando usi Amazon SQS come destinazione, ti consigliamo di impostare l'`MaximumMessageSize` attributo della coda su almeno 64 KB. Se la notifica di un evento supera la coda configurata `MaximumMessageSize`, Amazon SQS rifiuta la notifica e non consegna l'evento. Per ulteriori informazioni, consulta [Tipi di notifiche eventi e destinazioni](#).

```
{
  "Records": [
    {
      "eventVersion": "2.5",
      "eventSource": "aws:s3",
      "awsRegion": "us-west-2",
      "eventTime": "The time, in ISO-8601 format (for example,
1970-01-01T00:00:00.000Z) when Amazon S3 finished processing the request",
      "eventName": "The event type",
      "userIdentity": {
        "principalId": "The unique ID of the IAM resource that caused the event"
      },
      "requestParameters": {
        "sourceIPAddress": "The IP address where the request came from"
      },
      "responseElements": {
        "x-amz-request-id": "The Amazon S3 generated request ID",
        "x-amz-id-2": "The Amazon S3 host that processed the request"
      },
    },
  ],
}
```

```

"s3":{
  "s3SchemaVersion":"1.0",
  "configurationId":"The ID found in the bucket notification configuration",
  "bucket":{
    "name":"The name of the bucket, for example, amzn-s3-demo-bucket",
    "ownerIdentity":{
      "principalId":"The Amazon retail customer ID of the bucket owner"
    },
    "arn":"The bucket Amazon Resource Name (ARN)",
    "awsGeneratedTags":"A map of tag key-value pairs generated by AWS
services and attached to the bucket; only present when AWS generated tags exist on the
bucket. This field is not present for cross-Region replication events"
  },
  "object":{
    "key":"The object key name",
    "size":"The object size in bytes (as a number)",
    "eTag":"The object entity tag (ETag)",
    "versionId":"The object version if the bucket is versioning-enabled;
null or not present if the bucket isn't versioning-enabled",
    "sequencer": "A string representation of a hexadecimal value used to
determine event sequence; only used with PUT and DELETE requests"
  }
},
"glacierEventData": {
  "restoreEventData": {
    "lifecycleRestorationExpiryTime": "The time, in ISO-8601 format (for
example, 1970-01-01T00:00:00.000Z), when the temporary copy of the restored object
expires",
    "lifecycleRestoreStorageClass": "The source storage class for restored
objects"
  }
}
]
}

```

Notare quanto segue sulla struttura dei messaggi di evento:

- Il valore della chiave `eventVersion` contiene una versione maggiore e minore nel formato *major.minor*.

La versione principale viene incrementata se Amazon S3 apporta una modifica alla struttura dell'evento che non è compatibile con le versioni precedenti. Questo include la rimozione di un

campo JSON che è già presente o la modifica del modo in cui i contenuti di un campo vengono rappresentati (ad esempio, un formato di data).

La versione secondaria viene incrementata se Amazon S3 apporta una modifica retrocompatibile alla struttura dell'evento. Ciò include l'aggiunta di nuovi campi alla struttura dell'evento o l'introduzione di nuovi tipi di eventi. Per mantenere la compatibilità con le nuove versioni secondarie della struttura degli eventi, è consigliabile che le applicazioni ignorino i nuovi campi.

Per fare in modo che le applicazioni analizzino correttamente la struttura dell'evento, è consigliabile eseguire un confronto "uguale a" sul numero della versione maggiore. Per fare in modo che i campi richiesti dall'applicazione siano presenti, è inoltre consigliabile eseguire un confronto "maggiore di o uguale a" sulla versione minore.

- Il valore di chiave `eventName` fa riferimento all'elenco dei [tipi di notifiche degli eventi](#) ma non contiene il prefisso `s3`.
- Il valore `userIdentity` chiave fa riferimento all'ID univoco della risorsa AWS Identity and Access Management (IAM) (utente, ruolo, gruppo e così via) che ha causato l'evento. Per la definizione di ciascun prefisso di identificazione IAM (ad esempio AIDA, AROA, AGPA) e per informazioni su come ottenere l'identificatore univoco, consulta [Identificatori univoci](#) nella Guida per l'utente IAM.
- Il valore `responseElements` chiave è utile se si desidera tracciare una richiesta procedendo con Supporto AWS. Sia `x-amz-request-id` sia `x-amz-id-2` aiutano Amazon S3 a tenere traccia di una singola richiesta. Questi valori corrispondono a quelli che Amazon S3 restituisce nella risposta alla richiesta che avvia gli eventi. Pertanto, è possibile utilizzare questi valori per abbinare l'evento alla richiesta.
- Il valore di chiave `s3` fornisce informazioni sul bucket e sull'oggetto coinvolto nell'evento. Il valore del nome della chiave dell'oggetto ha la codifica URL. Ad esempio `red flower.jpg` diventa `red+flower.jpg`. Amazon S3 restituisce "application/x-www-form-urlencoded" come tipo di contenuto nella risposta.

Il valore `ownerIdentity` chiave corrisponde all'ID cliente Amazon retail (Amazon.com) del proprietario del bucket. Questo valore di ID non viene più utilizzato e viene mantenuto solo per motivi di compatibilità con le versioni precedenti.

- Il valore di chiave `sequencer` fornisce un modo per stabilire la sequenza degli eventi. Non è garantito che le notifiche di eventi arrivino nello stesso ordine in cui avvengono gli eventi. Tuttavia, notifiche di eventi che creano oggetti (richieste PUT) ed eliminano oggetti contengono un `sequencer`. È possibile utilizzare questo valore per determinare l'ordine degli eventi per una specifica chiave dell'oggetto.

Se si confrontano le stringhe `sequencer` da due notifiche eventi nella stessa chiave dell'oggetto, la notifica evento con il valore esadecimale `sequencer` più elevato è l'evento che è avvenuto per ultimo. Se si utilizzano notifiche di eventi per mantenere un database o un indice separato degli oggetti Amazon S3, è consigliabile confrontare e archiviare i valori `sequencer` man mano che la notifica di ciascun evento viene elaborata.

Tenere presente quanto segue:

- Il valore di chiave `sequencer` non può essere utilizzato per determinare l'ordine degli eventi su diverse chiavi degli oggetti.
- Le stringhe `sequencer` possono essere di diversa lunghezza. Quindi, per confrontare questi valori, per prima cosa aggiungi gli zeri al valore più breve e poi esegui un confronto lessicografico.
- Il valore di chiave `glacierEventData` è visibile solo per gli eventi `s3:ObjectRestore:Completed`.
- Il valore di chiave `restoreEventData` contiene attributi correlati alla richiesta di ripristino.
- Il valore di chiave `replicationEventData` è visibile solo per gli eventi di replica.
- Il valore della `intelligentTieringEventData` chiave è visibile solo per gli eventi S3 Intelligent-Tiering .
- Il valore di chiave `lifecycleEventData` è visibile solo per gli eventi di transizione del ciclo di vita S3.
- Il valore della `objectAnnotation` chiave è visibile solo per gli eventi di annotazione (`ObjectAnnotation:PutObjectAnnotation:Delete`). Contiene un array con `l'annotazione`name, `size` (solo eventi Put) e `eTag` (solo eventi Put).
- Per `ObjectCreated:Copy` gli eventi, il `object` blocco include un campo `hasObjectAnnotation` booleano che indica se l'oggetto copiato contiene annotazioni.

Messaggi di esempio

Di seguito sono riportati alcuni esempi di messaggi di notifica degli eventi Amazon S3.

Messaggio di prova Amazon S3

Quando configuri una notifica di eventi in un bucket, Amazon S3 invia il messaggio di prova riportato di seguito.

```
{
```

```

"Service": "Amazon S3",
"Event": "s3:TestEvent",
"Time": "2014-10-13T15:57:02.089Z",
"Bucket": "amzn-s3-demo-bucket",
"RequestId": "5582815E1AEA5ADF",
"HostId": "8cLeGAmw098X5cv4Zkwcmo8vvZa3eH3eKxsPzbB9wrR+YstdA6Knx4Ip8EXAMPLE"
}

```

Note

Il messaggio `s3:TestEvent` utilizza un formato diverso rispetto alle normali notifiche degli eventi S3. A differenza di altre notifiche degli eventi che utilizzano la struttura dell'array `Records` mostrata in precedenza, l'evento di test utilizza un formato semplificato con campi diretti. Quando si implementa la gestione degli eventi, è necessario assicurarsi che il codice sia in grado di distinguere e gestire correttamente entrambi i formati di messaggio.

Messaggio di esempio quando un oggetto viene creato utilizzando una richiesta PUT

Quello che segue è un esempio di un messaggio inviato da Amazon S3 per pubblicare un evento `s3:ObjectCreated:Put`.

```

{
  "Records": [
    {
      "eventVersion": "2.5",
      "eventSource": "aws:s3",
      "awsRegion": "us-west-2",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "AIDAJDPLRKL7UEXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "172.16.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "C3D13FE58DE4C810",
        "x-amz-id-2": "FMYUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/JRWeUWerMUE5JgHvAN0jpD"
      }
    ]
  }
}

```

```
"s3":{
  "s3SchemaVersion":"1.0",
  "configurationId":"testConfigRule",
  "bucket":{
    "name":"amzn-s3-demo-bucket",
    "ownerIdentity":{
      "principalId":"A3NL1K0ZZKExample"
    },
    "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
  },
  "object":{
    "key":"HappyFace.jpg",
    "size":1024,
    "eTag":"d41d8cd98f00b204e9800998ecf8427e",
    "versionId":"096fKKXTRTt13on89fV0.nfljtsv6qko",
    "sequencer":"0055AED6DCD90281E5"
  }
}
}
```

Usando EventBridge

Amazon S3 può inviare eventi ad Amazon EventBridge ogni volta che si verificano determinati eventi nel tuo bucket. A differenza di altre destinazioni, non è necessario selezionare i tipi di eventi che si desidera inviare. Dopo EventBridge l'attivazione, tutti gli eventi seguenti vengono inviati a EventBridge. È possibile utilizzare EventBridge le regole per indirizzare gli eventi verso obiettivi aggiuntivi. Di seguito sono elencati gli eventi a cui Amazon S3 invia. EventBridge

Tipo di evento	Description
Oggetto creato	Un oggetto è stato creato. Il campo motivo nella struttura dei messaggi di evento indica quale API S3 è stata utilizzata per creare l'oggetto : PutObject , POST Object , CopyObject o CompleteMultipartUpload .
Oggetto eliminato () DeleteObject	Un oggetto è stato eliminato.

Tipo di evento	Description
Oggetto eliminato (scadenza del ciclo di vita)	<p>Quando un oggetto viene eliminato utilizzando una chiamata API S3, il campo del motivo è impostato su DeleteObject. Quando un oggetto viene eliminato da una regola di scadenza del ciclo di vita S3, il campo motivo è impostato su Scadenza ciclo di vita. Per ulteriori informazioni, consulta Oggetti in scadenza.</p> <p>Quando viene eliminato un oggetto senza controllo delle versioni o quando viene eliminato in modo permanente un oggetto con controllo delle versioni, il campo del tipo di eliminazione è impostato su Permanently Deleted. Quando viene creato un indicatore di eliminazione per un oggetto con controllo delle versioni, il campo deletion-type è impostato su Delete Marker Created. Per ulteriori informazioni, consulta Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata.</p>
Ripristino oggetti avviato	Il ripristino degli oggetti è stato avviato dalla classe di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive o dal livello S3 Archive Access o Deep Archive Intelligent-Tiering Access. Per ulteriori informazioni, consulta Utilizzo di oggetti archiviati .
Ripristino oggetti completato	È stato completato un ripristino di oggetti.
Ripristino oggetti scaduto	La copia temporanea di un oggetto ripristinato da S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive è scaduta ed è stata eliminata.
Classe di archiviazione di oggetti modificata	Un oggetto è stato trasferito a una classe di archiviazione diversa. Per ulteriori informazioni, consulta Trasferimento degli oggetti utilizzando il ciclo di vita Amazon S3 .

Tipo di evento	Description
Livello di accesso agli oggetti modificato	Un oggetto è stato trasferito al livello S3 Archive Access o al livello Deep Archive Access Intelligent-Tiering . Per ulteriori informazioni, consulta Gestione dei costi di storage con il Piano intelligente Amazon S3 .
Aggiornamento dell'ACL dell'oggetto	La lista di controllo degli accessi (ACL) di un oggetto è stata impostata utilizzando <code>PutObjectAc1</code> . Un evento non viene generato quando una richiesta non comporta alcuna modifica all'ACL di un oggetto. Per ulteriori informazioni, consulta Panoramica delle liste di controllo accessi (ACL) .
Aggiunti tag degli oggetti	Un set di tag è stato aggiunto a un oggetto utilizzando <code>PutObjectTagging</code> . Per ulteriori informazioni, consulta Etichettare i tuoi oggetti .
Eliminazione di tag degli oggetti	Tutti i tag sono stati rimossi da un oggetto utilizzando <code>DeleteObjectTagging</code> . Per ulteriori informazioni, consulta Etichettare i tuoi oggetti .
Annotazione dell'oggetto creata	Un'annotazione è stata creata o aggiornata su un oggetto utilizzando <code>PutObjectAnnotation</code> . Per ulteriori informazioni, consulta Annotazione degli oggetti .
Annotazione dell'oggetto rimossa	Un'annotazione è stata eliminata da un oggetto utilizzando <code>DeleteObjectAnnotation</code> . Per ulteriori informazioni, consulta Annotazione degli oggetti .

 Note

Per ulteriori informazioni su come i tipi di eventi di Amazon S3 vengono mappati ai tipi di EventBridge eventi, consulta. [Mappatura e risoluzione dei problemi di Amazon EventBridge](#)

Puoi utilizzare Amazon S3 Event Notifications con EventBridge per scrivere regole che intraprendano azioni quando si verifica un evento nel tuo bucket. Ad esempio, è possibile scegliere di ricevere

una notifica. Per ulteriori informazioni, consulta [What is? EventBridge](#) nella Guida per EventBridge l'utente di Amazon.

Per ulteriori informazioni sulle azioni e sui tipi di dati con cui puoi interagire utilizzando l' EventBridge API, consulta [Amazon EventBridge API Reference](#) nell'Amazon EventBridge API Reference.

Per informazioni sui prezzi, consulta i EventBridge prezzi di [Amazon](#).

Argomenti

- [EventBridge Autorizzazioni Amazon](#)
- [Abilitare Amazon EventBridge](#)
- [EventBridge struttura del messaggio di evento](#)
- [Mappatura e risoluzione dei problemi di Amazon EventBridge](#)

EventBridge Autorizzazioni Amazon

Amazon S3 non richiede autorizzazioni aggiuntive per fornire eventi ad Amazon. EventBridge

Abilitare Amazon EventBridge

Puoi abilitare Amazon EventBridge utilizzando la console S3, AWS Command Line Interface (AWS CLI) o l'API REST di Amazon S3.

Note

Dopo l'attivazione EventBridge, sono necessari circa cinque minuti affinché le modifiche abbiano effetto.

Utilizzo della console S3

Per abilitare la distribuzione EventBridge degli eventi nella console S3.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome del bucket per il quale desideri abilitare gli eventi.

4. Scegliere Properties (Proprietà).
5. Vai alla sezione Notifiche degli eventi e trova la EventBridge sottosezione Amazon. Scegli Modifica.
6. In Invia notifiche ad Amazon EventBridge per tutti gli eventi di questo bucket, scegli Attivato.

Utilizzo di AWS CLI

L'esempio seguente crea una configurazione di notifica del bucket per un bucket *amzn-s3-demo-bucket1* con Amazon abilitato. EventBridge

```
aws s3api put-bucket-notification-configuration --bucket amzn-s3-demo-bucket1 --notification-configuration='{ "EventBridgeConfiguration": {} }'
```

Utilizzo della REST API

Puoi abilitare Amazon in modo programmatico EventBridge su un bucket chiamando l'API REST di Amazon S3. Per ulteriori informazioni, consulta [PutBucketNotificationConfiguration](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

L'esempio seguente mostra l'XML utilizzato per creare una configurazione di notifica del bucket con Amazon abilitato. EventBridge

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <EventBridgeConfiguration>
  </EventBridgeConfiguration>
</NotificationConfiguration>
```

Creazione di regole EventBridge

Una volta abilitato, puoi creare EventBridge regole Amazon per determinate attività. Ad esempio, è possibile inviare notifiche via e-mail quando viene creato un oggetto. Per un tutorial completo, consulta [Tutorial: Invia una notifica quando viene creato un oggetto Amazon S3](#) nella Amazon EventBridge User Guide.

EventBridge struttura del messaggio di evento

Il messaggio di notifica inviato da Amazon S3 per pubblicare un evento è in formato JSON. Quando Amazon S3 invia un evento ad Amazon EventBridge, sono presenti i seguenti campi.

- **version**: attualmente 0 (zero) per tutti gli eventi. Si tratta di un campo Amazon EventBridge envelope e non viene utilizzato per il controllo delle versioni dello schema. Per il controllo delle versioni dello schema degli eventi, consulta il campo `event-version` nel campo dei dettagli.
- **id**: un UUID generato per ogni evento.
- **detail-type**: il tipo di evento inviato. Per un elenco dei tipi di evento, consulta [Usando EventBridge](#).
- **source**: identifica il servizio che ha generato l'evento.
- **account**— L' Account AWS ID a 12 cifre del proprietario del bucket.
- **time**: l'ora in cui si è verificato l'evento.
- **region**— Identifica il numero del Regione AWS bucket.
- **resources**: un array JSON che contiene il nome della risorsa Amazon (ARN) del bucket.
- **detail** – Un oggetto JSON contenente informazioni sull'evento. Per ulteriori informazioni su ciò che può essere incluso in questo campo, consulta [Campo dei dettagli del messaggio di evento](#).

Esempi di struttura dei messaggi di evento

Di seguito sono riportati alcuni esempi di messaggi di notifica degli eventi di Amazon S3 che possono essere inviati ad Amazon. EventBridge

Oggetto creato

```
{
  "version": "0",
  "id": "17793124-05d4-b198-2fde-7ededc63b103",
  "detail-type": "Object Created",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "event-version": "1.1",
    "bucket": {
      "name": "amzn-s3-demo-bucket1",
      "aws-generated-tags": {
```

```

    "aws:cloudformation:stack-id": "arn:aws:cloudformation:us-
east-1:111122223333:stack/amzn-s3-demo-stack/51af3dc0-da77-11e4-872e-1234567db123",
    "aws:cloudformation:logical-id": "S3DemoBucket",
    "aws:cloudformation:stack-name": "amzn-s3-demo-stack"
  }
},
"object": {
  "key": "example-key",
  "size": 5,
  "etag": "b1946ac92492d2347c6235b4d2611184",
  "version-id": "IYV3p45BT0ac8hjHg1houSdS1a.Mro8e",
  "sequencer": "617f08299329d189"
},
"request-id": "N4N7GDK58NMKJ12R",
"requester": "123456789012",
"source-ip-address": "1.2.3.4",
"reason": "PutObject"
}
}

```

Oggetto eliminato (utilizzando DeleteObject)

```

{
  "version": "0",
  "id": "2ee9cc15-d022-99ea-1fb8-1b1bac4850f9",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "event-version": "1.1",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",

```

```

    "version-id": "1QW9g1Z99LUNbvaaYVpW9xD10LU.qxgF",
    "sequencer": "617f0837b476e463"
  },
  "request-id": "0BH729840619AG5K",
  "requester": "123456789012",
  "source-ip-address": "1.2.3.4",
  "reason": "DeleteObject",
  "deletion-type": "Delete Marker Created"
}
}

```

Oggetto eliminato (utilizzando la scadenza del ciclo di vita)

```

{
  "version": "0",
  "id": "ad1de317-e409-eba2-9552-30113f8d88e3",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "event-version": "1.1",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "mtB0cV.jejK63XkRNceanNMC.qXPWLeK",
      "sequencer": "617b398000000000"
    },
    "request-id": "20EB74C14654DC47",
    "requester": "s3.amazonaws.com",
    "reason": "Lifecycle Expiration",
    "deletion-type": "Delete Marker Created"
  }
}

```

Ripristino oggetti completato

```
{
  "version": "0",
  "id": "6924de0d-13e2-6bbf-c0c1-b903b753565e",
  "detail-type": "Object Restore Completed",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "event-version": "1.1",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "KKsjUC1.6gIjqtvhfg5AdMI0eCePIiT3"
    },
    "request-id": "189F19CB7FB1B6A4",
    "requester": "s3.amazonaws.com",
    "restore-expiry-time": "2021-11-13T00:00:00Z",
    "source-storage-class": "GLACIER"
  }
}
```

Annotazione dell'oggetto creato

```
{
  "version": "0",
  "id": "8c2bfa57-4a67-b2ea-c4e0-6d420ea3b3a6",
  "detail-type": "Object Annotation Created",
  "source": "aws.s3",
  "account": "111122223333",
```

```
"time": "2025-03-15T00:00:00Z",
"region": "us-east-1",
"resources": [
  "arn:aws:s3:::amzn-s3-demo-bucket1"
],
"detail": {
  "version": "0",
  "event-version": "1.1",
  "bucket": {
    "name": "amzn-s3-demo-bucket1"
  },
  "object": {
    "key": "example-key",
    "etag": "b1946ac92492d2347c6235b4d2611184",
    "version-id": "IYV3p45BT0ac8hjHg1houSdS1a.Mro8e",
    "sequencer": "617f08299329d189"
  },
  "request-id": "4B4NGD358NMKJ12R",
  "requester": "123456789012",
  "source-ip-address": "1.2.3.4",
  "reason": "PutObjectAnnotation",
  "object-annotation": {
    "name": "my-annotation",
    "size": 24,
    "etag": "05df351ea190dffc26f55c74425b9d7a"
  }
}
}
```

Annotazione dell'oggetto rimossa

```
{
  "version": "0",
  "id": "a3d1bc94-5f82-c7e1-d290-7e531fb4c5b8",
  "detail-type": "Object Annotation Removed",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2025-03-15T00:00:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
```

```
"detail": {
  "version": "0",
  "event-version": "1.1",
  "bucket": {
    "name": "amzn-s3-demo-bucket1"
  },
  "object": {
    "key": "example-key",
    "etag": "b1946ac92492d2347c6235b4d2611184",
    "version-id": "IYV3p45BT0ac8hjHg1houSdS1a.Mro8e",
    "sequencer": "617f08299329d190"
  },
  "request-id": "7C5NGD358NMKJ34S",
  "requester": "123456789012",
  "source-ip-address": "1.2.3.4",
  "reason": "DeleteObjectAnnotation",
  "object-annotation": {
    "name": "my-annotation"
  }
}
```

Campo dei dettagli del messaggio di evento

Il campo dei dettagli contiene un oggetto JSON con informazioni sull'evento. I seguenti campi possono essere presenti nel campo dettagli.

- `version`: attualmente 0 (zero) per tutti gli eventi.
- `event-version`— La versione dello schema degli eventi nel modulo *major.minor* (ad esempio, 1.1).

La versione principale viene incrementata se Amazon S3 apporta una modifica alla struttura dell'evento che non è compatibile con le versioni precedenti. Questo include la rimozione di un campo JSON che è già presente o la modifica del modo in cui i contenuti di un campo vengono rappresentati (ad esempio, un formato di data).

La versione secondaria viene incrementata se Amazon S3 apporta una modifica retrocompatibile alla struttura degli eventi. Ciò include l'aggiunta di nuovi campi alla struttura dell'evento o l'introduzione di nuovi tipi di eventi. Per mantenere la compatibilità con le nuove versioni secondarie della struttura degli eventi, è consigliabile che le applicazioni ignorino i nuovi campi.

Per fare in modo che le applicazioni analizzino correttamente la struttura dell'evento, è consigliabile eseguire un confronto "uguale a" sul numero della versione maggiore. Per fare in modo che i campi richiesti dall'applicazione siano presenti, è inoltre consigliabile eseguire un confronto "maggiore di o uguale a" sulla versione minore.

- **bucket**: informazioni sul bucket Amazon S3 coinvolto nell'evento.
- **aws-generated-tags**— Tag allegati al bucket dai AWS servizi. Sono presenti solo quando i tag AWS generati sono presenti nel bucket. Questo campo non è presente per gli eventi di replica tra regioni.
- **object**: informazioni sull'oggetto Amazon S3 coinvolto nell'evento.
- **request-id**: ID della richiesta nella risposta S3.
- **requester**— Account AWS ID o principale del AWS servizio del richiedente.
- **source-ip-address**: l'indirizzo IP di origine della richiesta S3. Presente solo per eventi attivati da una richiesta S3.
- **reason**: per gli eventi Oggetto creato, l'API S3 utilizzata per creare l'oggetto: [PutObject](#), [POST Object](#), [CopyObject](#) o [CompleteMultipartUpload](#). Per gli eventi Oggetto eliminato, questo campo è impostato su DeleteObject quando un oggetto viene eliminato da una chiamata API S3, oppure su Scadenza del ciclo di vita quando un oggetto viene eliminato da una regola di scadenza del ciclo di vita S3. Per ulteriori informazioni, consulta [Oggetti in scadenza](#).
- **deletion-type**: per gli eventi Oggetto eliminato, quando viene eliminato un oggetto senza controllo delle versioni o quando viene eliminato in modo permanente un oggetto con controllo delle versioni, questo campo è impostato su Eliminato definitivamente. Quando viene creato un contrassegno di eliminazione per un oggetto con versione, verrà impostato su Contrassegno di eliminazione creato. Per ulteriori informazioni, consulta [Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata](#).

Note

Alcuni attributi degli oggetti (come etag e size) sono presenti solo quando viene creato un marcatore di cancellazione.

- **restore-expiry-time**: per gli eventi Ripristino oggetto completato, il momento in cui la copia temporanea dell'oggetto viene eliminata da S3. Per ulteriori informazioni, consulta [Utilizzo di oggetti archiviati](#).

- `source-storage-class`: per gli eventi Ripristino oggetto avviato e Ripristino oggetto completato, la classe di archiviazione dell'oggetto in fase di ripristino. Per ulteriori informazioni, consulta [Utilizzo di oggetti archiviati](#).
- `destination-storage-class`: per gli eventi Classe di archiviazione di oggetti modificata, la nuova classe di archiviazione dell'oggetto. Per ulteriori informazioni, consulta [Trasferimento degli oggetti utilizzando il ciclo di vita Amazon S3](#).
- `destination-access-tier`: per gli eventi Livello di accesso agli oggetti modificato, il nuovo livello di accesso dell'oggetto. Per ulteriori informazioni, consulta [Gestione dei costi di storage con il Piano intelligente Amazon S3](#).
- `object-annotation`— Per gli eventi Object Annotation Created e Object Annotation Removed, il `detail` campo include un `object-annotation` campo contenente informazioni sull'annotazione.
- `has-object-annotation`— Per gli eventi Object Created con motivoCopyObject, il `object` blocco include un campo `has-object-annotation` booleano che indica se l'oggetto copiato contiene annotazioni.

Mappatura e risoluzione dei problemi di Amazon EventBridge

La tabella seguente descrive come i tipi di eventi Amazon S3 vengono mappati ai tipi di eventi Amazon EventBridge .

Tipo di evento S3	Tipo di dettaglio Amazon EventBridge
ObjectCreated:Put	Oggetto creato
ObjectCreated:Post	
ObjectCreated:Copy	
ObjectCreated:CompleteMulti partUpload	
ObjectRemoved:Delete	Oggetto eliminato
ObjectRemoved:DeleteMarkerCreated	
LifecycleExpiration:Delete	

Tipo di evento S3	Tipo di dettaglio Amazon EventBridge
LifecycleExpiration:DeleteMarkerCreated	
ObjectRestore:Post	Ripristino oggetti avviato
ObjectRestore:Completed	Ripristino oggetti completato
ObjectRestore:Delete	Ripristino oggetti scaduto
LifecycleTransition	Classe di archiviazione di oggetti modificata
IntelligentTiering	Livello di accesso agli oggetti modificato
ObjectTagging:Put	Aggiunti tag degli oggetti
ObjectTagging:Delete	Eliminazione di tag degli oggetti
ObjectAcl:Put	Aggiornamento dell'ACL dell'oggetto
ObjectAnnotation:Put	Annotazione dell'oggetto creata
ObjectAnnotation:Delete	Annotazione dell'oggetto rimossa

Risoluzione dei problemi di Amazon EventBridge

Per informazioni su come risolvere i problemi EventBridge, consulta [Troubleshooting Amazon EventBridge](#) nella Amazon User Guide. EventBridge

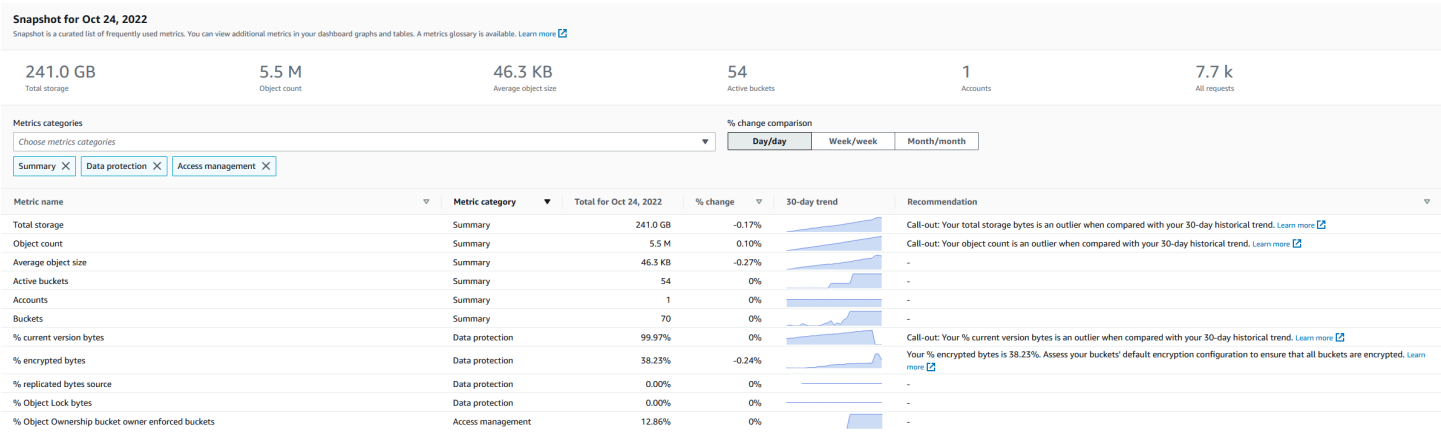
Monitoraggio dell'attività e dell'utilizzo dello storage con Amazon S3 Storage Lens

Amazon S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che permette di avere una panoramica completa a livello di organizzazione sull'utilizzo e sull'archiviazione di oggetti. S3 Storage Lens analizza i parametri di archiviazione per fornire raccomandazioni contestuali che puoi usare per ottimizzare i costi di archiviazione e applicare le best practice sulla protezione dei dati.

Puoi utilizzare i parametri di S3 Storage Lens per generare approfondimenti di riepilogo. Ad esempio, per scoprire la quantità di spazio di archiviazione disponibile in tutta l'organizzazione o quali sono

i bucket e i prefissi caratterizzati da una crescita più rapida. Puoi anche utilizzare le metriche di S3 Storage Lens per identificare opportunità di ottimizzazione dei costi, implementare le migliori pratiche di protezione dei dati e gestione degli accessi e migliorare le prestazioni dei carichi di lavoro delle applicazioni. Ad esempio, puoi identificare i bucket che non hanno regole del ciclo di vita S3 configurate per far scadere i caricamenti in più parti incompleti che risalgono a più di 7 giorni. Puoi anche identificare i bucket che non seguono le best practice di protezione dei dati, come l'utilizzo di S3 Replication o S3 Versioning.

S3 Storage Lens aggrega i tuoi parametri e mostra le informazioni nella sezione Account snapshot (Snapshot dell'account) nella pagina Buckets (Bucket) della console di Amazon S3. S3 Storage Lens fornisce anche una dashboard interattiva che puoi utilizzare per visualizzare informazioni e tendenze, segnalare valori anomali e ricevere consigli per ottimizzare i costi di storage e applicare le migliori pratiche di protezione dei dati. La dashboard offre opzioni di approfondimento per generare e visualizzare informazioni dettagliate a livello di organizzazione, account, classe di archiviazione, bucket Regione AWS, prefisso o gruppo Storage Lens. Puoi anche inviare un rapporto giornaliero sulle metriche in Parquet formato CSV o a un bucket S3 generico o esportare le metriche direttamente in un bucket di tabelle S3 gestito. AWS



Caratteristiche e parametri di S3 Storage Lens

In S3 Storage Lens è disponibile un pannello di controllo interattivo predefinito che viene aggiornato quotidianamente. S3 Storage Lens preconfigura questo pannello di controllo per visualizzare le informazioni dettagliate di riepilogo e le tendenze per l'intero account e le aggiorna quotidianamente nella console S3. I parametri di questo pannello di controllo vengono riepilogati anche nello snapshot dell'account nella paginaBuckets (Bucket). Per ulteriori informazioni, consulta [Pannello di controllo predefinito](#).

Per creare altre dashboard e classificarle in base Regioni AWS a bucket S3 o account (per AWS Organizations), crei una configurazione della dashboard di S3 Storage Lens. Puoi creare e gestire le

configurazioni del dashboard di S3 Storage Lens utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), gli AWS SDK o l'API REST di Amazon S3. Quando si crea o si modifica una dashboard S3 Storage Lens, si definisce l'ambito della dashboard e la selezione delle metriche.

S3 Storage Lens offre metriche di livello gratuito e metriche di livello avanzato, a cui puoi effettuare l'upgrade a un costo aggiuntivo. Con il livello avanzato, puoi accedere a metriche e funzionalità aggiuntive per ottenere informazioni dettagliate sul tuo spazio di archiviazione. Queste funzionalità includono categorie di metriche avanzate, aggregazione dei prefissi, consigli contestuali, report sulle metriche dei prefissi estesi e pubblicazione su Amazon CloudWatch. L'aggregazione a livello di prefisso e i suggerimenti contestuali sono disponibili solo nella console di Amazon S3. Per maggiori informazioni sui prezzi di S3 Storage Lens, consulta i [prezzi di Amazon S3](#).

Categorie di parametri

All'interno dei livelli gratuiti e avanzati, i parametri sono organizzati in categorie in linea con i principali casi d'uso, come l'ottimizzazione dei costi e la protezione dei dati. I parametri gratuiti includono parametri per riepilogo, ottimizzazione dei costi, protezione dei dati, gestione degli accessi, prestazioni ed eventi. Quando esegui l'upgrade al livello avanzato, puoi abilitare l'ottimizzazione avanzata dei costi e le metriche di protezione dei dati. Puoi utilizzare queste metriche avanzate per ridurre ulteriormente i costi di storage S3 e migliorare il tuo livello di protezione dei dati. Puoi anche abilitare i parametri relativi alle attività e quelli relativi ai codici di stato dettagliati per migliorare le prestazioni dei carichi di lavoro delle applicazioni che accedono ai bucket S3. Per ulteriori informazioni sulle categorie di parametri gratuiti e avanzati, consulta [Selezione delle metriche](#).

Puoi valutare la tua archiviazione in base alle best practice S3, ad esempio per analizzare la percentuale di bucket per i quali è abilitata la crittografia o il blocco degli oggetti S3 o la funzionalità S3 di controllo delle versioni. È anche possibile individuare potenziali opportunità di risparmio sui costi. Ad esempio, puoi utilizzare i parametri relativi al conteggio delle regole del ciclo di vita S3 per identificare i bucket senza regole di scadenza o di transizione del ciclo di vita. Puoi anche analizzare l'attività di richiesta per bucket per individuare i bucket in cui gli oggetti possono essere trasferiti a una classe di archiviazione con costi più bassi. Per ulteriori informazioni, consulta [Casi d'uso relativi ai parametri di Amazon S3 Storage Lens](#).

Esportazione delle metriche

Rapporto sulle metriche predefinito

Il rapporto sulle metriche predefinito in S3 Storage Lens include metriche gratuite e metriche di livello avanzato che coprono l'utilizzo dello storage di oggetti e le tendenze delle attività in tutto il tuo.

Account AWS Il rapporto include l'aggregazione dei prefissi per i prefissi i cui oggetti comprendono almeno l'1% dei dati totali archiviati nel bucket e supporta fino a 10 livelli di profondità dei prefissi. Il report può essere esportato giornalmente in formato CSV o in un bucket S3 per uso generico.

Parquet Il report può anche essere inviato a un bucket di tabelle S3 AWS gestito (con nome `aws-s3`), semplificando l'interrogazione tramite servizi di analisi o strumenti di terze parti. AWS

Con il report sulle metriche predefinito, puoi identificare opportunità di ottimizzazione dei costi, ad esempio bucket senza regole S3 Lifecycle per caricamenti multipart incompleti e bucket che non seguono le best practice di protezione dei dati come S3 Replication o S3 Versioning. Il rapporto sulle metriche predefinite fornisce inoltre consigli contestuali per ottimizzare i costi di storage e applicare le best practice di protezione dei dati, senza costi aggiuntivi oltre ai costi di storage standard di S3.

Rapporto esteso sulle metriche dei prefissi

Il report sulle metriche estese dei prefissi di Storage Lens fornisce un'analisi completa a livello di prefisso su tutti i dati di storage S3, ampliando la copertura per supportare miliardi di prefissi nel bucket. Questo rapporto fornisce metriche per tutti i prefissi nei bucket, tra cui l'utilizzo dello spazio di archiviazione, i byte trasferiti, il conteggio delle richieste per codice di stato e le metriche di conformità alla protezione dei dati, che puoi esportare quotidianamente in formato CSV o in formato nel bucket generico S3. Parquet Puoi anche esportare le metriche direttamente nel bucket di tabelle S3 gestito. `aws-s3` AWS

Note

Il report elabora le metriche per prefissi con una profondità massima di 50 livelli ed esclude le metriche a livello di prefisso per qualsiasi bucket in cui le combinazioni di prefisso e classe di archiviazione superano il doppio del numero di oggetti.

Con il report esteso sulle metriche dei prefissi, puoi identificare opportunità di ottimizzazione delle prestazioni, come tassi di errore elevati, oggetti di piccole dimensioni o modelli di richiesta non ottimali, tra miliardi di prefissi nel tuo bucket. A differenza del rapporto sulle metriche predefinito, il rapporto espanso sulle metriche dei prefissi fornisce le metriche relative ai prefissi granulari presenti nel bucket. Ad esempio, puoi identificare i prefissi con un numero elevato di oggetti di dimensioni inferiori a 128 KB per isolare rapidamente tali set di dati per la compattazione che migliorerà le prestazioni delle applicazioni. Questo report è disponibile in tutti i casi Regioni AWS come funzionalità di attivazione nella configurazione avanzata del dashboard di Storage Lens.

Pubblicazione delle metriche

Pubblicazione su Amazon CloudWatch

Puoi pubblicare le metriche di utilizzo e attività di S3 Storage Lens su Amazon CloudWatch per creare una visione unificata dello stato operativo in dashboard. CloudWatch https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html

Puoi anche utilizzare CloudWatch funzionalità, come allarmi e azioni attivate, calcoli matematici e rilevamento delle anomalie, per monitorare e intervenire sulle metriche di S3 Storage Lens. Inoltre, le operazioni CloudWatch API consentono alle applicazioni, compresi i provider di terze parti, di accedere alle metriche di S3 Storage Lens. L'opzione di CloudWatch pubblicazione è disponibile per le dashboard aggiornate al livello avanzato di S3 Storage Lens. Per ulteriori informazioni sul supporto per le metriche di S3 Storage Lens in, consulta. CloudWatch [Monitora le metriche di S3 Storage Lens in CloudWatch](#)

Per ulteriori informazioni sull'utilizzo di S3 Storage Lens, consulta i seguenti argomenti.

Argomenti

- [Informazioni su Amazon S3 Storage Lens](#)
- [Glossario dei parametri di Amazon S3 Storage Lens](#)
- [Impostazione delle autorizzazioni di Amazon S3 Storage Lens](#)
- [Utilizzo di Amazon S3 Storage Lens con la console e l'API](#)
- [Visualizzazione dei parametri con Amazon S3 Storage Lens](#)
- [Utilizzo dei dati di S3 Storage Lens nelle tabelle S3](#)
- [Utilizzo di Amazon S3 Storage Lens con AWS Organizations](#)
- [Operazioni con i gruppi S3 Storage Lens per filtrare e aggregare le metriche](#)

Informazioni su Amazon S3 Storage Lens

Important

Amazon S3 ora applica la crittografia lato server con le chiavi gestite da Amazon S3 (SSE-S3) come livello base di crittografia per ogni bucket in Amazon S3. A partire dal 5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, in S3 Storage Lens, nella

console Amazon S3 e come intestazione di risposta API Amazon S3 aggiuntiva negli SDK and. AWS CLI AWS Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

Amazon S3 Storage Lens è una funzionalità di analisi del cloud-storage che può essere utilizzata per ottenere visibilità a livello di organizzazione sull'utilizzo e l'attività dell'object-storage. È possibile utilizzare i parametri di S3 Storage Lens per generare approfondimenti, ad esempio per scoprire la quantità di spazio di archiviazione disponibile nell'intera organizzazione o quali sono i bucket e i prefissi caratterizzati da una crescita più rapida. Puoi anche utilizzare i parametri di S3 Storage Lens per individuare le opportunità di ottimizzazione dei costi, implementare le best practice di protezione e sicurezza dei dati e migliorare le prestazioni dei carichi di lavoro delle applicazioni. Ad esempio, puoi identificare i bucket che non hanno regole del ciclo di vita S3 per far scadere i caricamenti in più parti incompleti che risalgono a più di 7 giorni. Puoi anche individuare i bucket non conformi alle best practice di protezione dei dati, come quelli che usano la replica S3 o il controllo delle versioni S3. S3 Storage Lens analizza i parametri di archiviazione per fornire raccomandazioni contestuali che puoi usare per ottimizzare i costi di archiviazione e applicare le best practice sulla protezione dei dati.

S3 Storage Lens aggrega i tuoi parametri e mostra le informazioni nella sezione Account snapshot (Snapshot dell'account) nella pagina Buckets (Bucket) della console di Amazon S3. S3 Storage Lens fornisce anche una dashboard interattiva che puoi utilizzare per visualizzare informazioni e tendenze, segnalare valori anomali e ricevere consigli per ottimizzare i costi di storage e applicare le migliori pratiche di protezione dei dati. La dashboard offre opzioni di approfondimento per generare e visualizzare informazioni dettagliate a livello di organizzazione, account, classe di archiviazione, bucket Regione AWS, prefisso o gruppo Storage Lens. Puoi anche inviare un rapporto giornaliero sulle metriche in Parquet formato CSV o a un bucket S3 generico o esportare le metriche direttamente in un bucket di tabelle S3 gestito. AWS Puoi creare e gestire le dashboard di S3 Storage Lens utilizzando la console Amazon S3, (), AWS Command Line Interface gli SDK o l'API REST di Amazon S3. AWS CLI AWS

Concetti e terminologia di S3 Storage Lens

Questa sezione contiene la terminologia e i concetti essenziali per comprendere e utilizzare correttamente Amazon S3 Storage Lens.

Argomenti

- [Configurazione del pannello di controllo](#)
- [Pannello di controllo predefinito](#)

- [Pannelli di controllo](#)
- [Snapshot dell'account](#)
- [Esportazione dei parametri](#)
- [Destinazioni di esportazione delle metriche](#)
- [Regione d'origine](#)
- [Periodo di conservazione](#)
- [Categorie di parametri](#)
- [Raccomandazioni](#)
- [Selezione delle metriche](#)
- [Delimitatore di prefisso](#)
- [S3 Storage Lens e AWS Organizations](#)

Configurazione del pannello di controllo

S3 Storage Lens richiede una configurazione del pannello di controllo contenente le proprietà necessarie per aggregare i parametri per tuo conto per un singolo pannello di controllo o un'esportazione. Quando crei una configurazione, scegli il nome del pannello di controllo e la regione principale, che non puoi modificare successivamente alla creazione del pannello di controllo. Facoltativamente, puoi aggiungere tag e configurare un'esportazione di parametri in formato CSV o Parquet.

Nella configurazione del pannello di controllo, definisci anche l'ambito del pannello e la selezione dei parametri. L'ambito può includere tutto lo spazio di archiviazione per l'account o le sezioni dell'organizzazione filtrati per regione, bucket e account. Quando configuri la selezione delle metriche, puoi scegliere tra metriche di livello gratuito e metriche di livello avanzato, a cui puoi eseguire l'upgrade a un costo aggiuntivo. Con il livello avanzato, puoi accedere a metriche e funzionalità aggiuntive. Queste funzionalità includono categorie di metriche avanzate, aggregazione a livello di prefisso, consigli contestuali e pubblicazione su Amazon CloudWatch. Per maggiori informazioni sui prezzi di S3 Storage Lens, consulta i [prezzi di Amazon S3](#).

Pannello di controllo predefinito

La dashboard predefinita di S3 Storage Lens sulla console è denominato default-account-dashboard. S3 preconfigura questo pannello di controllo per visualizzare le informazioni dettagliate di riepilogo e le tendenze per l'intero account e le aggiorna quotidianamente nella console S3. Non puoi modificare

l'ambito di configurazione della dashboard predefinita, ma puoi aggiornare la selezione delle metriche da metriche di livello gratuito a metriche di livello avanzato. Puoi configurare l'esportazione facoltativa dei parametri o addirittura disabilitare il pannello di controllo. Tuttavia, il pannello di controllo predefinito non può essere eliminato.

Note

Se disabiliti la dashboard predefinita, non viene più aggiornata. Non riceverai più alcun nuovo parametro giornaliero in S3 Storage Lens, nell'esportazione dei parametri o nello snapshot dell'account nella pagina Bucket S3. Se la tua dashboard utilizza metriche avanzate, non ti verrà più addebitato alcun costo. Puoi comunque visualizzare i dati della cronologia nel pannello di controllo fino alla scadenza delle query di dati (14 giorni). Questo periodo è di 15 mesi se hai abilitato le metriche avanzate. Per accedere ai dati della cronologia, puoi riattivare il pannello di controllo entro il periodo di scadenza.

Pannelli di controllo

Puoi creare dashboard S3 Storage Lens aggiuntive e classificarle per Regioni AWS bucket S3 o account (per). AWS Organizations Quando crei o modifichi un pannello di controllo di S3 Storage Lens, ne definisci l'ambito e la selezione dei parametri. S3 Storage Lens offre metriche di livello gratuito e metriche di livello avanzato, a cui puoi effettuare l'upgrade a un costo aggiuntivo. Con le metriche avanzate, puoi accedere a metriche e funzionalità aggiuntive per ottenere informazioni dettagliate sul tuo spazio di archiviazione. Questi includono categorie di metriche avanzate, aggregazione a livello di prefisso, consigli contestuali e pubblicazione su Amazon CloudWatch. Per maggiori informazioni sui prezzi di S3 Storage Lens, consulta i [prezzi di Amazon S3](#).

Puoi anche disabilitare o eliminare i pannelli di controllo. Se disabiliti una dashboard, questa non viene più aggiornata e non riceverai più nuove metriche giornaliere. Puoi comunque visualizzare i dati della cronologia fino al periodo di scadenza di 14 giorni. Se hai abilitato le metriche avanzate per quella dashboard, questo periodo è di 15 mesi. Per accedere ai dati della cronologia, puoi riattivare il pannello di controllo entro il periodo di scadenza.

Se si elimina la dashboard, si perdono tutte le impostazioni di configurazione della dashboard. Non riceverai più nuovi parametri giornalieri e perderai anche l'accesso ai dati della cronologia associati a tale pannello di controllo. Se desideri accedere ai dati della cronologia di un pannello di controllo eliminato, dovrai creare un altro pannello di controllo con lo stesso nome nella stessa regione di origine.

 Note

- S3 Storage Lens può essere utilizzato per creare fino a 50 pannelli di controllo per ogni regione.
- Organization-level Le dashboard possono essere limitate solo a un ambito regionale.

Snapshot dell'account

Lo snapshot dell'account S3 Storage Lens riepiloga i parametri del pannello di controllo predefinito e mostra l'archiviazione totale, il numero di oggetti e la dimensione media degli oggetti nella pagina Buckets (Bucket) della console S3. Questo snapshot dell'account consente di accedere rapidamente a informazioni dettagliate sullo spazio di archiviazione senza dover uscire dalla pagina Buckets (Bucket). Lo snapshot dell'account fornisce anche l'accesso con un clic al pannello di controllo interattivo di S3 Storage Lens.

Puoi utilizzare la dashboard per visualizzare informazioni e tendenze, segnalare valori anomali e ricevere consigli per ottimizzare i costi di storage e applicare le migliori pratiche di protezione dei dati. Nel pannello di controllo sono disponibili opzioni di drill-down per generare informazioni dettagliate a livello di organizzazione, account, bucket, oggetto o prefisso. Puoi anche inviare un'esportazione di parametri una volta al giorno a un bucket S3 in formato CSV o Parquet.

Non è possibile modificare l'ambito del pannello di controllo dell'account predefinito perché è collegato allo snapshot dell'account. Tuttavia, puoi aggiornare la selezione delle metriche nella dashboard dell'account predefinito da metriche gratuite a metriche avanzate a pagamento. Dopo l'aggiornamento, è quindi possibile visualizzare tutte le richieste, i byte caricati e i byte scaricati nello snapshot dell'account S3 Storage Lens.

 Note

In caso di disattivazione del pannello di controllo predefinito, lo snapshot dell'account non viene più aggiornata. Per riprendere la visualizzazione dei parametri nello snapshot dell'account, è possibile riattivare il pannello di controllo dell'account predefinito.

Esportazione dei parametri

Una esportazione dei parametri di S3 Storage Lens è un file che contiene tutti i parametri identificati nella configurazione di S3 Storage Lens. Queste informazioni vengono generate giornalmente in formato CSV o in Parquet formato e vengono inviate a un bucket S3 generico. Puoi anche esportare le metriche direttamente nel bucket di tabelle S3 `aws-s3` AWS gestito, semplificando l'interrogazione utilizzando servizi di analisi o strumenti di terze parti. AWS Puoi utilizzare l'esportazione dei parametri metriche per ulteriori analisi utilizzando lo strumento per i parametri di tua scelta. Il bucket specificato per l'esportazione delle metriche deve trovarsi nella stessa regione della configurazione di S3 Storage Lens. Puoi generare un'esportazione dei parametri di S3 Storage Lens dalla console S3 modificando la configurazione del pannello di controllo. Puoi anche configurare un'esportazione delle metriche utilizzando gli SDK e. AWS CLI AWS

In Storage Lens sono disponibili due tipi di esportazioni di metriche:

- Rapporto sulle metriche predefinite: il rapporto sulle metriche predefinito in S3 Storage Lens include metriche gratuite e tendenze delle attività in tutto il tuo account Account AWS e aggrega le metriche di utilizzo per i prefissi principali.
- Rapporto sulle metriche dei prefissi espansi: il rapporto sulle metriche dei prefissi estesi di Storage Lens fornisce metriche granulari di archiviazione e attività (come l'utilizzo dello spazio di archiviazione, i byte trasferiti e il conteggio delle richieste per codice di stato) a livello di prefisso per ogni prefisso nel bucket. Questo report è interamente disponibile come funzionalità di attivazione, tramite il livello di prezzo avanzato nella configurazione della dashboard di Storage Lens Regioni AWS. Per informazioni sui prezzi delle funzionalità di S3 Storage Lens, consulta i prezzi di [Amazon S3](#).

Note

Storage Lens genera solo metriche per i bucket [S3 per uso generico](#).

Destinazioni di esportazione delle metriche

Quando si esportano i dati delle metriche di Storage Lens, è possibile scegliere sia un bucket S3 generico che un bucket da tavolo S3 come destinazione. I bucket per uso generico offrono un'ampia compatibilità con gli strumenti e le applicazioni esistenti, offrendo la flessibilità necessaria per elaborare i dati all'interno dell'account, utilizzando i servizi di analisi preferiti. Questa opzione supporta modelli di accesso e integrazioni S3 standard per l'analisi dei dati all'interno di singoli bucket

nella tua regione. Al contrario, S3 table bucket consente di eseguire query immediate su più account e regioni, creare dashboard personalizzate con Amazon Quick e unire i dati con altri AWS servizi o strumenti di terze parti, senza la necessità di un'infrastruttura di elaborazione aggiuntiva. Ad esempio, puoi combinare le metriche di Storage Lens con S3 Metadata per analizzare i modelli di attività degli oggetti all'interno dell'organizzazione.

Secchio S3 per uso generico

L'esportazione delle metriche di Storage Lens in un bucket S3 per uso generico offre flessibilità e continuità per l'archiviazione dei dati Storage Lens. È possibile mantenere i flussi di lavoro e la coerenza operativa esistenti continuando a utilizzare l'infrastruttura attuale e i processi di estrazione, trasformazione e caricamento (ETL), gli strumenti di analisi o i flussi di lavoro automatizzati esistenti. I bucket generici funzionano anche con l'intera gamma di AWS servizi e strumenti di terze parti che supportano le API S3 standard. Questo ti offre la massima flessibilità nel modo in cui elabori, analizzi o visualizzi le tue informazioni su Storage Lens. Inoltre, puoi implementare policy sul ciclo di vita di S3 per gestire automaticamente la conservazione dei dati, trasferendo le metriche precedenti a classi di storage a basso costo o eliminandole dopo periodi specifici per ottimizzare i costi. Pertanto, se la continuità operativa e la flessibilità del flusso di lavoro sono le tue priorità per l'implementazione di Storage Lens, valuta la possibilità di scegliere un bucket S3 generico per l'esportazione dei dati di Storage Lens. Per ulteriori informazioni sui prezzi dei bucket generici S3, consulta i prezzi di Amazon S3. <https://aws.amazon.com/s3/pricing>

Bucket da tavolo S3

Quando si esportano le metriche di Storage Lens nel bucket da tavolo S3, è possibile analizzare facilmente le metriche di utilizzo e attività dello storage senza creare pipeline di dati. Le metriche sono organizzate in tabelle S3 create in un bucket di tabelle S3 AWS gestito per garantire prestazioni ottimali delle query, con periodi di conservazione personalizzabili e impostazioni di crittografia aws-s3 per soddisfare le esigenze di gestione dei dati. Con le tue metriche in S3 Tables, puoi eseguire query su più account e regioni utilizzando strumenti e servizi di AWS analisi SQL (come Amazon Athena, Amazon Quick, Amazon EMR e Amazon Redshift) per creare dashboard personalizzate e generare informazioni più approfondite. Ad esempio, puoi unire le metriche di S3 Storage Lens con S3 Metadata per identificare gli oggetti nei prefissi che non mostrano alcuna attività recente. Tutti i dati archiviati in un bucket di tabelle S3 comportano costi per S3 Tables. Per ulteriori informazioni sui prezzi di S3 Tables, consulta i prezzi di Amazon S3. <https://aws.amazon.com/s3/pricing>

Regione d'origine

La regione principale è la regione Regione AWS in cui sono archiviate tutte le metriche di S3 Storage Lens per una determinata configurazione del dashboard. Quando crei la configurazione del pannello di controllo di S3 Storage Lens, dovrai scegliere una regione di origine. Dopo aver scelto una regione di origine, non puoi più cambiarla. Inoltre, se crei un gruppo Storage Lens, ti consigliamo di scegliere la stessa regione del pannello di controllo di Storage Lens.

Note

Come regione di origine puoi scegliere una delle seguenti regioni:

- Stati Uniti orientali (Virginia settentrionale) – us-east-1
- Stati Uniti orientali (Ohio) – us-east-2
- Stati Uniti occidentali (California settentrionale) – us-west-1
- Stati Uniti occidentali (Oregon) – us-west-2
- Asia Pacifico (Mumbai) – ap-south-1
- Asia Pacifico (Seul) - ap-northeast-2
- Asia Pacifico (Singapore) – ap-southeast-1
- Asia Pacifico (Sydney) - ap-southeast-2
- Asia Pacifico (Tokyo) - ap-northeast-1
- Canada (Central) – ca-central-1
- Cina (Pechino): cn-north-1
- Cina (Ningxia): cn-northwest-1
- Europe (Francoforte) – eu-central-1
- Europa (Irlanda) – eu-west-1
- Europe (Londra) – eu-west-2
- Europe (Paris) – eu-west-3
- Europe (Stockholm) – eu-north-1
- Sud America (San Paolo) – sa-east-1

Periodo di conservazione

I parametri di S3 Storage Lens vengono conservati in modo da poter vedere le tendenze cronologiche e confrontare le differenze in termini di archiviazione e attività nel tempo. I parametri di Amazon S3 Storage Lens per le query possono essere utilizzate in modo da poter vedere le tendenze cronologiche e confrontare le differenze nell'utilizzo e nell'attività di archiviazione nel tempo.

Tutti i parametri S3 Storage Lens sono conservati per un periodo di 15 mesi. Tuttavia, i parametri sono disponibili solo per le query per una durata specifica, che dipende dalla [selezione dei parametri](#). Questa durata non può essere modificata. Sono disponibili parametri gratuiti per query per un periodo di 14 giorni, mentre quelli avanzati per query per 15 mesi.

Categorie di parametri

All'interno dei livelli gratuiti e avanzati, i parametri di S3 Storage Lens sono organizzati in categorie in linea con i principali casi d'uso, come l'ottimizzazione dei costi e la protezione dei dati. I parametri gratuiti includono parametri per riepilogo, ottimizzazione dei costi, protezione dei dati, gestione degli accessi, prestazioni ed eventi. Quando esegui l'upgrade a metriche avanzate, puoi abilitare ulteriori metriche di ottimizzazione dei costi e protezione dei dati che puoi utilizzare per ridurre ulteriormente i costi di archiviazione di S3 e garantire la protezione dei dati. Puoi anche abilitare i parametri delle attività e i parametri dei codici di stato dettagliati che puoi utilizzare per migliorare le prestazioni dei flussi di lavoro delle applicazioni.

L'elenco seguente mostra tutte le categorie di parametri gratuiti e avanzati. Per un elenco completo delle singole metriche incluse in ciascuna categoria, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#)

Parametri di riepilogo

I parametri di riepilogo forniscono informazioni generali sull'archiviazione S3, inclusi i byte totali di archiviazione e il conteggio degli oggetti.

Metriche di ottimizzazione dei costi

Le metriche di ottimizzazione dei costi forniscono informazioni utili per gestire e ottimizzare i costi di storage. Ad esempio, puoi identificare i bucket con caricamenti in più parti incompleti che risalgono a più di 7 giorni fa.

Con le metriche avanzate, puoi abilitare metriche avanzate di ottimizzazione dei costi. Questi parametri includono i parametri relativi al conteggio delle regole del ciclo di vita S3 che puoi utilizzare per ottenere i conteggi delle regole del ciclo di vita S3 per ogni bucket.

Data-protection metriche

Data-protection le metriche forniscono informazioni sulle funzionalità di protezione dei dati, come la crittografia e il controllo delle versioni di S3. Puoi utilizzare queste metriche per identificare i bucket che non seguono le best practice di protezione dei dati. Ad esempio, puoi identificare i bucket che non utilizzano la crittografia predefinita con AWS Key Management Service keys (SSE-KMS) o S3 Versioning.

Con le metriche avanzate, puoi abilitare le metriche avanzate di protezione dei dati. Questi parametri includono i parametri relativi al conteggio delle regole di replica per bucket.

Metriche di gestione degli accessi

Le metriche di gestione degli accessi forniscono informazioni dettagliate sulla proprietà degli oggetti S3. Puoi utilizzare questi parametri per visualizzare le impostazioni di Object Ownership usate dai tuoi bucket.

Parametri degli eventi

I parametri degli eventi forniscono approfondimenti relativi alla funzionalità S3 di notifica eventi. Con i parametri degli eventi, puoi vedere in quali bucket è configurata la funzionalità S3 di notifica eventi.

Metriche delle prestazioni

I parametri relativi alle prestazioni forniscono informazioni su Accelerazione del trasferimento Amazon S3 (Amazon S3TA). Con i parametri relativi alle prestazioni, puoi vedere in quali bucket è abilitata la funzionalità di accelerazione del trasferimento.

Parametri delle attività (avanzati)

Se aggiorni la dashboard al livello **Advanced**, puoi abilitare le metriche delle attività. Le metriche delle attività forniscono dettagli su come viene richiesto lo spazio di archiviazione (ad esempio, tutte le richieste, richieste Get, richieste Put), i byte caricati o scaricati e gli errori.

Prefix-level le metriche di attività possono essere utilizzate per aiutarti a determinare quali prefissi vengono utilizzati di rado, in modo da poter [passare a una classe di archiviazione più ottimale utilizzando S3 Lifecycle](#).

Parametri dei codici di stato dettagliati (avanzati)

Se aggiorni la dashboard al livello **Advanced**, puoi abilitare metriche dettagliate sul codice di stato. I parametri relativi ai codici di stato dettagliati forniscono informazioni sui codici di stato HTTP,

come 403 Accesso negato e 503 Servizio non disponibile, che puoi utilizzare per risolvere problemi di accesso o prestazioni. Ad esempio, puoi esaminare il parametro 403 Forbidden error count (Conteggio errori 403 Accesso negato) per identificare i carichi di lavoro che accedono ai bucket senza le autorizzazioni corrette applicate.

Prefix-level le metriche dettagliate del codice di stato possono essere utilizzate per comprendere meglio le occorrenze del codice di stato HTTP per prefisso. Ad esempio, le metriche del conteggio degli errori 503 consentono di identificare i prefissi che ricevono richieste di limitazione (della larghezza di banda della rete) durante l'importazione dei dati.

Advanced cost optimization metrics (Parametri avanzati ottimizzazione costi)

Le metriche avanzate di ottimizzazione dei costi forniscono informazioni dettagliate sulle configurazioni di gestione del ciclo di vita di S3 per aiutarvi a ottimizzare i costi di storage attraverso transizioni ed eliminazioni automatizzate dei dati. Queste metriche tracciano il numero di regole del ciclo di vita configurate in diversi tipi di regole del ciclo di vita. Puoi utilizzare queste metriche per garantire una copertura completa delle regole del ciclo di vita in tutti i bucket e identificare le opportunità per implementare ulteriori strategie di ottimizzazione dei costi attraverso la gestione automatizzata dei dati.

Advanced data protection metrics (Parametri avanzati protezione dati)

Le metriche avanzate di protezione dei dati ti aiutano a proteggere i tuoi dati fornendo informazioni dettagliate sul conteggio delle regole di replica, sull'utilizzo della SSE-KMS crittografia e sulle vulnerabilità di sicurezza come firme non supportate e richieste TLS. (Nota: le metriche sul conteggio delle regole di replica non sono disponibili per i prefissi.)

Questa visibilità consente di garantire una corretta ridondanza dei dati, convalidare la conformità alla crittografia, identificare i rischi di sicurezza derivanti da protocolli obsoleti, risolvere gli errori di configurazione delle repliche e mantenere solide strategie di protezione dei dati a livello di organizzazione, account e bucket.

Metriche prestazionali avanzate

Le metriche avanzate delle prestazioni rivelano come le applicazioni interagiscono con i dati in S3 e possono aiutare a identificare le opportunità per ottimizzare le prestazioni delle applicazioni, ad esempio I/O modelli inefficienti, accesso interregionale e numero di accessi univoci agli oggetti. Le metriche prestazionali avanzate di Storage Lens eliminano la necessità di costosi strumenti di monitoraggio personalizzati e consentono ai clienti di implementare le best practice di S3 in modo più efficace, in particolare a vantaggio delle applicazioni sensibili alle prestazioni come la formazione

sull'apprendimento automatico, l'analisi dei dati e altri carichi di lavoro di elaborazione ad alte prestazioni.

Raccomandazioni

S3 Storage Lens fornisce raccomandazioni automatizzate per ottimizzare lo storage. Le raccomandazioni vengono posizionate contestualmente insieme ai parametri pertinenti nel pannello di controllo di S3 Storage Lens. I dati della cronologia non sono idonei per le raccomandazioni in quanto le raccomandazioni sono rilevanti per quanto sta accadendo nel periodo più recente. I suggerimenti appaiono solo quando sono rilevanti.

Le raccomandazioni di S3 Storage Lens sono disponibili nelle seguenti forme:

- **Suggerimenti**

I suggerimenti segnalano le tendenze relative allo storage e alle attività che potrebbero indicare un'opportunità di ottimizzazione dei costi di storage o una best practice per la protezione dei dati. Per maggiori dettagli sulle regioni, i bucket o i prefissi specifici, consulta gli argomenti riportati nella Guida per l'utente di Amazon S3 e nel pannello di controllo di S3 Storage Lens.

- **Call-outs**

Call-outs sono consigli che segnalano anomalie interessanti nello storage e nell'attività per un periodo che potrebbero richiedere ulteriore attenzione o monitoraggio.

- **Callout anomalie**

S3 Storage Lens fornisce callout per i parametri che sono valori anomali, in base alla recente tendenza di 30 giorni. L'anomalia viene calcolata utilizzando un punteggio standard, noto anche come z-score. Per ottenere questo punteggio, il parametro del giorno corrente viene sottratto dalla media dei valori del parametro degli ultimi 30 giorni. Il valore del parametro del giorno corrente viene quindi diviso per la deviazione standard di tale parametro negli ultimi 30 giorni. Il punteggio risultante è solitamente compreso tra -3 e +3. Questo numero rappresenta il numero di deviazioni standard che il parametro del giorno corrente rappresenta dalla media.

S3 Storage Lens considera i parametri con un punteggio >2 o <-2 come valori anomali perché sono superiori o inferiori al 95% dei dati normalmente distribuiti.

- **Callout delle modifiche significative**

Il callout delle modifiche significative si applica ai parametri che dovrebbero cambiare meno frequentemente. Pertanto, è impostato su una sensibilità più elevata rispetto al calcolo dei valori

anomali, che in genere è compreso tra +/- 20 percento rispetto al giorno, alla settimana o al mese precedenti.

Risoluzione dei callout relativi ad archiviazione e utilizzo: se ricevi un callout di modifica significativa, non si tratta necessariamente di un problema. Tale call-out potrebbe essere il risultato di una modifica dell'archiviazione prevista. Ad esempio, è possibile che di recente sia stato aggiunto un numero elevato di nuovi oggetti, eliminato un numero elevato di oggetti o apportate modifiche pianificate.

Se nel pannello di controllo viene visualizzato un callout di modifica significativa, prendine nota e determina se può essere spiegata dalle circostanze recenti. In caso contrario, utilizza il pannello di controllo di S3 Storage Lens per espandere ulteriori dettagli per comprendere le regioni, i bucket o i prefissi specifici che determinano la fluttuazione.

- Promemoria

I promemoria forniscono informazioni dettagliate sul funzionamento di Amazon S3. Possono aiutarti a saperne di più sulle modalità di utilizzo delle funzionalità S3 per ridurre i costi di storage o applicare best practice per la protezione dei dati.

Selezione delle metriche

S3 Storage Lens offre due selezioni di metriche che puoi scegliere per la dashboard e l'esportazione: livello gratuito e livello avanzato.

- Piano gratuito

S3 Storage Lens offre parametri gratuiti per tutti i pannelli di controllo e le configurazioni. I parametri gratuiti contengono dati rilevanti per l'archiviazione, come il numero di bucket e gli oggetti nel tuo account. Le metriche gratuite includono anche metriche basate sui casi d'uso (ad esempio, ottimizzazione dei costi e metriche di protezione dei dati) che puoi utilizzare per verificare se lo storage è configurato secondo le best practice di S3. Tutte le metriche del livello gratuito vengono raccolte giornalmente e possono essere esportate in un bucket S3 generico (CSV o formato) o Parquet in un bucket da tabella S3 (solo formato). Parquet I dati sono disponibili per le interrogazioni per 14 giorni nella console Amazon S3. Per ulteriori informazioni sui parametri disponibili con i parametri gratuiti, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

- Livello avanzato

S3 Storage Lens offre metriche gratuite per tutte le dashboard e le configurazioni con la possibilità di passare a metriche avanzate. Si applicano costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Le metriche di livello avanzato includono tutte le metriche delle metriche gratuite insieme a metriche aggiuntive, come metriche avanzate di protezione dei dati e ottimizzazione dei costi, metriche delle attività e metriche dettagliate sui codici di stato. Le metriche di livello avanzato forniscono anche consigli per aiutarti a ottimizzare lo spazio di archiviazione. Le raccomandazioni vengono posizionate contestualmente insieme ai parametri pertinenti nel pannello di controllo.

Il livello avanzato include le seguenti funzionalità:

- **Categorie di metriche avanzate:** genera metriche aggiuntive. Per un elenco completo delle categorie di parametri avanzati, consulta [Categorie di parametri](#). Per un elenco completo di parametri, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).
- **CloudWatch Pubblicazione su Amazon:** pubblica le metriche di S3 Storage Lens per CloudWatch creare una visione unificata dello stato operativo nelle dashboard. CloudWatch https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html
Puoi anche utilizzare le operazioni e le funzionalità delle CloudWatch API, come allarmi e azioni attivate, calcoli matematici e rilevamento delle anomalie, per monitorare e intervenire sulle metriche di S3 Storage Lens. Per ulteriori informazioni, consulta [Monitora le metriche di S3 Storage Lens in CloudWatch](#).
- **Rapporto sulle metriche predefinite:** il rapporto sulle metriche predefinito in S3 Storage Lens include metriche gratuite e funzionalità di aggregazione dei prefissi per i principali prefissi per l'utilizzo dello storage di oggetti e le tendenze delle attività in tutto il tuo Account AWS. Con il report sulle metriche predefinito, puoi identificare le opportunità di ottimizzazione dei costi senza costi aggiuntivi oltre ai costi di storage standard di S3.
- **Rapporto sulle metriche dei prefissi esteso:** il rapporto sulle metriche dei prefissi espansi di Storage Lens fornisce un'analisi completa a livello di prefisso su tutti i dati di storage S3, ampliando la copertura per supportare fino a miliardi di prefissi per bucket.
- **Aggregazione di metriche aggiuntive**
 - **Aggregazione di prefisso:** raccoglie i parametri a livello di [prefisso](#). Questa impostazione specifica i prefissi aggregati come parte del rapporto sulle metriche predefinito, visualizzato nella dashboard di Storage Lens. Tieni presente che le metriche applicabili a livello di prefisso sono disponibili con l'aggregazione dei prefissi, ad eccezione delle impostazioni a livello di

bucket e delle metriche di conteggio delle regole. Prefix-level le metriche non si applicano all'esportazione delle metriche con prefissi espansi e non vengono pubblicate in CloudWatch

- **Aggregazione dei gruppi Storage Lens:** raccoglie i parametri a livello di gruppo Storage Lens. Dopo aver abilitato le metriche di livello avanzato e l'aggregazione dei gruppi Storage Lens, puoi specificare quali gruppi Storage Lens includere o escludere dalla dashboard di Storage Lens. Devi specificare almeno un gruppo Storage Lens. I gruppi Storage Lens specificati devono inoltre risiedere nella regione di origine designata nell'account del pannello di controllo. Le metriche a livello di gruppo di Storage Lens non vengono pubblicate su CloudWatch

Tutti i parametri avanzati vengono raccolti quotidianamente. I dati sono disponibili per l'interrogazione per un massimo di 15 mesi nella console Amazon S3. Per ulteriori informazioni sui parametri di archiviazione aggregati da S3 Storage Lens, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

Delimitatore di prefisso

I delimitatori di prefisso determinano il modo in cui Storage Lens conta la profondità del prefisso, separando i livelli gerarchici all'interno delle chiavi degli oggetti. È possibile specificare un solo carattere per indicare ogni livello all'interno dei prefissi. Se il delimitatore del prefisso non è definito, Amazon S3 utilizza "/" come delimitatore predefinito. /

Note

Quando aggiorni la configurazione del dashboard di Storage Lens tramite l'API, il delimitatore e il delimitatore di prefisso aggiornato devono essere definiti allo stesso modo, altrimenti riceverai un errore. Il delimitatore si applica solo alle metriche a livello di prefisso esportate nel rapporto sulle metriche predefinito. Il delimitatore di prefisso si applica a tutti i prefissi esportati nel report espanso sulle metriche dei prefissi.

S3 Storage Lens e AWS Organizations

AWS Organizations è una soluzione Servizio AWS che ti aiuta ad aggregare tutte le tue gerarchie organizzative Account AWS in un'unica gerarchia. Amazon S3 Storage Lens funziona con Amazon S3 AWS Organizations per fornire una visione unica dello storage di oggetti e delle attività nello storage Amazon S3.

Per ulteriori informazioni, consulta [Utilizzo di Amazon S3 Storage Lens con AWS Organizations](#).

- Accesso attendibile

Utilizzando l'account di gestione dell'organizzazione, devi abilitare l'accesso attendibile per S3 Storage Lens per aggregare i parametri di archiviazione e i dati di utilizzo per tutti gli account membri dell'organizzazione. Puoi quindi creare pannelli di controllo o esportazioni per l'organizzazione utilizzando l'account di gestione o assegnando l'accesso da amministratore delegato ad altri account dell'organizzazione.

Puoi disabilitare l'accesso attendibile per S3 Storage Lens in qualsiasi momento, evitando che S3 Storage Lens aggregi i parametri per la tua organizzazione.

- Amministratore delegato

Puoi creare dashboard e metriche per S3 Storage Lens per la tua organizzazione utilizzando il tuo account di AWS Organizations gestione o concedendo l'accesso di amministratore delegato ad altri account della tua organizzazione. Puoi annullare la registrazione degli amministratori delegati in qualsiasi momento. Questa azione interrompe automaticamente tutti i pannelli di controllo a livello di organizzazione creati dall'amministratore delegato dall'aggregazione di nuovi parametri di archiviazione.

Per maggiori informazioni, consulta [Amazon S3 Storage Lens e AWS Organizations](#) nella Guida per l'utente di AWS Organizations .

Ruoli collegati ai servizi per Amazon S3 Storage Lens

Oltre all'accesso AWS Organizations affidabile, Amazon S3 Storage Lens utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a S3 Storage Lens. Service-linked i ruoli sono predefiniti da S3 Storage Lens e includono tutte le autorizzazioni necessarie per raccogliere le metriche giornaliere di archiviazione e attività dagli account dei membri dell'organizzazione.

Per ulteriori informazioni, consulta [Utilizzo dei ruoli collegati ai servizi per Amazon S3 Storage Lens](#).

Glossario dei parametri di Amazon S3 Storage Lens

Il glossario dei parametri di Amazon S3 Storage Lens fornisce un elenco completo di parametri gratuiti e avanzati per S3 Storage Lens.

S3 Storage Lens offre parametri gratuiti per tutti i pannelli di controllo e le configurazioni con la possibilità di eseguire l'aggiornamento ai parametri avanzati.

- I parametri gratuiti contengono dati rilevanti per l'utilizzo dell'archiviazione, come il numero di bucket e gli oggetti nel tuo account. I parametri gratuiti includono anche parametri basati sui casi d'uso, come quelli relativi all'ottimizzazione dei costi e alla protezione dei dati. Tutti i parametri gratuiti vengono raccolti quotidianamente e i dati sono disponibili per le query per un massimo di 14 giorni.
- Le metriche avanzate includono tutte le metriche delle metriche gratuite insieme a metriche aggiuntive, come prestazioni avanzate, protezione avanzata dei dati e metriche avanzate di ottimizzazione dei costi. I parametri avanzati includono anche categorie di parametri aggiuntive, come i parametri di attività e i parametri dettagliati relativi al codice di stato. I dati dei parametri avanzati sono disponibili per le query per 15 mesi.

Per l'uso di S3 Storage Lens con le raccomandazioni e i parametri avanzati sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sui parametri avanzati e sulle funzioni di suggerimento, consulta [Selezione delle metriche](#).

Note

Per i gruppi Storage Lens sono disponibili solo i parametri di archiviazione del piano gratuito. I parametri di livello avanzato non sono disponibili a livello di gruppo Storage Lens.

Nomi dei parametri

Nella colonna Nome parametro nella tabella seguente è riportato il nome di ogni parametro S3 Storage Lens nella console S3. La colonna CloudWatch ed esportazione fornisce il nome di ogni metrica in Amazon CloudWatch e il file di esportazione delle metriche che puoi configurare nella dashboard di S3 Storage Lens.

Formule dei parametri derivati

Le metriche derivate non sono disponibili per l'esportazione delle metriche e l'opzione di pubblicazione. CloudWatch Puoi tuttavia usare le formule dei parametri riportate nella colonna Formule dei parametri derivati per calcolarli.

Interpretazione dei simboli dei prefissi per multipli di unità delle metriche di Amazon S3 Storage Lens (K, M, G e così via)

I multipli di unità di parametri di S3 Storage Lens sono scritti con simboli di prefisso. Questi simboli di prefisso sono rappresentati tramite i simboli del Sistema di unità internazionale (SI) standardizzati

dall'International Bureau of Weights and Measures (BIPM). Vengono inoltre utilizzati nel codice unificato per le unità di misura (UCUM). Per ulteriori informazioni, consulta [Elenco dei simboli dei prefissi SI](#).

 Note

- L'unità di misura per i byte di archiviazione S3 è espressa in gigabyte binari (GB), dove 1 GB è pari a 2³⁰ byte, 1 TB a 2⁴⁰ byte e 1 PB a 2⁵⁰ byte. Questa unità di misura è nota anche come gibibyte (GiB), come definito dalla Commissione elettrotecnica internazionale (IEC).
- Quando un oggetto raggiunge la fine del suo ciclo di vita in base alla relativa configurazione, Amazon S3 lo aggiunge alla coda degli oggetti da eliminare e lo rimuove in modo asincrono. Deve pertanto esistere un ritardo tra la data di scadenza dell'oggetto e la data in cui Amazon S3 rimuove tale oggetto. S3 Storage Lens non include i parametri per gli oggetti scaduti e non ancora rimossi. Per ulteriori informazioni sulle operazioni di scadenza nel ciclo di vita S3, consulta [Oggetti in scadenza](#).
- Amazon S3 archivia i metadati (chiave dell'oggetto, timestamp, ecc.) per ogni oggetto, che richiede uno spazio di archiviazione minimo anche per file di dati da 0 KB. Questo è il motivo per cui gli oggetti da 0 KB vengono visualizzati nell'intervallo di dimensioni (0KB-128KB) in S3 Storage Lens.
- S3 Storage Lens consente di tracciare al meglio i trasferimenti di dati tra regioni, concentrandosi principalmente sulle richieste provenienti da risorse gestite dal cliente come le istanze EC2. Le richieste effettuate tramite AWS PrivateLink o determinate richieste interne non sono classificate.

La tabella seguente mostra il glossario delle metriche di S3 Storage Lens.

Nome parametro	CloudWatch ed esporta	Description	Live	Cate ²	D	Form para deriv	Gruppi Storage Lens
Archiviazione totale	StorageBytes	Archiviazione totale, inclusi i caricamenti multiparte	Grat	Riep	N	-	Y

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Formato per derivare	Gruppi Storage Lens	
		incompleti, i metadati degli oggetti e gli indicatori di eliminazione						
Object count (Conteggio oggetti)	ObjectCount	Numero totale di oggetti comprensivo della versione corrente, delle versioni non correnti, dei caricamenti multiparte incompleti e degli indicatori di eliminazione	Grat	Riep	N	-	Y	
Dimensione media degli oggetti	-	Dimensione media degli oggetti	Grat	Riep	Y	sum() / sum() Storage Object nt	Y	
Active buckets (Bucket attivi)	-	Numero di bucket con spazio di archiviazione > 0 byte	Grat	Riep	Y	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria ²	D	Forma per deriv	Gruppi Storage Lens	
Bucket	-	Numero di bucket	Grat	Riep	Y	-	Y	
Account	-	Numero di account il cui spazio di archiviazione rientra nell'ambito	Grat	Riep	Y	-	Y	
Current version bytes (Byte versione corrente)	CurrentVersionStorageBytes	Numero di byte che rappresentano la versione corrente di un oggetto	Grat	Ottir zion dei cost	N	-	Y	
% current version bytes (% byte versione corrente)	-	Percentuale di byte nell'ambito che rappresentano le versioni correnti degli oggetti	Grat	Ottir zion dei cost	Y	sum (CurrentStorage) / sum (Storage)	Y	
Conteggio oggetti versione corrente	CurrentVersionObjectCount	Numero di oggetti della versione corrente, inclusi gli indicatori di eliminazione correnti	Grat	Prote dei dati	N	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens	
% current version objects (% oggetti versione corrente)	-	Percentuale di oggetti nell'ambito che sono una versione corrente	Grat	Ottir zion dei cost	Y	sum (CurrentObjectCount)	Y	
Byte di versione non correnti	NonCurrentVersionStorageBytes	Numero di byte della versione non corrente	Grat	Ottir zion dei cost	N	-	Y	
% noncurrent version bytes (% byte versione non corrente)	-	Percentuale di byte nell'ambito che sono versioni non correnti	Grat	Ottir zion dei cost	Y	sum (NonCurrentVersionStorageBytes)	Y	
Conteggio di oggetti versione non corrente	NonCurrentVersionObjectCount	Numero delle versioni degli oggetti non correnti, inclusi gli indicatori di eliminazione non correnti	Grat	Ottir zion dei cost	N	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens	
% noncurrent version objects (% oggetti versione non corrente)	-	Percentuale di oggetti nell'ambito che sono una versione non corrente	Grat	Ottir zion dei cost	Y	sum (NonntVe Object) / sum () Object	Y	
Delete marker bytes (Byte contrassegni di eliminazione)	DeleteMarkerStorageBytes	Numero di byte nell'ambito che sono indicatori di eliminazione	Grat	Ottir zion dei cost	N	-	Y	
% delete marker bytes (% byte contrassegni di eliminazione)	-	Percentuale di byte nell'ambito che sono indicatori di eliminazione	Grat	Ottir zion dei cost	Y	sum (DeleteMarkerBytes) / sum () Storage	Y	
Conteggio oggetti contrassegno di eliminazione	DeleteMarkerObjectCount	Numero di oggetti con un indicatore di eliminazione, correnti e non correnti	Grat	Ottir zion dei cost	N	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens	
% delete marker objects (% oggetti contrassegnati di eliminazione)	-	Percentuale di oggetti inclusi nell'ambito con un indicatore di eliminazione	Grat	Ottir zion dei cost	Y	sum (DeleteMarkerCount) Object	Y	
Byte con caricamento in più parti incompleto	IncompleteMultipartUploadStorageBytes	Numero totale di byte utilizzabili per i caricamenti multipart incompleti	Grat	Ottir zion dei cost	N	-	Y	
% incomplete multipart upload bytes (% byte caricamenti in più parti incompleti)	-	Percentuale di byte nell'ambito che sono il risultato di caricamenti multipart incompleti	Grat	Ottir zion dei cost	Y	sum (IncompleteMultipartUploads) / sum (Storage) Storages	Y	
Conteggio di oggetti con caricamento in più parti incompleto	IncompleteMultipartUploadObjectCount	Numero di oggetti inclusi nell'ambito che sono caricamenti multipart incompleti	Grat	Ottir zion dei cost	N	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per derivare	Gruppi Storage Lens	
% incomplete multipart upload objects (% oggetti caricamenti in più parti incompleti)	-	Percentuale di oggetti nell'ambito che sono caricamenti multiparte incompleti	Gratuito	Ottimizzazione dei costi	Y	sum (IncompleteMultipartUploadObjects) / sum (Objects)	Y	
Incomplete multipart upload storage bytes greater than 7 days old (Byte archiviazione caricamenti in più parti incompleti risalenti a più di 7 giorni)	IncompleteMultipartUploadStorageBytesOlderThan7Days	Byte totali relativi ai caricamenti multiparte incompleti che risalgono a più di 7 giorni	Gratuito	Ottimizzazione dei costi	N	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens	
% incomplete multipart upload storage bytes greater than 7 days old (% byte archiviazione caricamenti in più parti incompleti risalenti a più di 7 giorni)	-	Percentuale di byte per i caricamenti multiparte incompleti che risalgono a più di 7 giorni	Grat	Ottimizzazione dei costi	Y	summary (Includete Metadata- Days: summary) Storages	Y	
Incomplete multipart upload object count greater than 7 days old (Conteggio oggetti caricamenti in più parti incompleti risalenti a più di 7 giorni)	IncompleteMPUObjectCountOlderThan7Days	Numero di oggetti caricati in più parti incompleti risalenti a più di 7 giorni fa	Grat	Ottimizzazione dei costi	N	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma deriv	Gruppi Storage Lens	
% incomplete multipart upload object count greater than 7 days old (% conteggio oggetti caricamenti in più parti incompleti risalenti a più di 7 giorni)	-	Percentuale di oggetti caricati in più parti incompleti da più di 7 giorni	Grat	Ottir zion dei cost	Y	sum (Inco teMf ctCc derT ays) sum () Obje nt	Y	
Transition lifecycle rule count (Conteggio regole ciclo di vita transizione)	TransitionLifecycleRuleCount	Numero di regole del ciclo di vita per la transizione degli oggetti in un'altra classe di archiviazione	Avar	Ottir zion dei cost	N	-	N	
Average transition lifecycle rules per bucket (Media regole ciclo di vita transizioni per bucket)	-	Numero medio di regole del ciclo di vita per la transizione degli oggetti in un'altra classe di storage	Avar	Ottir zion dei cost	Y	sum (Tra onLi leRu nt) / sum () Disti umb cket	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per derivare	Gruppi Storage Lens
Expiration lifecycle rule count (Conteggio regole ciclo di vita scadenza)	ExpirationLifecycleRuleCount	Numero di regole del ciclo di vita per far scadere gli oggetti	Average	Ottimizzazione dei costi	No	-	No
Average expiration lifecycle rules per bucket (Media regole ciclo di vita scadenza per bucket)	-	Numero medio di regole del ciclo di vita per far scadere gli oggetti	Average	Ottimizzazione dei costi	Yes	sum (ExpirationLifecycleRuleCount) / Distinct bucket	No
Noncurrent version transition lifecycle rule count (Conteggio regole ciclo di vita transizione versioni non correnti)	NoncurrentVersionTransitionLifecycleRuleCount	Numero di regole del ciclo di vita per la transizione delle versioni non correnti degli oggetti a un'altra classe di archiviazione	Average	Ottimizzazione dei costi	No	-	No

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	Dati	Formato per derivare	Gruppi Storage Lens	
Average noncurrent version transition lifecycle rules per bucket (Media regole ciclo di vita transizioni versioni non correnti per bucket)	-	Numero medio di regole del ciclo di vita per la transizione delle versioni non correnti degli oggetti a un'altra classe di storage	Average	Ottimizzazione dei costi	Yes	sum (Normalized TransitionLifeCycleRuleCount) / sum () Distribution bucket	N	
Noncurrent version expiration lifecycle rule count (Conteggio regole ciclo di vita scadenza versioni non correnti)	NoncurrentVersionExpiration LifecycleRuleCount	Numero di regole del ciclo di vita per le quali scadono le versioni non correnti degli oggetti	Average	Ottimizzazione dei costi	No	-	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	Dati	Formato per derivare	Gruppi Storage Lens
Average noncurrent version expiration lifecycle rules per bucket (Media regole ciclo di vita scadenza versioni non correnti per bucket)	-	Numero medio di regole del ciclo di vita con cui scadono le versioni non correnti degli oggetti	Average	Ottimizzazione dei costi	Yes	summary / summary NoncurrentVersionExpirationLifecycleRuleDistribution bucket	N
Abort incomplete multipart upload lifecycle rule count (Conteggio regole ciclo di vita interruzioni caricamenti in più parti incompleti)	AbortIncompleteMultipartLifecycleRuleCount	Numero di regole del ciclo di vita per eliminare i caricamenti multipart incompleti	Average	Ottimizzazione dei costi	No	-	N

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens
Average abort incomplete multipart upload lifecycle rules per bucket (Media interruzioni regole ciclo di vita caricamenti in più parti incompleti per bucket)	-	Numero medio di regole del ciclo di vita per eliminare i caricamenti multiparte incompleti	Average	Ottimizzazione dei costi	Yes	sum() / sum() Abort incomplete Lifecycle Rule Distribution bucket	N
Expired object delete marker lifecycle rule count (Conteggio regole ciclo di vita contrassegni di eliminazione oggetti scaduti)	ExpiredObjectDeleteMarkerLifecycleRuleCount	Numero di regole del ciclo di vita per rimuovere i marker di eliminazione di oggetti scaduti	Average	Ottimizzazione dei costi	No	-	N

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	Dati	Forma per deriv	Gruppi Storage Lens	
Average expired object delete marker lifecycle rules per bucket (Media regole ciclo di vita contrassegni di eliminazione oggetti scaduti per bucket)	-	Numero medio di regole del ciclo di vita per rimuovere gli indicatori di eliminazione di oggetti scaduti	Average	Ottimizzazione dei costi	Yes	summary() / summary() ExpiredObjectLifecycleDistributionBucket	N	
Total lifecycle rule count (Conteggio totale regole ciclo di vita)	TotalLifecycleRuleCount	Numero di regole del ciclo di vita	Average	Ottimizzazione dei costi	No	-	N	
Average lifecycle rule count per bucket (Media conteggio regole ciclo di vita per bucket)	-	Numero medio di regole del ciclo di vita	Average	Ottimizzazione dei costi	Yes	summary(TotalLifecycleRuleCountSummary()) DistributionBucket	N	
Encrypted bytes (Byte crittografati)	EncryptedStorageBytes	Numero di byte crittografati	Gratuito	Protezione dei dati	No	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	Dimensione	Formato per derivare	Gruppi Storage Lens	
% encrypted bytes (% byte crittografati)	-	Percentuale di byte totali crittografati	Gratuito	Protezione dei dati	Y	sum (EncryptedStorageBytes) / (sum (StorageBytes) - sum (DeletedStorageBytes))	Y	
Encrypted object count (Conteggi o oggetti crittografati)	Encrypted ObjectCount	Numero di oggetti crittografati	Gratuito	Protezione dei dati	N	-	Y	
% encrypted objects (% oggetti crittografati)	-	Percentuale di oggetti crittografati	Gratuito	Protezione dei dati	Y	sum (EncryptedObjectCount) / (sum (ObjectCount) - sum (DeletedObjectCount))	Y	

Nome parametro	CloudWatch ed esporta	Description	Live	Cate 2	D	Form para deriv	Gruppi Storage Lens	
Unencrypted bytes (Byte non crittografati)	-	Numero di byte non crittografati	Grat	Prot e dei dati	Y	sum (Sto ytes - sum (Del rker: geBy - sum () Encr Stor tes	Y	
% unencrypt ed bytes (% byte non crittografati)	-	Percentuale di byte non crittografati	Grat	Prot e dei dati	Y	sum (Un tedS eByl (sum (Sto ytes - sum (Del rker: geBy	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per deriv	Gruppi Storage Lens	
Unencrypted object count (Conteggio oggetti non crittografati)	-	Numero di oggetti non crittografati	Grat	Prote dei dati	Y	sum (Obj unt) - sum (Dele rker tCou - sum (Enc dOb unt)	Y	
% unencrypted objects (% oggetti non crittografati)	-	Percentuale di oggetti non crittografati	Grat	Prote dei dati	Y	sum (Un tedC Cou (s um (Obj unt) - sum (Dele rker tCou	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per deriv	Gruppi Storage Lens	
Replicated storage bytes source (Origine byte di archiviazione replicati)	ReplicatedStorageBytesSource	Numero di byte che vengono replicati dal bucket di origine	Gratuito	Protezione dei dati	No	-	Y	
% replicated bytes source (% origine byte replicati)	-	Percentuale di byte totali replicati dal bucket di origine	Gratuito	Protezione dei dati	Sì	sum (ReplicatedStorageBytesSource) / sum (StorageBytes)	Y	
Replicated object count source (Origine conteggio oggetti replicati)	ReplicatedObjectCountSource	Numero di oggetti replicati dal bucket di origine	Gratuito	Protezione dei dati	No	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Category	Default	Forma per derivare	Gruppi Storage Lens	
% replicated objects source (% origine oggetti replicati)	-	Percentuale del totale degli oggetti replicati dal bucket di origine	Grat	Protezione dei dati	Y	sum (ReplicatedObjectCount) / sum (ObjectCount)	Y	
Destinazione dei byte di archiviazione replicati	ReplicatedStorageBytes	Numero di byte replicati nel bucket di destinazione	Grat	Protezione dei dati	N	-	N	
% replicated bytes destination (% destinazione byte replicati)	-	Percentuale di byte totali replicati nel bucket di destinazione	Grat	Protezione dei dati	Y	sum (ReplicatedStorageBytes) / sum (StorageBytes)	Y	
Replicated object count destination (Destinazione conteggio oggetti replicati)	ReplicatedObjectCount	Numero di oggetti replicati nel bucket di destinazione	Grat	Protezione dei dati	N	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens	
% replicate d objects destination (% destinazione oggetti replicati)	-	Percentuale del totale degli oggetti replicati nel bucket di destinazione	Grat	Protezione dei dati	Y	sum (ReplicatedObjectCount)	Y	
Object Lock bytes (Byte blocco oggetti)	ObjectLockEnabledStorageBytes	Numero di byte di archiviazione abilitati per Object Lock	Grat	Protezione dei dati	N	-	Y	
% Object Lock bytes (% byte blocco oggetti)	-	Percentuale di byte di archiviazione abilitati per Object Lock	Grat	Protezione dei dati	Y	sum (ObjectLockEnabledStorageBytes)	Y	
Object Lock object count (Conteggio oggetti con blocco oggetti)	ObjectLockEnabledObjectCount	Numero di oggetti Object Lock	Grat	Protezione dei dati	N	-	Y	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma derivata	Gruppi Storage Lens	
% Object Lock objects (% oggetti blocco oggetti)	-	Percentuale del totale degli oggetti con Blocco oggetti abilitato	Grat	Protezione dei dati	Y	sum (ObjectLockEnabledObjectSum())	Y	
Versioning-enabled numero di secchi	VersioningEnabledBucketCount	Numero di bucket con S3 Versioning abilitato	Grat	Protezione dei dati	N	-	N	
% versioning-enabled buckets (% bucket con controllo delle versioni abilitato)	-	Percentuale di bucket con S3 Versioning abilitato	Grat	Protezione dei dati	Y	sum (VersioningEnabledBucketSum())	N	
MFA delete-enabled bucket count (Conteggio bucket con eliminazione MFA abilitata)	MFADeleteEnabledBucketCount	Numero di bucket con cancellazione MFA (autenticazione a più fattori) abilitata	Grat	Protezione dei dati	N	-	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per deriv	Gruppi Storage Lens	
% MFA delete-enabled bucket count (% conteggio bucket con eliminazione MFA abilitata)	-	Percentuale di bucket con l'eliminazione MFA (autenticazione a più fattori) abilitata	Grat	Protezione dei dati	Y	sum (MFA delete-enabled bucket) / sum ()	Distriumbucket	
SSE-KMS conteggio dei bucket abilitato	SSEKMSEnableBucketCount	Numero di bucket che utilizzano la crittografia lato server con AWS Key Management Service keys (SSE-KMS) per la crittografia predefinita	Grat	Protezione dei dati	N	-	N	
% SSE-KMS di bucket abilitati	-	Percentuale di bucket utilizzati a SSE-KMS per la crittografia predefinita	Grat	Protezione dei dati	Y	sum (SSE-enabled bucketCount) / sum ()	Distriumbucket	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	Dati	Forma per deriv	Gruppi Storage Lens	
All unsupported signature requests (Tutte le richieste di firma non supportate)	AllUnsupportedSignatureRequests	Numero totale di richieste che utilizzano versioni di firma non supportate AWS	Availability	Protection	No	-	No	
% all unsupported signature requests (% tutte le richieste di firma non supportate)	-	Percentuale di richieste che utilizzano versioni di firma non supportate AWS	Availability	Protection	Yes	sum (AllUnsupportedSignatureRequests)	No	
All unsupported TLS requests (Tutte le richieste TLS non supportate)	AllUnsupportedTLRequests	Numero totale di richieste che utilizzano versioni TLS (Transport Layer Security) non supportate	Availability	Protection	No	-	No	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens	
% all unsupported TLS requests (% tutte le richieste TLS non supportate)	-	Percentuale di richieste che utilizzano versioni TLS non supportate	Avanzato	Protezione dei dati	Y	sum (AllRequestsUnsupportedTLSRequests)	N	
Tutte le richieste SSE-KMS	AllSSEKMSRequests	Numero totale di richieste che specificano SSE-KMS	Avanzato	Protezione dei dati	N	-	N	
% tutte le SSE-KMS richieste	-	Percentuale di richieste che specificano SSE-KMS	Avanzato	Protezione dei dati	Y	sum (tutte le richieste SSEKMSRequests)	N	
Same-Region Numero delle regole di replica	SameRegionReplicationRuleCount	Numero di regole di replica per Same-Region Replication (SRR)	Avanzato	Protezione dei dati	N	-	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per derivare	Gruppi Storage Lens	
Regole di Same-Region replica medie per bucket	-	Numero medio di regole di replica per SRR	Avanzato	Protezione dei dati	Y	sum (SameRegionFunctionCountSum()) Distribuito per bucket	N	
Cross-Region Conteggio delle regole di replica	CrossRegionReplicationRuleCount	Numero di regole di replica per Cross-Region Replication (CRR)	Avanzato	Protezione dei dati	N	-	N	
Regole di Cross-Region replica medie per bucket	-	Numero medio di regole di replica per il CRR	Avanzato	Protezione dei dati	Y	sum (CrossRegionReplicationRuleCountSum()) Distribuito per bucket	N	
Same-account conteggio delle regole di replica	SameAccountReplicationRuleCount	Numero di regole di replica per la replica all'interno dello stesso account	Avanzato	Protezione dei dati	N	-	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per deriv	Gruppi Storage Lens	
Average same-account replication rules per bucket (Media regole di replica stesso account per bucket)	-	Numero medio di regole di replica per la replica all'interno dello stesso account	Average	Protezione dei dati	Yes	summary (Summary of Distribution Counts)	Number of Distinct Buckets	
Cross-account conteggio delle regole di replica	CrossAccountReplicationRuleCount	Numero di regole di replica per la replica su più account	Average	Protezione dei dati	No	-	Number of Distinct Buckets	
Average cross-account replication rules per bucket (Media regole di replica tra account per bucket)	-	Numero medio di regole di replica per la replica tra account	Average	Protezione dei dati	Yes	summary (Cross-account Distribution Counts)	Number of Distinct Buckets	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per derivare	Gruppi Storage Lens	
Invalid destination replication rule count (Conteggi o regole di replica di destinazione non valida)	InvalidDestinationReplicationRuleCount	Numero di regole di replica con una destinazione di replica non valida	Average	Protezione dei dati	No	-	N	
Average invalid destination replication rules per bucket (Media regole di replica destinazione non valida per bucket)	-	Numero medio di regole di replica con una destinazione di replica non valida	Average	Protezione dei dati	Yes	summary (InvalidDestinationReplicationRuleCount) summary (Distribution bucket)	N	

Nome parametro	CloudWatch ed esporta	Description	Live	Cate 2	D	Form para deriv	Gruppi Storage Lens	
Total replicati on rule count (Conteggio totale regole di replica)	-	Total replicati on rule count (Conteggio totale regole di replica)	Avar	Prot e dei dati	Y	som (Invæ estir nRe ionR unt) + som (Cro ount catic eCo + som (Sar untF atior Cou	N	

Nome parametro	CloudWatch ed esporta	Description	Live	Cate 2	D	Form para deriv	Gruppi Storage Lens	
Average replication rule count per bucket (Media conteggio regole di replica per bucket)	-	Numero totale medio delle regole di replica	Avar	Prot e dei dati	Y	(sum (Inv estir nRe ionR unt) + sum (Cro ount catic eCo + sum (Sar untF atior Cou sum (Disti umb cket	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens	
Object Ownership bucket owner enforced bucket count (Numero di bucket con Object Ownership impostata su Bucket owner enforced [Applicata da proprietario bucket])	ObjectOwnershipBucketOwnerEnforcedBucketCount	Numero di bucket con elenchi di controllo degli accessi (ACL) disattivati utilizzando l'impostazione imposta dal proprietario del bucket per Object Ownership	Grat	Gest degli acc	N	-	N	
% Object Ownership bucket owner enforced buckets (Bucket con % Object Ownership applicata da proprietario bucket)	-	Percentuale di bucket con ACL disattivati utilizzando l'impostazione applicata dal proprietario del bucket per Object Ownership	Grat	Gest degli acc	Y	sum () / sum ()	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria 2	D	Forma per deriv	Gruppi Storage Lens
Object Ownership bucket owner preferred bucket count (Numero di bucket con Object Ownership impostata su Bucket Owner Preferred [Preferita da proprietario bucket])	ObjectOwnershipBucketOwnerPreferredBucketCount	Numero di bucket che utilizzano l'impostazione preferita dal proprietario del bucket per Object Ownership	Grat	Gest degli access	N	-	N
% Object Ownership bucket owner preferred buckets (Bucket con % Object Ownership preferita da proprietario bucket)	-	Percentuale di bucket che utilizzano l'impostazione preferita del proprietario del bucket per Object Ownership	Grat	Gest degli access	Y	sum (ObjectOwnershipBucketOwnerPreferredBucketCount) / sum (DistributionBucketCount)	N

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per deriv	Gruppi Storage Lens	
Object Ownership object writer bucket count (Conteggio bucket object writer Object Ownership)	ObjectOwnershipObjectWriterBucketCount	Numero di bucket che utilizzano l'impostazione Object Writer per Object Ownership	Grat	Gest degli acc	N	-	N	
% Object Ownership object writer buckets (% bucket object writer Object Ownership)	-	Percentuale di bucket che utilizzano l'impostazione Object Writer per Object Ownership	Grat	Gest degli acc	Y	sum (ObjectWriterBucketCount) sum () Distinct bucket	N	
Transfer Acceleration enabled bucket count (Numero di bucket con Transfer Acceleration abilitata)	TransferAccelerationEnabledBucketCount	Numero di bucket con Transfer Acceleration abilitata	Grat	Perf ce	N	-	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per deriv	Gruppi Storage Lens	
% Transfer Acceleration enabled buckets (% bucket con Transfer Acceleration abilitata)	-	Percentuale di bucket con Transfer Acceleration abilitata	Grat	Perf	Y	sum (TransferAccelerationEnabledBuckets) / sum () Distriumbucket	N	
Event Notification enabled bucket count (Conteggio di bucket con alla notifica eventi abilitata)	EventNotificationEnabledBucketCount	Numero di bucket con Notifiche di eventi abilitate	Grat	Event	N	-	N	
% Event Notification enabled buckets (% bucket con notifica eventi abilitata)	-	Percentuale di bucket con Notifiche di eventi abilitate	Grat	Event	Y	sum (EventNotificationEnabledBuckets) / sum () Distriumbucket	N	

Nome parametro	CloudWatch ed esporta	Description	Live	Cate 2	D	Form para deriv	Gruppi Storage Lens	
Tutte le richieste	AllRequests	Numero totale di richieste effettuate	Avar	Attiv	N	-	N	
Richieste GET	GetRequests	Numero totale di GET richieste effettuate	Avar	Attiv	N	-	N	
Put requests (Richieste PUT)	PutRequests	Numero totale di PUT richieste effettuate	Avar	Attiv	N	-	N	
Head requests (Richieste HEAD)	HeadRequests	Numero di HEAD richieste effettuate	Avar	Attiv	N	-	N	
Delete requests (Richieste DELETE)	DeleteRequests	Numero di DELETE richieste effettuate	Avar	Attiv	N	-	N	
Richieste LIST	ListRequests	Numero di LIST richieste effettuate	Avar	Attiv	N	-	N	
Post requests (Richieste POST)	PostRequests	Numero di POST richieste effettuate	Avar	Attiv	N	-	N	
Select requests (Richieste Select)	SelectRequests	Numero di richieste S3 Select	Avar	Attiv	N	-	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	D	Forma per deriv	Gruppi Storage Lens
Select scanned bytes (Byte Select scansionati)	SelectScannedBytes	Numero di byte S3 Select scansionati	Average	Attivo	N	-	N
Select returned bytes (Byte Select restituiti)	SelectReturnedBytes	Numero di byte S3 Select restituiti	Average	Attivo	N	-	N
Byte scaricati	BytesDownloaded	Numero di byte scaricati	Average	Attivo	N	-	N
% retrieval rate (% tasso di recupero)	-	Percentuale di byte scaricati	Average	Attivo	Yes	sum(BytesDownloaded) / sum(StoredBytes)	N
Byte caricati	BytesUploaded	Numero di byte caricati	Average	Attivo	N	-	N
% ingest ratio (% rapporto di acquisizione)	-	Percentuale di byte caricati	Average	Attivo	Yes	sum(BytesLoaded) / sum(StoredBytes)	N

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	Dati	Forma per derivare	Gruppi Storage Lens
4xx errors (Errori 4xx)	4xxErrors	Numero di codici di stato HTTP 4xx	Average	Active	No	-	N
5xx errors (Errori 5xx)	5xxErrors	Numero di codici di stato HTTP 5xx	Average	Active	No	-	N
Total errors (Totale errori)	-	Somma di tutti gli errori 4xx e 5xx	Average	Active	Yes	sum of errors + sum of errors	N
% error rate (% tasso di errore)	-	Numero totale di errori 4xx e 5xx in percentuale del totale delle richieste	Average	Active	Yes	sum of errors (Total errors) / sum of requests (All Requests)	N
200 OK status count (Conteggio dello stato 200 OK)	200 OKStatusCount	Numero di 200 codici di stato OK	Average	Codice di stato definito	No	-	N

Nome parametro	CloudWatch ed esporta	Description	Level	Category	Dimension	Forma dei dati	Gruppi Storage Lens	
% 200 OK status (% stato 200 OK)	-	Numero totale di 200 codici di stato OK in percentuale del totale delle richieste	Availability	Codici di stato dettati	Y	summary (200 OK status) AllRequests	N	
206 Partial Content status count (Conteggi o stato 206 contenuto parziale)	206 PartialContentStatusCount	Numero di 206 codici di stato per contenuti parziali	Availability	Codici di stato dettati	N	-	N	
% 206 Partial Content status (% stato 206 contenuto parziale)	-	Numero di 206 codici di stato per i contenuti parziali in percentuale del totale delle richieste	Availability	Codici di stato dettati	Y	summary (206 PartialContentStatus) / summary AllRequests	N	
400 Bad Request error count (Conteggi o errori 400 Richiesta non valida)	400 BadRequestErrorCount	Numero di 400 codici di stato di Bad Request	Availability	Codici di stato dettati	N	-	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Categoria	D	Forma per deriv	Gruppi Storage Lens	
% 400 Bad Request errors (% errori 400 Richiesta non valida)	-	Numero di 400 codici di stato di Richiesta non valida come percentuale del totale delle richieste	Avar	Cod di stato detto to	Y	som (400 ques rCou som ()) AllR ts	N	
403 Forbidden error count (Conteggi o errori 403 Accesso negato)	403 Forbidden ErrorCount	Numero di 403 codici di stato Proibiti	Avar	Cod di stato detto to	N	-	N	
% 403 Forbidden errors (% errori 403 Accesso negato)	-	Numero di 403 codici di stato Proibiti come percentuale del totale delle richieste	Avar	Cod di stato detto to	Y	som (403 dder Cou som ()) AllR ts	N	
404 Not Found error count (Conteggio errori 404 Non trovato)	404 NotFoundErrorCount	Numero di codici di stato 404 Not Found	Avar	Cod di stato detto to	N	-	N	

Nome parametro	CloudWatch ed esporta	Description	Level	Category	Dimension	Forma per derivare	Gruppi Storage Lens	
% 404 Not Found errors (% errori 404 Non trovato)	-	Numero di codici di stato 404 Not Found come percentuale del totale delle richieste	Average	Codice di stato determinato	Yes	summary (404 undelimited count summary) AllRequests	N	
500 Internal Server Error count (Conteggi o errori 500 Errore interno del server)	500 InternalServerErrorCount	Numero di 500 codici di stato Internal Server Error	Average	Codice di stato determinato	No	-	N	
% 500 Internal Server Errors (% errori 500 Errore interno del server)	-	Numero di 500 codici di stato Internal Server Error come percentuale del totale delle richieste	Average	Codice di stato determinato	Yes	summary (500 InternalServerError) / summary (AllRequests)	N	

Nome parametro	CloudWatch ed esporta	Description	Livello	Categoria ²	Deriva	Formula derivata	Gruppi Storage Lens
503 Service Unavailable error count (Conteggi o errori 503 Servizio non disponibile)	503 ServiceUnavailable ErrorCount	Numero di 503 codici di stato Service Unavailable	Avanzata	Codice di stato determinato	N	-	N
% 503 Service Unavailable errors (% errori 503 Servizio non disponibile)	-	Numero di 503 codici di stato del servizio non disponibile in percentuale del totale delle richieste	Avanzata	Codice di stato determinato	Y	somma (503 ServiceUnavailable Count) AllRequests	N

¹Tutti i parametri di archiviazione del piano gratuito non sono disponibili a livello di gruppo Storage Lens. I parametri di livello avanzato non sono disponibili a livello di gruppo Storage Lens.

² I parametri relativi al conteggio delle regole e quelli relativi alle impostazioni dei bucket non sono disponibili a livello di prefisso.

La tabella seguente mostra le metriche delle prestazioni disponibili in S3 Storage Lens e la loro disponibilità in: CloudWatch

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Latency	AverageFirstByteLatency	Tempo medio per richiesta	Avanzata	Prestazioni	N	-	N

Nome del parametro	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Latency		Tempo medio trascorso per richiesta tra il primo byte ricevuto e l'ultimo byte inviato a un bucket Amazon S3, misurato nelle ultime 24 ore	Avanzata	Performance	N	-	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
Legge il numero di richieste da 0 a 128 KB	Read0KBRequestCount*	Numero di GetObject richieste con dimensioni inferiori di dati di 0 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Legge il numero di richieste da 0 a 128 KB	Read0KBTo128KBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 0 KB e fino a 128 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N

Nome	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Leggi il numero di richieste da 128 KB a 256 KB	Read128KBTo256KBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 128 KB e fino a 256 KB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Leggi il numero di richieste da 256 KB a 512 KB	Read256KBTo512KBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 256 KB e fino a 512 KB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N

Nome del metrico	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Leggila il numero di richieste da 512 KB a 1 MB	Read512KBTo1MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 512 KB e fino a 1 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Leggila il numero di richieste da 1 MB a 2 MB	Read1MBTo2MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 1 MB e fino a 2 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Legge il numero di richieste da 2 MB a 4 MB	Read2MBTo4MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 2 MB e fino a 4 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Legge il numero di richieste da 4 MB a 8 MB	Read4MBTo8MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 4 MB e fino a 8 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N

Nome	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Leggi il numero di richieste da 8 MB a 16 MB	Read8MBTo16MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 8 MB e fino a 16 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Leggi il numero di richieste da 16 MB a 32 MB	Read16MBTo32MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 16 MB e fino a 32 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N

Nome	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Leggila il numero di richieste da 32 MB a 64 MB	Read32MBO64MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 32 MB e fino a 64 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Leggila il numero di richieste da 64 MB a 128 MB	Read64MBO128MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 64 MB e fino a 128 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N

Nome	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Leggi il numero di richieste da 128 MB a 256 MB	Read128MBTo256MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 128 MB e fino a 256 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Leggi il numero di richieste da 256 MB a 512 MB	Read256MBTo512MBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 256 MB e fino a 512 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
Leggila il numero di richieste da 512 MB a 1 GB	Read512MBTo1GBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 512 MB e fino a 1 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Leggila il numero di richieste da 1 GB a 2 GB	Read1GBTo2GBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 1 GB e fino a 2 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N

Nome dell'azione	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
Leggere il numero di richieste da 2 GB a 4 GB	Read2GBTo4GBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 2 GB e fino a 4 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Leggere il numero di richieste di oltre 4 GB	ReadLargeThan4GBRequestCount*	Numero di GetObject richieste con dimensioni dei dati superiori a 4 GB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto	Avanzata	Performance	N	-	N
Scrivere un numero di richieste di 0 KB	Write0KBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati di 0 KB	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Scrittura di richieste con tra 0 KB e 128 KB	Write0KBT o128KBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 0 KB e fino a 128 KB	Avanzata	Performance	N	-	N
Scrittura di richieste da 128 KB a 256 KB	Write128KBT o256KBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 128 KB e fino a 256 KB	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Scrittura di richieste da 256 KB a 512 KB	Write256K BTo512KBR equestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 256 KB e fino a 512 KB	Avanzata	Performance	N	-	N
Scrittura di richieste da 512 KB a 1 MB	Write512K BTo1MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 512 KB e fino a 1 MB	Avanzata	Performance	N	-	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
Scritture di richieste con tra 1 MB e 2 MB	Write1MBTo2MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 1 MB e fino a 2 MB	Avanzata	Performance	N	-	N
Scritture di richieste con tra 2 MB e 4 MB	Write2MBTo4MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 2 MB e fino a 4 MB	Avanzata	Performance	N	-	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
Scritture di richieste con tra 4 MB e 8 MB	Write4MBTo8MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 4 MB e fino a 8 MB	Avanzata	Performance	N	-	N
Scritture di richieste con tra 8 MB e 16 MB	Write8MBTo16MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 8 MB e fino a 16 MB	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Scrittura di richieste con tra 16 MB e 32 MB	Write16MBTo32MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 16 MB e fino a 32 MB	Avanzata	Performance	N	-	N
Scrittura di richieste con tra 32 MB e 64 MB	Write32MBTo64MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 32 MB e fino a 64 MB	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
Scrittura di richieste con tra 64 MB e 128 MB	Write64MBTo128MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 64 MB e fino a 128 MB	Avanzata	Performance	N	-	N
Scrittura di richieste da 128 MB a 256 MB	Write128MBTo256MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 128 MB e fino a 256 MB	Avanzata	Performance	N	-	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
Scrittura di richieste da 256 MB a 512 MB	Write256MBTo512MBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 256 MB e fino a 512 MB	Avanzata	Performance	N	-	N
Scrittura di richieste da 512 MB a 1 GB	Write512MBTo1GBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 512 MB e fino a 1 GB	Avanzata	Performance	N	-	N

Nome	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Scrittura di richieste da 1 GB a 2 GB	Write1GBTo2GBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 1 GB e fino a 2 GB	Avanzata	Performance	N	-	N
Scrittura di richieste da 2 GB a 4 GB	Write2GBTo4GBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 2 GB e fino a 4 GB	Avanzata	Performance	N	-	N
Scrittura di richieste di oltre 4 GB	WriteLargerThan4GBRequestCount*	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 4 GB	Avanzata	Performance	N	-	N

Nome	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Conteggio degli oggetti da 0 a 0 KB	Conteggio 0 KB dell'oggetto	Numero di oggetti con dimensioni pari a 0 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N
Numero di oggetti con tra 0 KB e 128 KB	Object0KB To128KBCount	Numero di oggetti con dimensioni superiori a 0 KB e inferiori o uguali a 128 KB, incluse la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome del parametro	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 128 KB e 256 KB	Object128KBTo256KBCount	Numero di oggetti con dimensioni superiori a 128 KB e inferiori o uguali a 256 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Oggetti con dimensioni da 256 KB a 512 KB	Object256KBTto512KBCount	Numero di oggetti con dimensioni superiori a 256 KB e inferiori o uguali a 512 KB, incluse la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell'indicatore	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 512 KB e 1 MB	Object512KBTo1MBCount	Numero di oggetti con dimensioni superiori a 512 KB e inferiori o uguali a 1 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 1 MB e 2 MB	Object1MBTo2MBCount	Numero di oggetti con dimensioni superiori a 1 MB e inferiori o uguali a 2 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome del metrico	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 2 MB e 4 MB	Object2MBTo4MBCount	Numero di oggetti con dimensioni superiori a 2 MB e inferiori o uguali a 4 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 4 MB e 8 MB	Object4MBTo8MBCount	Numero di oggetti con dimensioni superiori a 4 MB e inferiori o uguali a 8 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 8 MB e 16 MB	Object8MBTo16MBCount	Numero di oggetti con dimensioni superiori a 8 MB e inferiori o uguali a 16 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 16 MB e 32 MB	Object16MBTo32MBCount	Numero di oggetti con dimensioni superiori a 16 MB e inferiori o uguali a 32 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome del parametro	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 32 MB e 64 MB	Object32MBTo64MBCount	Numero di oggetti con dimensioni superiori a 32 MB e inferiori o uguali a 64 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 64 MB e 128 MB	Object64MBTo128MBCount	Numero di oggetti con dimensioni superiori a 64 MB e inferiori o uguali a 128 MB, incluse la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 128 MB e 256 MB	Object128MBTo256MBCount	Numero di oggetti con dimensioni superiori a 128 MB e inferiori o uguali a 256 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell' metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Numero di oggetti con tra 256 MB e 512 MB	Object256MBTo512MBCount	Numero di oggetti con dimensioni superiori a 256 MB e inferiori o uguali a 512 MB, incluse la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell'indicatore	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Gli oggetti da 512 MB a 1 GB	Object512MBTo1GBCount	Numero di oggetti con dimensioni superiori a 512 MB e inferiori o uguali a 1 GB, incluse la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell'indicatore	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Gli oggetti corrono da 1 GB a 2 GB	Object1GBTo2GBCount	Numero di oggetti con dimensioni superiori a 1 GB e inferiori o uguali a 2 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome dell'indicatore	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
Gli oggetti da 2 GB a 4 GB	Object2GBTo4GBCount	Numero di oggetti con dimensioni superiori a 2 GB e inferiori o uguali a 4 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N
Numero di oggetti pari o superiore a 4 GB	ObjectLargerThan4GBCount	Numero di oggetti con dimensioni superiori a 4 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione	Avanzata	Performance	N	-	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
ConcurrentPut503ErrorCount	ConcurrentPut503ErrorCount	Numero di errori 503 generati a causa di scritture simultanee sullo stesso oggetto	Avanzata	Performance	N	-	N
% di errori 503 di Put simultaneo	-	Percentuale di errori 503 generati a causa di scritture simultanee sullo stesso oggetto	Avanzata	Performance	Y	100 * / ConcurrentPut503ErrorCount AllRequests	N
CrossRegionRequestCount	CrossRegionRequestCount	Numero di richieste che provengono da un cliente in una regione diversa da quella di origine del bucket	Avanzata	Performance	N	-	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
% richieste Cross Region	-	Percentuale di richieste provenienti da un cliente in una regione diversa da quella di origine del bucket	Avanzata	Performance	Y	$100 * \frac{\text{CrossRegionRequestCount}}{\text{AllRequests}}$	N
Cross Region bytes trasferiti	CrossRegionTransferredBytes	Numero di byte trasferiti da chiamate in una regione diversa da quella di origine del bucket	Avanzata	Performance	N	-	N
% Cross Region di byte trasferiti	-	Percentuale di byte trasferiti che provengono da chiamate in una regione diversa da quella di origine del bucket	Avanzata	Performance	Y	$100 * \frac{\text{CrossRegionTransferredBytes}}{(\text{BytesDownloaded} + \text{BytesUploaded})}$	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
CrossRegionRequestCount	CrossRegionWithoutReplicationRequestCount	Numero di richieste che provengono da un client in una regione diversa da quella di origine del bucket, escluse le richieste di replica tra regioni	Avanzata	Performance	N	-	N
% di richieste di replica	CrossRegionRequestCount	Percentuale di richieste provenienti da un cliente in una regione diversa da quella di origine del bucket, escluse le richieste di replica tra regioni	Avanzata	Performance	Y	100 * CrossRegionWithoutReplicationRequestCount / AllRequests	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
CrossRegionTransferBytes	CrossRegionWithoutReplicatedBytes	Numero di byte trasferiti da chiamate in una regione diversa da quella di origine del bucket, esclusi i byte di replica tra regioni	Avanzata	Performance	N	-	N
CrossRegionTransferBytesPercentage	-	Percentuale di byte trasferiti che provengono da chiamate in una regione diversa da quella di origine del bucket, esclusi i byte di replica tra regioni	Avanzata	Performance	Y	$\frac{\text{CrossRegionWithoutReplicatedBytes} \times 100}{\text{BytesDownloaded} + \text{BytesUploaded}}$	N
InRegionRequestCount	InRegionRequestCount	Numero di richieste che provengono da un cliente nella stessa regione della regione di origine del bucket	Avanzata	Performance	N	-	N

Nome della metrica	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Derivata	Formula metrica derivata	Gruppi Storage Lens
% richieste In-Region	-	Percentuale di richieste provenienti da un cliente nella stessa regione della regione di origine del bucket	Avanzata	Performance	Y	$100 * \frac{\text{InRegionRequestsCount}}{\text{AllRequests}}$	N
In-Region bytes trasferiti	InRegionTransferredBytes	Numero di byte trasferiti dalle chiamate dalla stessa regione della regione di origine del bucket	Avanzata	Performance	N	-	N
% In-Region di byte trasferiti	-	Percentuale di byte trasferiti che provengono da chiamate dalla stessa regione della regione di origine del bucket	Avanzata	Performance	Y	$100 * \frac{\text{InRegionTransferredBytes}}{(\text{InRegionTransferredBytes} + \text{BytesDownloaded} + \text{BytesUploaded})}$	N

Nome dell'azione	CloudWatch ed esportazione	Descrizione	Livello	Categoria	Deriva	Formula metrica derivata	Gruppi Storage Lens
Gli oggetti unici a cui si accede con questa azione	UniqueObjectsAccessedDailyCount	Numero di oggetti a cui è stato effettuato l'accesso almeno una volta nelle ultime 24 ore	Avanzata	Performance	N	-	N
% Gli oggetti unici a cui si accede giornalmente	-	Percentuale di oggetti a cui è stato effettuato l'accesso almeno una volta nelle ultime 24 ore	Avanzata	Performance	Y	100 * / UniqueObjectsAccessedDailyCount ObjectCount	N

Impostazione delle autorizzazioni di Amazon S3 Storage Lens

Amazon S3 Storage Lens richiede nuove autorizzazioni in AWS Identity and Access Management (IAM) per autorizzare l'accesso alle azioni di S3 Storage Lens. Per concedere queste autorizzazioni, puoi utilizzare una policy IAM basata sull'identità. Per farlo, collega la policy a utenti, gruppi o ruoli IAM ai quali desideri concedere tali autorizzazioni. Le autorizzazioni possono riguardare, ad esempio, l'abilitazione o la disabilitazione di S3 Storage Lens, l'accesso a qualsiasi pannello di controllo o la configurazione di S3 Storage Lens.

L'utente o il ruolo IAM deve appartenere all'account del creatore o del titolare del pannello di controllo o della configurazione, a meno che non si verifichino entrambe le condizioni seguenti:

- Il tuo account è membro di. AWS Organizations
- Ti è stata concessa l'autorizzazione per creare pannelli di controllo a livello di organizzazione dal tuo account di gestione in qualità di amministratore delegato.

Note

- Non puoi utilizzare le credenziali utente root del tuo account per visualizzare i pannelli di controllo di Amazon S3 Storage Lens. Per accedere ai pannelli di controllo di S3 Storage Lens, è necessario concedere le autorizzazioni IAM necessarie a un utente IAM nuovo o esistente. Quindi, accedi con le credenziali utente per accedere ai pannelli di controllo di S3 Storage Lens. Per ulteriori informazioni, consulta [Best Practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.
- L'utilizzo di S3 Storage Lens nella console di Amazon S3 può richiedere più autorizzazioni. Ad esempio, per modificare un pannello di controllo nella console, sono necessarie le seguenti autorizzazioni:
 - `s3:ListStorageLensConfigurations`
 - `s3:GetStorageLensConfiguration`
 - `s3:PutStorageLensConfiguration`

Argomenti

- [Impostazione delle autorizzazioni dell'account per utilizzare S3 Storage Lens](#)
- [Impostazione delle autorizzazioni dell'account per utilizzare i gruppi S3 Storage Lens](#)
- [Impostazione delle autorizzazioni per l'utilizzo di S3 Storage Lens con AWS Organizations](#)

Impostazione delle autorizzazioni dell'account per utilizzare S3 Storage Lens

Per creare e gestire i pannelli di controllo di S3 Storage Lens e le configurazioni dei pannelli di controllo di Storage Lens, devi disporre delle seguenti autorizzazioni, a seconda delle azioni che desideri eseguire:

La tabella seguente mostra le autorizzazioni IAM relative ad Amazon S3 Storage Lens.

Azione	Autorizzazioni IAM
Creare o aggiornare un pannello di controllo di S3 Storage Lens nella console di Amazon S3.	<code>s3:ListStorageLensConfigurations</code> <code>s3:GetStorageLensConfiguration</code> <code>s3:GetStorageLensConfigurat ionTagging</code> <code>s3:PutStorageLensConfiguration</code> <code>s3:PutStorageLensConfigurat ionTagging</code>
Ottenere i tag di un pannello di controllo di S3 Storage Lens nella console di Amazon S3.	<code>s3:ListStorageLensConfigurations</code> <code>s3:GetStorageLensConfigurat ionTagging</code>
Visualizzare un pannello di controllo di S3 Storage Lens nella console di Amazon S3.	<code>s3:ListStorageLensConfigurations</code> <code>s3:GetStorageLensConfiguration</code> <code>s3:GetStorageLensDashboard</code>
Eliminare un pannello di controllo di S3 Storage Lens nella console di Amazon S3.	<code>s3:ListStorageLensConfigurations</code> <code>s3:GetStorageLensConfiguration</code> <code>s3>DeleteStorageLensConfigu ration</code>
Crea o aggiorna una configurazione di S3 Storage Lens utilizzando AWS CLI o un AWS SDK.	<code>s3:PutStorageLensConfiguration</code> <code>s3:PutStorageLensConfigurat ionTagging</code>
Ottieni i tag di una configurazione di S3 Storage Lens utilizzando AWS CLI o un SDK. AWS	<code>s3:GetStorageLensConfigurat ionTagging</code>

Azione	Autorizzazioni IAM
Visualizza una configurazione di S3 Storage Lens utilizzando AWS CLI o un SDK. AWS	<code>s3:GetStorageLensConfiguration</code>
Elimina una configurazione di S3 Storage Lens utilizzando o SDK. AWS CLI AWS	<code>s3:DeleteStorageLensConfiguration</code>

Note

- Puoi utilizzare i tag delle risorse in una policy IAM per gestire le autorizzazioni.
- Un ruolo o un utente IAM con queste autorizzazioni può visualizzare i parametri dai bucket e dai prefissi in cui potrebbero non disporre dell'autorizzazione diretta per leggere o elencare oggetti.
- Per i pannelli di controllo di S3 Storage Lens con parametri a livello di prefisso abilitati, se un percorso di prefisso selezionato corrisponde a una chiave di oggetto, il pannello di controllo potrebbe visualizzare la chiave di oggetto come un altro prefisso.
- Per le esportazioni dei parametri, archiviati in un bucket dell'account, le autorizzazioni vengono concesse mediante l'autorizzazione `s3:GetObject` esistente nella policy IAM. Allo stesso modo, per un' AWS Organizations entità, l'account di gestione dell'organizzazione o gli account di amministratore delegato possono utilizzare le politiche IAM per gestire le autorizzazioni di accesso per dashboard e configurazioni a livello di organizzazione.

Impostazione delle autorizzazioni dell'account per utilizzare i gruppi S3 Storage Lens

Puoi utilizzare i gruppi S3 Storage Lens per comprendere la distribuzione dell'archiviazione all'interno dei bucket in base al prefisso, al suffisso, al tag dell'oggetto, alla dimensione dell'oggetto o all'età dell'oggetto. Per visualizzare i parametri aggregati, collega i gruppi Storage Lens al pannello di controllo.

Per utilizzare i gruppi Storage Lens, sono necessarie autorizzazioni specifiche. Per ulteriori informazioni, consulta [the section called “Autorizzazioni gruppi Storage Lens”](#).

Impostazione delle autorizzazioni per l'utilizzo di S3 Storage Lens con AWS Organizations

Puoi utilizzare Amazon S3 Storage Lens per raccogliere metriche di archiviazione e dati di utilizzo per tutti gli account che fanno parte della tua gerarchia. AWS Organizations La tabella seguente mostra le azioni e le autorizzazioni relative all'uso di S3 Storage Lens con le organizzazioni.

Azione	Autorizzazioni IAM
Abilitare l'accesso attendibile per S3 Storage Lens per la tua organizzazione.	<code>organizations:EnableAWSServiceAccess</code>
Disabilitare l'accesso attendibile per S3 Storage Lens per la tua organizzazione.	<code>organizations:DisableAWSServiceAccess</code>
Registrare un amministratore delegato per creare pannelli di controllo o configurazioni S3 Storage Lens per l'organizzazione.	<code>organizations:RegisterDelegatedAdministrator</code>
Annullare la registrazione di un amministratore delegato in modo che non possa più creare pannelli di controllo o configurazioni di S3 Storage Lens per l'organizzazione.	<code>organizations:DeregisterDelegatedAdministrator</code>
Autorizzazioni aggiuntive per creare configurazioni S3 Storage Lens a livello di organizzazione.	<code>organizations:DescribeOrganization</code>
	<code>organizations:ListAccounts</code>
	<code>organizations:ListAWSServiceAccessForOrganization</code>
	<code>organizations:ListDelegatedAdministrators</code>
	<code>iam:CreateServiceLinkedRole</code>

Utilizzo di Amazon S3 Storage Lens con la console e l'API

Amazon S3 Storage Lens è una funzionalità di analisi dell'archiviazione su cloud che puoi utilizzare per avere una panoramica completa a livello di organizzazione sull'utilizzo e sulle attività relative all'archiviazione di oggetti. È possibile utilizzare i parametri di S3 Storage Lens per generare approfondimenti, ad esempio per scoprire la quantità di spazio di archiviazione disponibile nell'intera organizzazione o quali sono i bucket e i prefissi caratterizzati da una crescita più rapida. Puoi anche utilizzare i parametri di S3 Storage Lens per individuare le opportunità di ottimizzazione dei costi, implementare le best practice di protezione e sicurezza dei dati e migliorare le prestazioni dei carichi di lavoro delle applicazioni. Ad esempio, puoi identificare i bucket che non hanno regole del ciclo di vita S3 per far scadere i caricamenti in più parti incompleti che risalgono a più di 7 giorni. Puoi anche individuare i bucket non conformi alle best practice di protezione dei dati, come quelli che usano la replica S3 o il controllo delle versioni S3. S3 Storage Lens analizza i parametri di archiviazione per fornire raccomandazioni contestuali che puoi usare per ottimizzare i costi di archiviazione e applicare le best practice sulla protezione dei dati.

S3 Storage Lens aggrega i tuoi parametri e mostra le informazioni nella sezione Account snapshot (Snapshot dell'account) nella pagina Buckets (Bucket) della console di Amazon S3. S3 Storage Lens fornisce anche una dashboard interattiva che puoi utilizzare per visualizzare informazioni e tendenze, segnalare valori anomali e ricevere consigli per ottimizzare i costi di storage e applicare le migliori pratiche di protezione dei dati. La dashboard offre opzioni di approfondimento per generare e visualizzare informazioni dettagliate a livello di organizzazione, account, classe di archiviazione, bucket Regione AWS, prefisso o gruppo Storage Lens. Puoi anche inviare un rapporto giornaliero sulle metriche in Parquet formato CSV o a un bucket S3 generico o esportare le metriche direttamente in un bucket di tabelle S3 gestito. AWS

Note

Storage Lens aggrega solo le metriche per i bucket S3 per uso generico. [???](#)

Questa sezione contiene esempi di creazione, aggiornamento e visualizzazione delle configurazioni S3 Storage Lens e l'esecuzione di operazioni correlate alla funzione. Se utilizzi S3 Storage Lens con AWS Organizations, questi esempi coprono anche questi casi d'uso. Negli esempi, sostituisci eventuali valori segnaposto.

Argomenti

- [Creare una dashboard di Amazon S3 Storage Lens](#)

- [Aggiornare la dashboard di Amazon S3 Storage Lens](#)
- [Disattivare la dashboard di Amazon S3 Storage Lens](#)
- [Eliminare la dashboard di Amazon S3 Storage Lens](#)
- [Elenco delle dashboard di Amazon S3 Storage Lens](#)
- [Visualizzare i dettagli della configurazione della dashboard di Amazon S3 Storage Lens](#)
- [Gestione AWS tag delle risorse con S3 Storage Lens](#)
- [File helper per l'utilizzo di Amazon S3 Storage Lens](#)

Creare una dashboard di Amazon S3 Storage Lens

Puoi creare dashboard personalizzate aggiuntive di S3 Storage Lens che possono essere associate alla tua organizzazione in AWS Organizations o a specifici Regioni AWS bucket all'interno di un account.

Note

Affinché la visualizzazione di qualsiasi aggiornamento alla configurazione del pannello di controllo sia accurata, possono essere necessarie fino a 48 ore.

Utilizzo della console S3

Attieniti alla procedura seguente per creare un pannello di controllo Amazon S3 Storage Lens sulla console Amazon S3.

Fase 1: Configurare le impostazioni generali

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione a cui passare.
3. Nel pannello di navigazione a sinistra, in S3 Storage Lens scegli Pannelli di controllo.
4. Seleziona Crea pannello di controllo.
5. Nella sezione Generale della pagina Pannello di controllo completa le seguenti operazioni:

- a. Visualizzare la Regione di origine della dashboard. La regione principale è la regione Regione AWS in cui sono archiviate la configurazione e le metriche per questa dashboard di Storage Lens.
- b. Specifica il nome di un pannello di controllo.

I nomi del pannello di controllo devono contenere meno di 65 caratteri e non possono contenere caratteri speciali o spazi.

 Note

Il nome del pannello di controllo dopo la creazione non potrà più essere modificato.

- c. Scegli **Abilitato** per visualizzare le metriche giornaliere aggiornate nella dashboard.
- d. (Facoltativo) Puoi scegliere di aggiungere tag alla tua dashboard. I tag possono essere utilizzati per gestire le autorizzazioni per il pannello di controllo e tenere traccia dei costi per S3 Storage Lens. Per ulteriori informazioni, consulta [Controllare l'accesso alle AWS risorse utilizzando i tag](#) nella Guida per l'utente IAM e [Utilizzo dei tag AWS generati](#) nella Guida per l'AWS Billing utente.

 Note

Puoi aggiungere fino a 50 tag alla configurazione del pannello di controllo.

6. Scegli **Avanti** per salvare le modifiche e procedere.

Passaggio 2: definire l'ambito del dashboard

1. Nella sezione **Ambito del dashboard**, scegli le regioni e i bucket che desideri che S3 Storage Lens includa o escluda nella dashboard.
2. Scegli i bucket nelle regioni selezionate che desideri siano inclusi o esclusi da S3 Storage Lens. Puoi includere o escludere i bucket, ma non puoi eseguire entrambe le operazioni. Questa opzione non è disponibile quando crei dashboard a livello di organizzazione.

 Note

- Puoi anche includere o escludere Regioni e bucket. Questa opzione è limitata alle Regioni solo se si creano dashboard a livello di organizzazione tra gli account membri dell'organizzazione.
- Puoi scegliere fino a 50 bucket da includere o escludere.

3. Scegli **Avanti** per salvare le modifiche e procedere.

Passaggio 3: scegli il livello di Storage Lens

1. Nella sezione **Storage Lens tier**, scegli il livello di funzionalità che desideri aggregare per questa dashboard.
 - a. Per includere metriche gratuite aggregate a livello di bucket e disponibili per le domande per 14 giorni, scegli il livello gratuito.
 - b. Per abilitare le metriche avanzate, scegli il livello avanzato. Queste opzioni includono l'aggregazione dei gruppi di prefissi o Storage Lens, la CloudWatch pubblicazione su Amazon, il rapporto sui prefissi espansi e i consigli contestuali. I dati sono disponibili per le query per 15 mesi. I parametri e i suggerimenti avanzati hanno un costo aggiuntivo. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Per ulteriori informazioni su parametri avanzati e parametri gratuiti, consulta [Selezione delle metriche](#).

2. In **Categorie di metriche avanzate**, seleziona la categoria di metriche che desideri abilitare:

- Parametri delle attività
- Detailed status code metrics (Parametri dettagliati codice di stato)
- Metriche di ottimizzazione dei costi
- Metriche di protezione dei dati
- Metriche delle prestazioni

Per visualizzare in anteprima quali metriche sono incluse in ciascuna categoria, utilizza il pulsante freccia a discesa sotto l'elenco delle caselle di controllo della categoria delle metriche.

Per ulteriori informazioni sulle categorie di parametri, consulta [Categorie di parametri](#). Per un elenco completo di parametri, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

3. Scegli o specifica un delimitatore di prefisso per distinguere i livelli all'interno di ciascun prefisso. Questo valore viene utilizzato per identificare ogni livello di prefisso. Il valore predefinito in Amazon S3 è il carattere "/", ma la struttura di storage potrebbe utilizzare altri caratteri delimitatori.
4. Scegli **Avanti** per salvare le modifiche e procedere.

Fase 4: (Facoltativo) Scegli l'aggregazione delle metriche

1. In **Aggregazione delle metriche aggiuntive**, scegli quali metriche vuoi aggregare:
 - **Aggregazione di prefisso**
 - **Aggregazione dei gruppi Storage Lens**
2. Se hai abilitato l'aggregazione dei prefissi, specifica la soglia minima del prefisso per la dashboard e la profondità del prefisso. Quindi, scegli **Avanti** per salvare e procedere.

Note

L'impostazione della profondità del prefisso determina quanti livelli gerarchici di profondità S3 Storage Lens analizzerà i prefissi degli oggetti, con un limite massimo di 10 livelli. La soglia **Prefix** specifica la percentuale minima di spazio di archiviazione totale che un prefisso deve rappresentare prima di essere incluso nelle metriche di Storage Lens.

3. Se hai abilitato l'aggregazione dei gruppi Storage Lens, scegli una delle seguenti opzioni:
 - **Includi i gruppi Storage Lens**
 - **Escludere i gruppi Storage Lens**
4. Quando includi i gruppi Storage Lens nell'aggregazione, puoi includere tutti i gruppi Storage Lens nella tua regione principale o specificare i gruppi Storage Lens da includere.
5. Scegli **Avanti** per salvare le modifiche e procedere.

Passaggio 5: (Facoltativo) Scegli le impostazioni di esportazione e pubblicazione delle metriche

1. In **Pubblicazione delle metriche**, scegli la **CloudWatch pubblicazione** se desideri accedere alle metriche di Storage Lens nella dashboard. CloudWatch

Note

Prefix-level le metriche non sono disponibili in. CloudWatch

2. In **Esportazione delle metriche**, scegli i dati del dashboard di Storage Lens che desideri esportare giornalmente:
 - Rapporto sulle metriche predefinite
 - Rapporto sulle metriche dei prefissi espanso
3. (Facoltativo) Se hai scelto il rapporto sulle metriche predefinite, nelle **Impostazioni del rapporto sulle metriche predefinite**, scegli il tipo di bucket. Puoi esportare il report in un bucket Amazon S3 generico o in un bucket tabellare S3 gestito. AWS In base al tipo di bucket selezionato, aggiorna le opzioni **General Purpose bucket destination settings** o **Table bucket destination settings**.

Note

Il rapporto sulle metriche predefinito include solo i prefissi all'interno della soglia e della profondità impostate nelle impostazioni di aggregazione dei prefissi.

Se scegli di specificare una chiave di crittografia, devi scegliere una chiave (SSE-KMS) o una AWS KMS chiave gestita da Amazon S3 (). SSE-S3 Se la tua policy del bucket di destinazione richiede la crittografia, devi fornire una chiave di crittografia per l'esportazione delle metriche. Senza la chiave di crittografia, l'esportazione in S3 non riesce. Per ulteriori informazioni, consulta [Utilizzando un AWS KMS key per crittografare le esportazioni delle metriche](#).

4. (Facoltativo) Se hai scelto il rapporto sulle metriche dei prefissi espansi, nelle **impostazioni del rapporto sulle metriche dei prefissi espansi**, scegli il tipo di bucket. Puoi esportare il report in un bucket Amazon S3 generico o in un bucket tabellare S3 di sola lettura. In base al tipo di bucket selezionato, aggiorna le impostazioni di destinazione del bucket per uso generico o le impostazioni di destinazione del bucket Table.

 Note

Il rapporto sulle metriche dei prefissi estesi include tutti i prefissi fino alla profondità del prefisso 50 in tutti i bucket selezionati specificati nell'ambito della dashboard.

Se scegli di specificare una chiave di crittografia, devi scegliere una chiave (SSE-KMS) o una AWS KMS chiave gestita da Amazon S3 (). SSE-S3 Se la tua policy del bucket di destinazione richiede la crittografia, devi fornire una chiave di crittografia per l'esportazione delle metriche. Senza la chiave di crittografia, l'esportazione in S3 non riesce. Per ulteriori informazioni, consulta [Utilizzando un AWS KMS key per crittografare le esportazioni delle metriche](#).

5. Scegli **Avanti** per salvare le modifiche e procedere.
6. Controlla tutto nella pagina **Rivedi e crea**. Se non ci sono ulteriori modifiche, scegli **Avanti** per salvare le modifiche e creare la tua dashboard.

Passaggio 6: rivedi la configurazione della dashboard e crea la dashboard

1. Nella sezione **Generale**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
2. Nella sezione **Ambito del dashboard**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
3. Nella sezione **Storage Lens tier**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
4. Nella sezione **Aggregazione delle metriche**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
5. Nella sezione **Esportazione delle metriche**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
6. Dopo aver esaminato e confermato tutte le impostazioni di configurazione della dashboard, scegli **Invia** per creare la dashboard.

Dopo aver creato con successo la nuova dashboard di Storage Lens, puoi visualizzarla elencata nella pagina **Storage Lens Dashboard**.

Utilizzo di AWS CLI

Example

Il seguente esempio di comando crea una configurazione di Amazon S3 Storage Lens con tag. Per utilizzare questi esempi, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --  
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-  
configuration=file:///./config.json --tags=file:///./tags.json
```

Example

Il seguente esempio di comando crea una configurazione di Amazon S3 Storage Lens senza tag. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control put-storage-lens-configuration --account-id=222222222222 --config-  
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file:///./  
config.json
```

Utilizzo di AWS SDK per Java

Example- Creare e aggiornare la configurazione di Amazon S3 Storage Lens

L'esempio seguente crea e aggiorna una configurazione di Amazon S3 Storage Lens in SDK per Java:

```
package aws.example.s3control;  
  
import software.amazon.awssdk.awscore.exception.AwsServiceException;  
import software.amazon.awssdk.core.exception.SdkClientException;  
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.s3control.S3ControlClient;  
import software.amazon.awssdk.services.s3control.model.AccountLevel;  
import software.amazon.awssdk.services.s3control.model.ActivityMetrics;  
import software.amazon.awssdk.services.s3control.model.AdvancedCostOptimizationMetrics;  
import software.amazon.awssdk.services.s3control.model.AdvancedDataProtectionMetrics;  
import software.amazon.awssdk.services.s3control.model.AdvancedPerformanceMetrics;  
import software.amazon.awssdk.services.s3control.model.BucketLevel;  
import software.amazon.awssdk.services.s3control.model.CloudWatchMetrics;  
import software.amazon.awssdk.services.s3control.model.DetailedStatusCodesMetrics;  
import software.amazon.awssdk.services.s3control.model.Format;
```

```
import software.amazon.awssdk.services.s3control.model.Include;
import software.amazon.awssdk.services.s3control.model.OutputSchemaVersion;
import software.amazon.awssdk.services.s3control.model.PrefixLevel;
import software.amazon.awssdk.services.s3control.model.PrefixLevelStorageMetrics;
import
    software.amazon.awssdk.services.s3control.model.PutStorageLensConfigurationRequest;
import software.amazon.awssdk.services.s3control.model.S3BucketDestination;
import software.amazon.awssdk.services.s3control.model.SSE3;
import software.amazon.awssdk.services.s3control.model.SelectionCriteria;
import software.amazon.awssdk.services.s3control.model.StorageLensAwsOrg;
import software.amazon.awssdk.services.s3control.model.StorageLensConfiguration;
import software.amazon.awssdk.services.s3control.model.StorageLensDataExport;
import software.amazon.awssdk.services.s3control.model.StorageLensDataExportEncryption;
import
    software.amazon.awssdk.services.s3control.model.StorageLensExpandedPrefixesDataExport;
import software.amazon.awssdk.services.s3control.model.StorageLensTableDestination;
import software.amazon.awssdk.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        String exportAccountId = "Destination Account ID";
        String exportBucketArn = "arn:aws:s3:::destBucketName"; // The destination
        bucket for your metrics export must be in the same Region as your S3 Storage Lens
        configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
        abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = SelectionCriteria.builder()
                .delimiter("/")
                .maxDepth(5)
                .minStorageBytesPercentage(10.0)
                .build();

            PrefixLevelStorageMetrics prefixStorageMetrics =
            PrefixLevelStorageMetrics.builder()
                .isEnabled(true)
```

```

        .selectionCriteria(selectionCriteria)
        .build();

    BucketLevel bucketLevel = BucketLevel.builder()
        .activityMetrics(ActivityMetrics.builder().isEnabled(true).build())

    .advancedCostOptimizationMetrics(AdvancedCostOptimizationMetrics.builder().isEnabled(true).build())

    .advancedDataProtectionMetrics(AdvancedDataProtectionMetrics.builder().isEnabled(true).build())

    .advancedPerformanceMetrics(AdvancedPerformanceMetrics.builder().isEnabled(true).build())

    .detailedStatusCodesMetrics(DetailedStatusCodesMetrics.builder().isEnabled(true).build())

    .prefixLevel(PrefixLevel.builder().storageMetrics(prefixStorageMetrics).build())
    .build();

    AccountLevel accountLevel = AccountLevel.builder()
        .activityMetrics(ActivityMetrics.builder().isEnabled(true).build())

    .advancedCostOptimizationMetrics(AdvancedCostOptimizationMetrics.builder().isEnabled(true).build())

    .advancedPerformanceMetrics(AdvancedPerformanceMetrics.builder().isEnabled(true).build())

    .advancedDataProtectionMetrics(AdvancedDataProtectionMetrics.builder().isEnabled(true).build())

    .detailedStatusCodesMetrics(DetailedStatusCodesMetrics.builder().isEnabled(true).build())
        .bucketLevel(bucketLevel)
    .build();

    Include include = Include.builder()
        .buckets(Arrays.asList("arn:aws:s3:::bucketName"))
        .regions(Arrays.asList("us-west-2"))
    .build();

    StorageLensDataExportEncryption exportEncryption =
StorageLensDataExportEncryption.builder()
        .sses3(SSES3.builder().build())
    .build();

    S3BucketDestination s3BucketDestination = S3BucketDestination.builder()
        .accountId(exportAccountId)
        .arn(exportBucketArn)
        .encryption(exportEncryption)

```

```
.format(exportFormat)
.outputSchemaVersion(OutputSchemaVersion.V_1)
.prefix("Prefix")
.build();

StorageLensTableDestination s3TablesDestination =
StorageLensTableDestination.builder()
    .encryption(exportEncryption)
    .isEnabled(true)
    .build();

CloudWatchMetrics cloudWatchMetrics = CloudWatchMetrics.builder()
    .isEnabled(true)
    .build();

StorageLensDataExport dataExport = StorageLensDataExport.builder()
    .cloudWatchMetrics(cloudWatchMetrics)
    .s3BucketDestination(s3BucketDestination)
    .storageLensTableDestination(s3TablesDestination)
    .build();

StorageLensAwsOrg awsOrg = StorageLensAwsOrg.builder()
    .arn(awsOrgARN)
    .build();

StorageLensExpandedPrefixesDataExport expandedPrefixesDataExport =
StorageLensExpandedPrefixesDataExport.builder()
    .s3BucketDestination(s3BucketDestination)
    .storageLensTableDestination(s3TablesDestination)
    .build();

StorageLensConfiguration configuration = StorageLensConfiguration.builder()
    .id(configurationId)
    .accountLevel(accountLevel)
    .include(include)
    .dataExport(dataExport)
    .awsOrg(awsOrg)
    .expandedPrefixesDataExport(expandedPrefixesDataExport)
    .prefixDelimiter("/")
    .isEnabled(true)
    .build();

List<StorageLensTag> tags = Arrays.asList(
    StorageLensTag.builder().key("key-1").value("value-1").build(),
```

```
        StorageLensTag.builder().key("key-2").value("value-2").build()
    );

    S3ControlClient s3ControlClient = S3ControlClient.builder()
        .region(Region.US_WEST_2)
        .credentialsProvider(ProfileCredentialsProvider.create())
        .build();

    s3ControlClient.putStorageLensConfiguration(PutStorageLensConfigurationRequest.builder()
        .accountId(sourceAccountId)
        .configId(configurationId)
        .storageLensConfiguration(configuration)
        .tags(tags)
        .build()
    );

} catch (AwsServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
```

Per accedere ai gruppi di S3 Storage Lens o ai prefissi estesi, devi aggiornare la dashboard per utilizzare il livello avanzato. Si applicano costi aggiuntivi. Per ulteriori informazioni sui livelli gratuito e avanzato, consulta [Selezione delle metriche](#). Per ulteriori informazioni sui gruppi S3 Storage Lens, consulta [the section called “Operazioni con i gruppi Storage Lens”](#).

Aggiornare la dashboard di Amazon S3 Storage Lens

La dashboard predefinita di Amazon S3 Storage Lens è default-account-dashboard. Questo pannello di controllo è preconfigurato da Amazon S3 per aiutarti a visualizzare informazioni dettagliate di riepilogo e tendenze per i parametri avanzati e gratuiti aggregati dell'intero account nella console. Non puoi modificare l'ambito di configurazione del pannello di controllo predefinito, ma puoi aggiornare la selezione dei parametri dai parametri gratuiti ai suggerimenti e ai parametri avanzati a pagamento, configurare l'esportazione facoltativa dei parametri o addirittura disabilitare il pannello

di controllo predefinito. La dashboard predefinita non può essere eliminata, ma solo disattivata. Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

Utilizzo della console S3

Attieniti alla procedura seguente per aggiornare un pannello di controllo Amazon S3 Storage Lens sulla console Amazon S3.

Passaggio 1: aggiorna la dashboard e configura le impostazioni generali

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Storage Lens, Pannelli di controllo).
3. Scegli la dashboard che desideri modificare.
4. Scegli Visualizza configurazione del pannello di controllo.
5. Scegli Modifica. Ora puoi rivedere la configurazione della dashboard, passo dopo passo. Per apportare modifiche a uno qualsiasi dei passaggi, puoi scegliere il passaggio direttamente utilizzando la barra di navigazione a sinistra. Per istruzioni su come aggiornare questi passaggi,

Note

Non è possibile modificare quanto segue:

- Il nome del pannello di controllo
- La regione di origine

6. Nella pagina Dashboard, nella sezione Generale, puoi apportare modifiche a quanto segue:
 - Scegli **Abilitato** o **Disabilitato** per aggiornare se ricevi metriche giornaliere nella dashboard.
 - (Facoltativo) Puoi scegliere di aggiungere tag alla tua dashboard. I tag possono essere utilizzati per gestire le autorizzazioni per il pannello di controllo e tenere traccia dei costi per S3 Storage Lens. Per ulteriori informazioni, consulta [Controllare l'accesso alle AWS risorse utilizzando i tag](#) nella Guida per l'utente IAM e [Utilizzo dei tag AWS generati](#) nella Guida per l'AWS Billing utente.

 Note

Puoi aggiungere fino a 50 tag alla configurazione del pannello di controllo.

7. Scegli **Avanti** per salvare le modifiche e procedere.

Passaggio 2: aggiorna l'ambito del dashboard

1. Nella sezione **Ambito del dashboard**, aggiorna le regioni e i bucket che desideri che S3 Storage Lens includa o escluda nella dashboard.

 Note

- Puoi anche includere o escludere Regioni e bucket. Questa opzione è limitata alle Regioni solo se si creano dashboard a livello di organizzazione tra gli account membri dell'organizzazione.
- Puoi scegliere fino a 50 bucket da includere o escludere.

2. Scegli i bucket nelle regioni selezionate che desideri siano inclusi o esclusi da S3 Storage Lens. Puoi includere o escludere i bucket, ma non puoi eseguire entrambe le operazioni. Questa opzione non è disponibile quando crei dashboard a livello di organizzazione.

 Note

- Puoi anche includere o escludere Regioni e bucket. Questa opzione è limitata alle Regioni solo se si creano dashboard a livello di organizzazione tra gli account membri dell'organizzazione.
- Puoi scegliere fino a 50 bucket da includere o escludere.

3. Scegli **Avanti** per salvare le modifiche e procedere.

Fase 3: Aggiornamento del livello Storage Lens Configurazione della selezione delle metriche

1. Nella sezione di selezione delle metriche del livello Storage Lens, aggiorna il livello di metriche che desideri aggregare per questa dashboard.

 Note

- Se stai effettuando l'aggiornamento dal livello gratuito al livello Avanzato, dovrai aggiornare le impostazioni di aggregazione delle metriche. Per aggiornare le impostazioni di aggregazione delle metriche, consulta la Fase 4: Aggiornamento dell'aggregazione delle metriche.
- Se stai aggiornando il livello Storage Lens dal livello Advanced al livello Free, non dovrai aggiornare alcuna impostazione di aggregazione delle metriche. La funzione di aggregazione delle metriche si applica solo alle categorie di metriche di livello avanzato.

2. Per includere metriche gratuite aggregate a livello di bucket e disponibili per le query per 14 giorni, scegli il livello gratuito.
3. Per abilitare le metriche avanzate, scegli il livello avanzato. Queste opzioni includono l'aggregazione dei prefissi, la CloudWatch pubblicazione su Amazon e i consigli contestuali. I dati sono disponibili per le query per 15 mesi. I parametri e i suggerimenti avanzati hanno un costo aggiuntivo. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Per ulteriori informazioni su parametri avanzati e parametri gratuiti, consulta [Selezione delle metriche](#).

4. In Categorie di metriche avanzate, scegli la categoria di metriche che desideri abilitare:
 - Parametri delle attività
 - Detailed status code metrics (Parametri dettagliati codice di stato)
 - Metriche di ottimizzazione dei costi
 - Metriche di protezione dei dati
 - Metriche delle prestazioni

Per visualizzare in anteprima quali metriche sono incluse in ciascuna categoria, utilizza il pulsante freccia a discesa sotto l'elenco delle caselle di controllo della categoria delle metriche. Per ulteriori informazioni sulle categorie di parametri, consulta [Categorie di parametri](#). Per un elenco completo di parametri, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

5. Scegli o specifica un delimitatore di prefisso per distinguere i livelli all'interno di ciascun prefisso. Questo valore viene utilizzato per identificare ogni livello di prefisso. Il valore predefinito

in Amazon S3 è il carattere "/", ma la struttura di storage potrebbe utilizzare altri caratteri delimitatori.

6. Scegli **Avanti** per salvare le modifiche e procedere.

Fase 4: (Facoltativo) Aggiorna l'aggregazione delle metriche

1. In **Aggregazione delle metriche** aggiuntive, aggiorna le metriche che desideri aggregare scegliendo una delle seguenti opzioni:
 - Aggregazione di prefisso
 - Aggregazione dei gruppi Storage Lens
2. Se hai abilitato l'aggregazione dei prefissi, specifica la soglia minima del prefisso per la dashboard e la profondità del prefisso. Quindi, scegli **Avanti** per salvare e procedere.
3. Se hai abilitato l'aggregazione di gruppi Storage Lens, scegli una delle seguenti opzioni:
 - Includi gruppi Storage Lens
 - Escludere i gruppi Storage Lens
4. Quando includi i gruppi Storage Lens nell'aggregazione, puoi includere tutti i gruppi Storage Lens nella tua regione principale o specificare i gruppi Storage Lens da includere.
5. Scegli **Avanti** per salvare le modifiche e procedere.

Passaggio 5: (Facoltativo) Aggiorna le impostazioni di esportazione e pubblicazione delle metriche

1. In **Pubblicazione delle metriche**, scegli la **CloudWatch pubblicazione** se desideri accedere alle metriche di Storage Lens nella dashboard. CloudWatch

Note

Prefix-level le metriche non sono disponibili in. CloudWatch

2. In **Esportazione delle metriche**, scegli i dati del dashboard di Storage Lens che desideri esportare giornalmente:
 - Rapporto sulle metriche predefinito
 - Rapporto sulle metriche dei prefissi espanso

3. (Facoltativo) Se hai scelto il rapporto sulle metriche predefinite, nelle Impostazioni del rapporto sulle metriche predefinite, scegli il tipo di bucket. Puoi esportare il report in un bucket S3 generico o in un bucket di tabelle S3 di sola lettura. In base al tipo di bucket selezionato, aggiorna le opzioni Impostazioni di destinazione del bucket per uso generico o Table bucket destination settings.

Note

- Il rapporto sulle metriche predefinito include solo i prefissi all'interno della soglia e della profondità impostate nelle impostazioni di aggregazione dei prefissi. Se l'aggregazione dei prefissi non è già configurata, la soglia include fino a 100 prefissi più grandi per dimensione.
- Se scegli di specificare una chiave di crittografia, devi scegliere una chiave (SSE-KMS) o una AWS KMS chiave gestita da Amazon S3 (). SSE-S3 Se la policy del bucket di destinazione richiede la crittografia, devi fornire una chiave di crittografia per l'esportazione delle metriche. Senza la chiave di crittografia, l'esportazione in S3 non riesce. Per ulteriori informazioni, consulta [Utilizzando un AWS KMS key per crittografare le esportazioni delle metriche](#).

4. Scegli Avanti per salvare le modifiche e procedere.
5. (Facoltativo) Se hai scelto il rapporto sulle metriche dei prefissi espansi, nelle impostazioni del rapporto sulle metriche dei prefissi espansi, scegli il tipo di bucket. Puoi esportare il report in un bucket S3 generico o in un bucket di tabelle S3 di sola lettura. In base al tipo di bucket selezionato, aggiorna le impostazioni di destinazione del bucket per uso generico o le impostazioni di destinazione del bucket Table.

Note

- Il rapporto sulle metriche dei prefissi estesi include i prefissi in tutti i bucket specificati nell'ambito della dashboard.
- Se scegli di specificare una chiave di crittografia, devi scegliere una chiave (SSE-KMS) o una AWS KMS chiave gestita da Amazon S3 (). SSE-S3 Se la policy del bucket di destinazione richiede la crittografia, devi fornire una chiave di crittografia per l'esportazione delle metriche. Senza la chiave di crittografia, l'esportazione in

S3 non riesce. Per ulteriori informazioni, consulta [Utilizzando un AWS KMS key per crittografare le esportazioni delle metriche](#).

6. Scegli **Avanti** per salvare le modifiche e procedere.

Passaggio 6: rivedi e aggiorna la configurazione della dashboard

1. Nella sezione **Generale**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
2. Nella sezione **Ambito della Dashboard**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
3. Nella sezione **Storage Lens tier**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
4. Nella sezione **Aggregazione delle metriche**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
5. Nella sezione **Esportazione delle metriche**, rivedi le tue impostazioni. Scegli **Modifica** per apportare modifiche.
6. Dopo aver esaminato e confermato tutte le impostazioni di configurazione della dashboard, scegli **Invia** per aggiornare la dashboard.

Dopo aver aggiornato con successo la nuova dashboard di Storage Lens, puoi visualizzare la configurazione aggiornata della dashboard elencata nella pagina **Storage Lens Dashboard**.

Utilizzo di AWS CLI

Example

Il seguente esempio di comando aggiorna la configurazione della dashboard di Amazon S3 Storage Lens. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --  
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-  
configuration=file:///./config.json --tags=file:///./tags.json
```

Utilizzo di AWS SDK per Java

Example- Aggiornare la configurazione di Amazon S3 Storage Lens con metriche e raccomandazioni avanzate

Gli esempi seguenti mostrano come aggiornare la configurazione predefinita di S3 Storage Lens con metriche e raccomandazioni avanzate in SDK per Java:

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSE3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateDefaultConfigWithPaidFeatures {

    public static void main(String[] args) {
        String configurationId = "default-account-dashboard"; // This configuration ID
        cannot be modified.
```

```
String sourceAccountId = "111122223333";

try {
    SelectionCriteria selectionCriteria = new SelectionCriteria()
        .withDelimiter("/")
        .withMaxDepth(5)
        .withMinStorageBytesPercentage(10.0);
    PrefixLevelStorageMetrics prefixStorageMetrics = new
PrefixLevelStorageMetrics()
        .withIsEnabled(true)
        .withSelectionCriteria(selectionCriteria);
    BucketLevel bucketLevel = new BucketLevel()
        .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
        .withPrefixLevel(new
PrefixLevel().withStorageMetrics(prefixStorageMetrics));
    AccountLevel accountLevel = new AccountLevel()
        .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
        .withBucketLevel(bucketLevel);

    StorageLensConfiguration configuration = new StorageLensConfiguration()
        .withId(configurationId)
        .withAccountLevel(accountLevel)
        .withIsEnabled(true);

    AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
        .withCredentials(new ProfileCredentialsProvider())
        .withRegion(US_WEST_2)
        .build();

    s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
        .withAccountId(sourceAccountId)
        .withConfigId(configurationId)
        .withStorageLensConfiguration(configuration)
    );

} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
```

```
}  
  }  
}
```

Per accedere ai gruppi di S3 Storage Lens o ai prefissi estesi, devi aggiornare la dashboard per utilizzare il livello avanzato. Si applicano costi aggiuntivi. Per ulteriori informazioni sui livelli gratuito e avanzato, consulta [Selezione delle metriche](#). Per ulteriori informazioni sui gruppi S3 Storage Lens, consulta [the section called “Operazioni con i gruppi Storage Lens”](#).

Disattivare la dashboard di Amazon S3 Storage Lens

È possibile disattivare una dashboard Amazon S3 Storage Lens dalla console Amazon S3. La disabilitazione di una dashboard ne impedisce la generazione di metriche in futuro. Un pannello di controllo disabilitato conserva ancora le informazioni di configurazione, in modo che possano essere facilmente richiamate in caso di riattivazione. Un pannello di controllo disabilitato conserva i dati della cronologia fino a quando non sarà più disponibile per le query.

Utilizzo della console S3

Procedere come segue per disattivare una dashboard Amazon S3 Storage Lens sulla console Amazon S3.

Per disabilitare una dashboard Amazon S3 Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco delle dashboard, scegli la dashboard che desideri disabilitare, quindi scegli Disabilita.
4. Nella pagina visualizzata, conferma che desideri realmente disabilitare il pannello di controllo specificando il nome del pannello di controllo nel campo di testo, quindi seleziona Conferma.

Eliminare la dashboard di Amazon S3 Storage Lens

Non puoi eliminare il pannello di controllo predefinito. Tuttavia, è possibile effettuarne la disabilitazione. Prima di eliminare un pannello di controllo che hai creato in precedenza, considera quanto segue:

- In alternativa all'eliminazione di un pannello di controllo, puoi disabilitarlo in modo che sia disponibile per una riattivazione in futuro. Per ulteriori informazioni, consulta [Utilizzo della console S3](#).
- L'eliminazione del pannello di controllo comporta l'eliminazione di tutte le impostazioni di configurazione ad esso associate.
- I dati delle metriche della cronologia non saranno più disponibili. Questi dati storici sono ancora conservati per 15 mesi. Se desideri accedere nuovamente a questi dati, dovrai creare un pannello di controllo con lo stesso nome nella stessa regione di origine di quella eliminata.

Utilizzo della console S3

È possibile eliminare una dashboard Amazon S3 Storage Lens dalla console Amazon S3. Tuttavia, l'eliminazione di una dashboard ne impedisce la generazione di metriche in futuro.

Eliminazione di un pannello di controllo di Amazon S3 Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco delle dashboard, scegli la dashboard che desideri eliminare, quindi scegli Elimina.
4. Nella pagina Elimina pannelli di controllo conferma di voler realmente eliminare il pannello di controllo specificandone il nome nel campo di testo. Quindi scegli Conferma.

Utilizzo di AWS CLI

Example

L'esempio seguente elimina una configurazione di S3 Storage Lens. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control delete-storage-lens-configuration --account-id=222222222222 --region=us-east-1 --config-id=your-configuration-id
```

Utilizzo di AWS SDK per Java

Example- Eliminazione di una configurazione della dashboard Amazon S3 Storage Lens

L'esempio seguente mostra come eliminare una configurazione di S3 Storage Lens utilizzando SDK per Java:

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class DeleteDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();

            s3ControlClient.deleteStorageLensConfiguration(new
DeleteStorageLensConfigurationRequest()
                .withAccountId(sourceAccountId)
                .withConfigId(configurationId)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```



```
}
```

Elenco delle dashboard di Amazon S3 Storage Lens

Utilizzo della console S3

Per elencare le dashboard di S3 Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli Dashboard. Ora puoi visualizzare le dashboard nel tuo Account AWS

Utilizzo di AWS CLI

Example

Il seguente comando di esempio elenca le dashboard di S3 Storage Lens nel tuo Account AWS. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1 --next-token=abcdefghijkl1234
```

Example

L'esempio seguente elenca le configurazioni di S3 Storage Lens senza un token successivo. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1
```

Utilizzo di AWS SDK per Java

Example- Elenco delle configurazioni della dashboard S3 Storage Lens

Gli esempi seguenti mostrano come elencare le configurazioni di S3 Storage Lens in SDK per Java. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate. a ogni descrizione di esempio.

```
package aws.example.s3control;
```

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationEntry;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationsRequest;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class ListDashboard {

    public static void main(String[] args) {
        String sourceAccountId = "111122223333";
        String nextToken = "nextToken";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();

            final List<ListStorageLensConfigurationEntry> configurations =
                s3ControlClient.listStorageLensConfigurations(new
ListStorageLensConfigurationsRequest()
                    .withAccountId(sourceAccountId)
                    .withNextToken(nextToken)
                ).getStorageLensConfigurationList();

            System.out.println(configurations.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

```
}
```

Visualizzare i dettagli della configurazione della dashboard di Amazon S3 Storage Lens

Puoi visualizzare una dashboard di Amazon S3 Storage Lens dalla console Amazon S3 e l'SDK per AWS CLI Java.

Utilizzo della console S3

Per visualizzare i dettagli della configurazione della dashboard di S3 Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli Dashboard.
4. Dall'elenco delle dashboard, scegli la dashboard che desideri visualizzare. È ora possibile visualizzare i dettagli della dashboard di Storage Lens.

Utilizzo di AWS CLI

Example

L'esempio seguente recupera una configurazione di S3 Storage Lens in modo da poterne visualizzare i dettagli. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control get-storage-lens-configuration --account-id=222222222222 --config-id=your-configuration-id --region=us-east-1
```

Utilizzo di AWS SDK per Java

Example- Recuperare e visualizzare una configurazione S3 Storage Lens

L'esempio seguente mostra come recuperare la configurazione di un S3 Storage Lens in SDK for Java, in modo da poterne visualizzare i dettagli. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;
```

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationResult;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();

            final StorageLensConfiguration configuration =
                s3ControlClient.getStorageLensConfiguration(new
GetStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                ).getStorageLensConfiguration();

            System.out.println(configuration.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Gestione AWS tag delle risorse con S3 Storage Lens

Ogni dashboard di Amazon S3 Storage Lens viene conteggiata come AWS risorsa con il proprio Amazon Resource Name (ARN). Pertanto, quando configuri la dashboard di Storage Lens, puoi facoltativamente aggiungere tag di AWS risorse alla dashboard. È possibile aggiungere fino a 50 tag per ogni dashboard di Storage Lens. Per creare una dashboard Storage Lens con tag, è necessario disporre delle seguenti [Autorizzazioni S3 Storage Lens](#):

- `s3:ListStorageLensConfigurations`
- `s3:GetStorageLensConfiguration`
- `s3:GetStorageLensConfigurationTagging`
- `s3:PutStorageLensConfiguration`
- `s3:PutStorageLensConfigurationTagging`

È possibile utilizzare i tag AWS delle risorse per classificare le risorse in base al reparto, alla linea di business o al progetto. Questa funzione è utile quando si dispone di numerose risorse dello stesso tipo. Applicando i tag, è possibile identificare rapidamente una specifica dashboard S3 Storage Lens in base ai tag assegnati. È possibile utilizzare i tag anche per monitorare e allocare i costi.

Inoltre, quando aggiungi un tag di AWS risorsa alla dashboard di Storage Lens, attivi il controllo degli accessi [basato sugli attributi \(ABAC\)](#). ABAC è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi come i tag. Puoi anche utilizzare condizioni che specificano i tag delle risorse nelle tue policy IAM per [controllare l'accesso alle risorse. AWS](#)

Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Inoltre, tieni presente le limitazioni seguenti:

- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole.
- Se aggiungi un tag con la stessa chiave di un tag esistente su quella risorsa, il nuovo valore sovrascrive il vecchio valore.
- Se elimini una risorsa, verranno eliminati anche tutti i tag a essa associati.
- Non includere dati privati o sensibili nei tag delle AWS risorse.
- I tag di sistema (con chiavi di tag che iniziano con `aws:`) non sono supportati.
- La lunghezza di ogni chiave di tag non può superare i 128 caratteri. La lunghezza di ogni valore di tag non può superare i 256 caratteri.

Gli esempi seguenti dimostrano come utilizzare i tag AWS delle risorse con la dashboard di Storage Lens.

Argomenti

- [Add \(Aggiungi\) AWS tag di risorse in una dashboard di Storage Lens](#)
- [Retrieve AWS tag di risorse per una dashboard di Storage Lens](#)
- [Aggiornamento dei tag della dashboard di Storage Lens](#)
- [Eliminazione in corso AWS tag di risorse da una dashboard di S3 Storage Lens](#)

Add (Aggiungi) AWS tag di risorse in una dashboard di Storage Lens

Gli esempi seguenti mostrano come aggiungere tag di AWS risorse a una dashboard di S3 Storage Lens. Puoi aggiungere tag di risorse utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e. AWS SDK per Java

Utilizzo della console S3

Per aggiungere AWS tag di risorse in una dashboard di Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione sinistro, spostarsi su Storage Lens nel pannello di navigazione sinistro.
3. Scegli Dashboard.
4. Scegli il pulsante di opzione per la dashboard Storage Lens che si desidera aggiornare. Quindi scegli Edit (Modifica).
5. In Generale, scegli Aggiungi tag.
6. Nella pagina Aggiungi tag, aggiungere la nuova coppia chiave-valore.

Note

Aggiungendo un tag la cui chiave è la stessa di un tag esistente viene sovrascritto il valore del tag precedente.

7. (Facoltativo) Per aggiungere più di un nuovo tag, scegliete nuovamente Aggiungi tag e aggiungi nuove voci. Puoi aggiungere fino a 50 tag di AWS risorse alla dashboard di Storage Lens.

8. (Facoltativo) Se desideri rimuovere un tag appena aggiunto, scegli Rimuovi accanto al tag che desideri eliminare.
9. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Example

Il seguente esempio di comando aggiunge tag a una configurazione della dashboard S3 Storage Lens. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control put-storage-lens-configuration-tagging --account-id=222222222222 --  
region=us-east-1 --config-id=your-configuration-id --tags=file:///./tags.json
```

Utilizzo di AWS SDK per Java

L'esempio seguente aggiunge tag a una configurazione di Amazon S3 Storage Lens in SDK per Java. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

Example- Aggiungere tag a una configurazione di S3 Storage Lens

```
package aws.example.s3control;  
  
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import com.amazonaws.auth.profile.ProfileCredentialsProvider;  
import com.amazonaws.services.s3control.AWSS3Control;  
import com.amazonaws.services.s3control.AWSS3ControlClient;  
import  
    com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;  
import com.amazonaws.services.s3control.model.StorageLensTag;  
  
import java.util.Arrays;  
import java.util.List;  
  
import static com.amazonaws.regions.Regions.US_WEST_2;  
  
public class PutDashboardTagging {
```

```
public static void main(String[] args) {
    String configurationId = "ConfigurationId";
    String sourceAccountId = "111122223333";

    try {
        List<StorageLensTag> tags = Arrays.asList(
            new StorageLensTag().withKey("key-1").withValue("value-1"),
            new StorageLensTag().withKey("key-2").withValue("value-2")
        );

        AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
            .withCredentials(new ProfileCredentialsProvider())
            .withRegion(US_WEST_2)
            .build();

        s3ControlClient.putStorageLensConfigurationTagging(new
PutStorageLensConfigurationTaggingRequest()
            .withAccountId(sourceAccountId)
            .withConfigId(configurationId)
            .withTags(tags)
        );
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it and returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
```

Retrieve AWS tag di risorse per una dashboard di Storage Lens

Gli esempi seguenti dimostrano come recuperare i tag AWS delle risorse per una dashboard S3 Storage Lens. Puoi ottenere i tag delle risorse utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e. AWS SDK per Java

Utilizzo della console S3

Per recuperare il AWS tag delle risorse per una dashboard di Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli Dashboard.
4. Scegli il pulsante di opzione per la configurazione della dashboard Storage Lens che si desidera visualizzare. Quindi, scegli Visualizza configurazione dashboard.
5. In Tag, esaminare i tag associati alla dashboard.
6. (Facoltativo) Se si desidera aggiungere un nuovo tag, scegli Modifica. Quindi scegli Aggiungi tag. Nella pagina Aggiungi tag, aggiungere la nuova coppia chiave-valore.

Note

Aggiungendo un tag la cui chiave è la stessa di un tag esistente viene sovrascritto il valore del tag precedente.

7. (Facoltativo) Se desideri rimuovere un tag appena aggiunto, scegli Rimuovi accanto al tag che desideri eliminare.
8. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Example

Il seguente esempio di comando recupera i tag per una configurazione della dashboard S3 Storage Lens. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control get-storage-lens-configuration-tagging --account-id=222222222222 --  
region=us-east-1 --config-id=your-configuration-id --tags=file:///./tags.json
```

Utilizzo di AWS SDK per Java

Example- Ottenere i tag per una configurazione della dashboard S3 Storage Lens

L'esempio seguente mostra come recuperare i tag per una configurazione della dashboard S3 Storage Lens in SDK per Java. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;
import
    com.amazonaws.services.s3control.model.GetStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();

            final List<StorageLensTag> s3Tags = s3ControlClient
                .getStorageLensConfigurationTagging(new
                    GetStorageLensConfigurationTaggingRequest()
                        .withAccountId(sourceAccountId)
                        .withConfigId(configurationId)
                    ).getTags();

            System.out.println(s3Tags.toString());
        }
    }
}
```

```
    } catch (AmazonServiceException e) {  
        // The call was transmitted successfully, but Amazon S3 couldn't process  
        // it and returned an error response.  
        e.printStackTrace();  
    } catch (SdkClientException e) {  
        // Amazon S3 couldn't be contacted for a response, or the client  
        // couldn't parse the response from Amazon S3.  
        e.printStackTrace();  
    }  
}  
}
```

Aggiornamento dei tag della dashboard di Storage Lens

I seguenti esempi dimostrano come aggiornare i tag del dashboard di Storage Lens utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java

Utilizzo della console S3

Per aggiornare un AWS tag di risorsa per una dashboard di Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli Dashboard.
4. Scegli il pulsante di opzione per la configurazione della dashboard Storage Lens che si desidera visualizzare. Quindi, scegli Visualizza configurazione dashboard.
5. In Tag, esaminare i tag associati alla dashboard.
6. (Facoltativo) Se si desidera aggiungere un nuovo tag, scegli Modifica. Quindi scegli Aggiungi tag. Nella pagina Aggiungi tag, aggiungere la nuova coppia chiave-valore.

Note

Aggiungendo un tag la cui chiave è la stessa di un tag esistente viene sovrascritto il valore del tag precedente.

7. (Facoltativo) Se desideri rimuovere un tag appena aggiunto, scegli Rimuovi accanto al tag che desideri eliminare.
8. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Example

Il seguente esempio di comando aggiunge o sostituisce i tag in una configurazione esistente della dashboard Amazon S3 Storage Lens. Per utilizzare questi esempi, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control put-storage-lens-configuration-tagging --account-id=111122223333 --  
config-id=example-dashboard-configuration-id --region=us-east-1 --config-id=your-  
configuration-id
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente aggiorna i tag AWS delle risorse su una dashboard Storage Lens esistente. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

Example- Aggiornare i tag su una configurazione della dashboard Storage Lens esistente

```
package aws.example.s3control;  
  
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import com.amazonaws.auth.profile.ProfileCredentialsProvider;  
import com.amazonaws.services.s3control.AWSS3Control;  
import com.amazonaws.services.s3control.AWSS3ControlClient;  
import  
    com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;  
import com.amazonaws.services.s3control.model.StorageLensTag;  
  
import java.util.Arrays;  
import java.util.List;  
  
import static com.amazonaws.regions.Regions.US_WEST_2;  
  
public class PutDashboardTagging {  
  
    public static void main(String[] args) {  
        String configurationId = "ConfigurationId";  
        String sourceAccountId = "111122223333";  
  
        try {
```

```
List<StorageLensTag> tags = Arrays.asList(
    new StorageLensTag().withKey("key-1").withValue("value-1"),
    new StorageLensTag().withKey("key-2").withValue("value-2")
);

AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
    .withCredentials(new ProfileCredentialsProvider())
    .withRegion(US_WEST_2)
    .build();

s3ControlClient.putStorageLensConfigurationTagging(new
PutStorageLensConfigurationTaggingRequest()
    .withAccountId(sourceAccountId)
    .withConfigId(configurationId)
    .withTags(tags)
);
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
```

Eliminazione in corso AWS tag di risorse da una dashboard di S3 Storage Lens

I seguenti esempi dimostrano come eliminare i tag AWS delle risorse da una dashboard Storage Lens esistente. Puoi eliminare i tag utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

Per eliminare AWS tag di risorse da una dashboard Storage Lens esistente

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli Dashboard.

4. Scegli il pulsante di opzione per la configurazione della dashboard Storage Lens che si desidera visualizzare. Quindi, scegli Visualizza configurazione dashboard.
5. In Tag, esaminare i tag associati alla dashboard.
6. Scegli Rimuovi accanto al tag che si desidera rimuovere.
7. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Il AWS CLI comando seguente elimina i tag AWS delle risorse da una dashboard Storage Lens esistente. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

Example

```
aws s3control delete-storage-lens-configuration-tagging --account-id=222222222222 --  
config-id=your-configuration-id --region=us-east-1
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente elimina un tag di AWS risorsa dalla dashboard di Storage Lens utilizzando l'Amazon Resource Name (ARN) specificato nell'account. *111122223333* Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

Example- Eliminazione dei tag per una configurazione della dashboard S3 Storage Lens

```
package aws.example.s3control;  
  
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import com.amazonaws.auth.profile.ProfileCredentialsProvider;  
import com.amazonaws.services.s3control.AWSS3Control;  
import com.amazonaws.services.s3control.AWSS3ControlClient;  
import  
    com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationTaggingRequest;  
  
import static com.amazonaws.regions.Regions.US_WEST_2;  
  
public class DeleteDashboardTagging {  
  
    public static void main(String[] args) {  
        String configurationId = "ConfigurationId";
```

```
String sourceAccountId = "111122223333";
try {
    AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
        .withCredentials(new ProfileCredentialsProvider())
        .withRegion(US_WEST_2)
        .build();

    s3ControlClient.deleteStorageLensConfigurationTagging(new
DeleteStorageLensConfigurationTaggingRequest()
        .withAccountId(sourceAccountId)
        .withConfigId(configurationId)
    );
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
```

File helper per l'utilizzo di Amazon S3 Storage Lens

Utilizza i seguenti file JSON e i suoi input chiave per i tuoi esempi.

Esempio di configurazione di S3 Storage Lens in JSON

Example **config.json**

Il `config.json` file contiene i dettagli di una configurazione Organizations-level avanzata di metriche e raccomandazioni di S3 Storage Lens. Per utilizzare il seguente esempio, sostituisci *user input placeholders* con le tue informazioni.

Note

Per i suggerimenti e i parametri avanzati verranno applicati costi aggiuntivi. Per ulteriori informazioni, consulta [Parametri e suggerimenti avanzati](#).

```
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for AWS Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
  },
  "BucketLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
  },
  "PrefixLevel":{
    "StorageMetrics":{
      "IsEnabled":true,
      "SelectionCriteria":{
        "MaxDepth":5,
        "MinStorageBytesPercentage":1.25,
        "Delimiter":"/"
      }
    }
  }
}
```



```

},
"Exclude": { //Replace with "Include" if you prefer to include Regions.
  "Regions": [
    "eu-west-1"
  ],
  "Buckets": [ //This attribute is not supported for AWS Organizations-level
configurations.
    "arn:aws:s3:::amzn-s3-demo-source-bucket"
  ]
},
"IsEnabled": true, //Whether the configuration is enabled
"DataExport": { //Details about the metrics export
  "S3BucketDestination": {
    "OutputSchemaVersion": "V_1",
    "Format": "CSV", //You can add "Parquet" if you prefer.
    "AccountId": "111122223333",
    "Arn": "arn:aws:s3:::
amzn-s3-demo-destination-bucket", // The destination bucket for your metrics export
must be in the same Region as your S3 Storage Lens configuration.
    "Prefix": "prefix-for-your-export-destination",
    "Encryption": {
      "SSES3": {}
    }
  },
  "CloudWatchMetrics": {
    "IsEnabled": true
  }
}
}
}

```

Esempio di configurazione di S3 Storage Lens con gruppi Storage Lens in JSON

Example **config.json**

Il file `config.json` contiene i dettagli da applicare alla configurazione di Storage Lens quando si usano i gruppi Storage Lens. Per usare questo esempio, sostituisci *user input placeholders* con le tue informazioni.

Per collegare tutti i gruppi Storage Lens al pannello di controllo, aggiorna la configurazione di Storage Lens con la seguente sintassi:

```

{
  "Id": "ExampleS3StorageLensConfiguration",

```

```

"AccountLevel": {
  "ActivityMetrics": {
    "IsEnabled":true
  },
  "AdvancedCostOptimizationMetrics": {
    "IsEnabled":true
  },
  "AdvancedDataProtectionMetrics": {
    "IsEnabled":true
  },
  "BucketLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "StorageLensGroupLevel": {},
    "IsEnabled": true
  }
}

```

Per includere solo due gruppi Storage Lens nella configurazione (*slg-1* e *slg-2*) del dashboard di Storage Lens, utilizza la seguente sintassi:

```

{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true
      },
      "StorageLensGroupLevel": {
        "SelectionCriteria": {
          "Include": [
            "arn:aws:s3:us-east-1:111122223333:storage-lens-group/sl-g-1",
            "arn:aws:s3:us-east-1:444455556666:storage-lens-group/sl-g-2"
          ]
        }
      }
    }
  }
}

```

```
    },
    "IsEnabled": true
  }
}
```

Per escludere solo alcuni gruppi Storage Lens dalla configurazione del pannello di controllo, utilizza la seguente sintassi:

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled": true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled": true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled": true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled": true
      },
      "StorageLensGroupLevel": {
        "SelectionCriteria": {
          "Exclude": [
            "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
            "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
          ]
        }
      },
      "IsEnabled": true
    }
  }
}
```

File JSON con tag per configurazione di esempio di S3 Storage Lens

Example **tags.json**

Il file `tags.json` contiene i tag da applicare alla configurazione di S3 Storage Lens. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
[
  {
```

```
    "Key": "key1",
    "Value": "value1"
  },
  {
    "Key": "key2",
    "Value": "value2"
  }
]
```

Esempio di configurazione delle autorizzazioni IAM di S3 Storage Lens

Example **permissions.json** — Nome specifico del pannello di controllo

Questa policy di esempio mostra il file `permissions.json` IAM di S3 Storage Lens con un nome specificato per il pannello di controllo. Sostituisci *value1*, *us-east-1*, *your-dashboard-name* e *example-account-id* con il tuo valore.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetStorageLensConfiguration",
        "s3:DeleteStorageLensConfiguration",
        "s3:PutStorageLensConfiguration"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/key1": "value1"
        }
      },
      "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens/your-  
dashboard-name"
    }
  ]
}
```

Example **permissions.json** — Nessun nome specifico del pannello di controllo

Questa policy di esempio mostra il file `permissions.json` IAM di S3 Storage Lens senza un nome specificato per il pannello di controllo. Sostituisci *value1*, *us-east-1* e *example-account-id* con il tuo valore.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetStorageLensConfiguration",
        "s3:DeleteStorageLensConfiguration",
        "s3:PutStorageLensConfiguration"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/key1": "value1"
        }
      },
      "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens/*"
    }
  ]
}
```

Visualizzazione dei parametri con Amazon S3 Storage Lens

S3 Storage Lens aggrega i tuoi parametri e mostra le informazioni nella sezione Account snapshot (Snapshot dell'account) nella pagina Buckets (Bucket) della console Amazon S3. S3 Storage Lens fornisce anche una dashboard interattiva che puoi utilizzare per visualizzare informazioni e tendenze, segnalare i valori anomali e ricevere consigli per ottimizzare i costi di archiviazione e applicare le migliori pratiche di protezione dei dati. La dashboard offre opzioni di approfondimento per generare e visualizzare informazioni dettagliate a livello di organizzazione, account, classe di archiviazione, bucket Regione AWS, prefisso o gruppo Storage Lens. Puoi anche inviare un rapporto giornaliero sulle metriche in Parquet formato CSV o a un bucket S3 generico o esportare le metriche direttamente in un bucket di tabelle S3 gestito. AWS

Per impostazione predefinita, tutti pannelli di controllo sono configurati con parametri gratuiti, che includono i parametri che puoi utilizzare per comprendere l'utilizzo e l'attività dell'archiviazione S3, ottimizzare i costi di archiviazione e implementare le best practice per la protezione dei dati e la gestione degli accessi. I parametri gratuiti vengono aggregate fino al livello del bucket. Con i parametri gratuiti, i dati sono disponibili per le query per un massimo di 14 giorni.

I parametri avanzati e i suggerimenti includono le seguenti funzionalità aggiuntive che puoi utilizzare per ottenere ulteriori informazioni sull'utilizzo e sulle attività a livello di archiviazione, nonché le best practice per ottimizzarlo:

- Suggerimenti contestuali (disponibili solo nel pannello di controllo)
- Parametri avanzati (inclusi i parametri delle attività aggregati per bucket)
- Aggregazione di prefisso
- Aggregazione dei gruppi Storage Lens
- Aggregazione dei gruppi Storage Lens
- Pubblicazione su Amazon CloudWatch

I dati dei parametri avanzati sono disponibili per le query per 15 mesi. Per l'uso di S3 Storage Lens con i parametri avanzati sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni su parametri gratuiti e avanzati, consulta [Selezione delle metriche](#).

Argomenti

- [Visualizzazione dei parametri di S3 Storage Lens nei pannelli di controllo](#)
- [Visualizzazione dei parametri di Amazon S3 Storage Lens utilizzando una esportazione di dati](#)
- [Monitora le metriche di S3 Storage Lens in CloudWatch](#)
- [Casi d'uso relativi ai parametri di Amazon S3 Storage Lens](#)

Visualizzazione dei parametri di S3 Storage Lens nei pannelli di controllo

Nella console di Amazon S3, S3 Storage Lens fornisce un pannello di controllo interattivo predefinito con il quale è possibile visualizzare approfondimenti e tendenze relative ai dati. È possibile utilizzare il pannello di controllo per visualizzare informazioni dettagliate e tendenze, contrassegnare le anomalie e ricevere suggerimenti per ottimizzare i costi di archiviazione e applicare best practice per la protezione dei dati. Nel pannello di controllo sono disponibili opzioni di drill-down per generare e

visualizzare approfondimenti a livello di account, bucket, Regione AWS, prefisso o gruppo Storage Lens. Se hai abilitato S3 Storage Lens a funzionare AWS Organizations, puoi anche generare informazioni a livello di organizzazione (ad esempio dati per tutti gli account che fanno parte della tua AWS Organizations gerarchia). Il pannello di controllo viene sempre caricato per la data più recente per la quale sono disponibili i parametri.

La dashboard predefinita di S3 Storage Lens sulla console è denominato default-account-dashboard. Amazon S3 preconfigura questo pannello di controllo per visualizzare gli approfondimenti di riepilogo e le tendenze per l'intero account e le aggiorna quotidianamente nella console S3. Non è possibile modificare l'ambito di configurazione del pannello di controllo predefinito, ma è possibile aggiornare la selezione dei parametri, dai parametri gratuiti alle raccomandazioni e ai parametri avanzati a pagamento. I parametri avanzati e i suggerimenti ti consentono di accedere a parametri e funzionalità aggiuntive. Queste funzionalità includono categorie metriche avanzate, aggregazione a livello di prefisso, consigli contestuali e pubblicazione su Amazon CloudWatch.

Puoi disabilitare il pannello di controllo predefinito, ma non puoi eliminarlo. In caso di disattivazione del pannello di controllo predefinito, non viene più aggiornato. Non riceverai più alcun nuovo parametro giornaliero in S3 Storage Lens o nella sezione Snapshot dell'account nella pagina Buckets. Puoi comunque visualizzare i dati della cronologia nel pannello di controllo predefinito fino alla scadenza delle query di dati (14 giorni). Questo periodo è di 15 mesi se hai abilitato i parametri avanzati e i suggerimenti. Per accedere a questi dati, puoi riabilitare il pannello di controllo predefinito entro il periodo di scadenza.

Puoi creare dashboard S3 Storage Lens aggiuntive e classificarle per bucket S3 o account. Regioni AWS Puoi anche definire l'ambito delle dashboard per organizzazione se hai abilitato Storage Lens a lavorare con Storage Lens. AWS Organizations Quando crei o modifichi un pannello di controllo di S3 Storage Lens, ne definisci l'ambito e la selezione dei parametri.

Puoi disabilitare o eliminare eventuali pannelli di controllo aggiuntivi creati.

- Se disattivi un pannello di controllo, questo non sarà più aggiornato e non riceverai più nuovi parametri giornalieri. Puoi comunque visualizzare i dati della cronologia per i parametri gratuiti fino al periodo di scadenza di 14 giorni. Se hai abilitato i parametri avanzati e i suggerimenti per il pannello di controllo, questo periodo è di 15 mesi. Per accedere a questi dati, puoi riabilitare il pannello di controllo entro il periodo di scadenza.
- Se si elimina la dashboard, si perdono tutte le impostazioni di configurazione della dashboard. Non riceverai più nuovi parametri giornalieri e perderai anche l'accesso ai dati della cronologia associati a tale pannello di controllo. Se desideri accedere ai dati della cronologia di un pannello di controllo

eliminato, dovrai creare un altro pannello di controllo con lo stesso nome nella stessa regione di origine.

Argomenti

- [Visualizzazione di un pannello di controllo di Amazon S3 Storage Lens](#)
- [Informazioni sul pannello di controllo di S3 Storage Lens](#)

Visualizzazione di un pannello di controllo di Amazon S3 Storage Lens

La seguente procedura descrive come visualizzare un pannello di controllo di S3 Storage Lens nella console S3. Per le procedure dettagliate basate sui casi d'uso che mostrano come utilizzare il pannello di controllo per ottimizzare i costi di archiviazione, implementare le best practice e migliorare le prestazioni delle applicazioni che accedono ai bucket S3, consulta [Casi d'uso relativi ai parametri di Amazon S3 Storage Lens](#).

Note

Non puoi utilizzare le credenziali utente root del tuo account per visualizzare i pannelli di controllo di Amazon S3 Storage Lens. Per accedere alle dashboard di S3 Storage Lens, devi concedere le autorizzazioni AWS Identity and Access Management (IAM) richieste a un utente IAM nuovo o esistente. Quindi, accedi con le credenziali utente per accedere ai pannelli di controllo di S3 Storage Lens. Per ulteriori informazioni, consulta [Impostazione delle autorizzazioni di Amazon S3 Storage Lens](#) e [Best Practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.

Il pannello di controllo si apre in S3 Storage Lens. La sezione Snapshot for date (Snapshot per [data]) mostra l'ultima data in cui S3 Storage Lens ha raccolto i parametri. Il pannello di controllo viene sempre caricato alla data più recente per la quale sono disponibili i parametri.

4. (Facoltativo) Per modificare la data della dashboard di S3 Storage Lens, nel selettore delle date, scegli una nuova data.

5. (Facoltativo) Per applicare filtri temporanei per limitare ulteriormente l'ambito dei dati del pannello di controllo, procedi come segue:
 - a. Espandi la sezione Filtri.
 - b. Per filtrare in base ad account, classi di archiviazione Regioni AWS, bucket, prefissi o gruppi Storage Lens specifici, scegli le opzioni in base alle quali filtrare.
-  **Note**

Il filtro Prefissi e il filtro Gruppi Storage Lens non possono essere applicati contemporaneamente.
- c. Per aggiornare un filtro, scegli Apply (Applica).
 - d. Per rimuovere un filtro, scegli la X accanto al filtro.
 6. In qualsiasi sezione del pannello di controllo di S3 Storage Lens, per visualizzare i dati relativi a un parametro specifico, in Metric (Parametro), scegli il nome del parametro.
 7. In qualsiasi grafico o visualizzazione della dashboard S3 Storage Lens, puoi approfondire i livelli di aggregazione utilizzando le schede Account, Regioni AWS, Classi di archiviazione, Bucket, Prefissi o Gruppi Storage Lens. Per un esempio, consulta [Scoperta dei bucket Amazon S3 freddi](#).

Informazioni sul pannello di controllo di S3 Storage Lens

Il pannello di controllo di S3 Storage Lens è costituito da una scheda Overview (Panoramica) principale e da un massimo di cinque schede aggiuntive che rappresentano ogni livello di aggregazione:

- Account
- Regioni AWS
- Classi di archiviazione
- Bucket
- Prefissi
- Gruppi Storage Lens

Nella scheda Overview (Panoramica), i dati del pannello di controllo vengono aggregati in tre diverse sezioni: Snapshot for date (Snapshot per [data]), Trends and distributions (Tendenze e distribuzioni) e Top N overview (Panoramica primi N).

Per ulteriori informazioni sul pannello di controllo di S3 Storage Lens, consulta le sezioni seguenti.

Istantanea

La sezione Snapshot for date (Snapshot per [data]) mostra i parametri di riepilogo aggregati da S3 Storage Lens per la data selezionata. Questi parametri di riepilogo includono i seguenti parametri:

- Archiviazione totale: la quantità di archiviazione totale utilizzata in byte.
- Conteggio oggetti: il numero totale di oggetti nel tuo Account AWS.
- Dimensione media oggetto: dimensione media dell'oggetto.
- Bucket attivi: numero totale di bucket attivi in uso nel tuo account con archiviazione >0 byte.
- Account: numero di account la cui archiviazione è compresa nell'ambito. Questo valore è 1 a meno che tu non stia utilizzando AWS Organizations e il tuo S3 Storage Lens non abbia un accesso affidabile con un ruolo valido collegato al servizio. Per ulteriori informazioni, consulta [Utilizzo dei ruoli collegati ai servizi per Amazon S3 Storage Lens](#).
- Bucket: il numero totale di bucket nel tuo account.

Dati del parametro

Per ogni parametro visualizzato nello snapshot, puoi visualizzare i seguenti dati:

- Nome parametro: nome del parametro.
- Categoria parametro: categoria in cui è incluso il parametro.
- Totale per data: conteggio totale per la data selezionata.
- % variazione: variazione percentuale rispetto alla data dell'ultimo snapshot.
- Tendenza a 30 giorni: linea di tendenza che mostra le variazioni del parametro in un periodo di 30 giorni.
- Raccomandazione: suggerimento contestuale basato sui dati forniti nello snapshot. I suggerimenti sono disponibili con i parametri avanzati e i suggerimenti. Per ulteriori informazioni, consulta [Raccomandazioni](#).

Categorie di parametri

Facoltativamente, puoi aggiornare la sezione Snapshot for date (Snapshot per [data]) del pannello di controllo per visualizzare i parametri di altre categorie. Se desideri visualizzare i dati snapshot per altri parametri, puoi scegliere altri valori in Metrics categories (Categorie parametri):

- Ottimizzazione dei costi
- Protezione dei dati
- Attività (disponibile con i parametri avanzati)
- Gestione degli accessi
- Prestazioni
- Eventi

La sezione Snapshot for date (Snapshot per [data]) mostra solo una selezione di parametri per ogni categoria. Per visualizzare tutti i parametri di una categoria specifica, scegli il parametro desiderato nelle sezioni Trends and distributions (Tendenze e distribuzioni) o Top N overview (Panoramica primi N). Per ulteriori informazioni sulle categorie di parametri, consulta [Categorie di parametri](#). Per un elenco completo dei parametri di S3 Storage Lens, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

Trends and distributions (Tendenze e distribuzione)

La seconda sezione della scheda Overview (Panoramica) è Trends and distributions (Tendenze e distribuzione). Nella sezione Trends and distributions (Tendenze e distribuzioni), puoi scegliere due parametri da confrontare in un intervallo di date definito. La sezione Trends and distributions (Tendenze e distribuzioni) mostra la relazione tra due parametri nel tempo. In questa sezione sono visualizzati i grafici che puoi utilizzare per visualizzare le distribuzioni Storage class (Classe di archiviazione) e Region (Regione) tra le due tendenze che stai monitorando. Facoltativamente, puoi eseguire il drill-down su un punto dati in uno dei grafici per un'analisi più approfondita.

Per una procedura dettagliata che utilizza la sezione Trends and distributions (Tendenze e distribuzioni), consulta [Identifica i bucket che non utilizzano la crittografia lato server con AWS KMS per la crittografia predefinita \(\) SSE-KMS](#).

Panoramica Top N

La terza sezione del pannello di controllo di S3 Storage Lens è Panoramica Top N (ordinata in ordine crescente o decrescente). Questa sezione mostra le metriche selezionate sul numero principale di account, bucket Regioni AWS, prefissi o gruppi di Storage Lens. Se hai abilitato l'utilizzo di

S3 Storage Lens AWS Organizations, puoi anche visualizzare le metriche selezionate all'interno dell'organizzazione.

Per una procedura dettagliata che utilizza la sezione Top N overview (Panoramica primi N), consulta [Identificare i bucket S3 più grandi](#).

Drill-down e analisi per opzioni

Per fornire un'esperienza fluida nell'esecuzione delle analisi, il pannello di controllo di S3 Storage Lens offre un menu delle azioni, che viene visualizzato quando si sceglie un valore del grafico. Per utilizzare questo menu, seleziona un qualsiasi valore del grafico e scegli tra le due opzioni disponibili nella casella:

- L'azione Drill down (Drill-down) applica il valore selezionato come filtro in tutte le schede del pannello di controllo. Puoi quindi eseguire il drill-down in tale valore per un'analisi più approfondita.
- L'azione Analizza per consente di accedere alla scheda Dimensione selezionata e di applicare tale valore come filtro. Queste schede includono Account, Regioni AWS, Classi di archiviazione, Bucket, Prefissi (per pannelli di controllo con Parametri avanzati e Aggregazione prefissi abilitati) e Gruppi Storage Lens (per i pannelli di controllo con Parametri avanzati e Aggregazione dei gruppi Storage Lens abilitati). Analizza per ti permette di vedere i dati nel contesto della nuova dimensione per un'analisi più approfondita.

Le azioni Drill down e Analizza per potrebbero essere disabilitate se il risultato dovesse produrre valori illogici o nessun valore. Entrambe le azioni Drill down e Analizza per determinano l'applicazione di filtri oltre a qualsiasi altro filtro esistente in tutte le schede del pannello di controllo. È inoltre possibile rimuovere filtri in base alle esigenze.

Schede

Le schede a livello di dimensione forniscono una vista dettagliata di tutti i valori all'interno di una determinata dimensione. Ad esempio, la scheda Regioni AWS mostra i parametri per tutte le Regioni AWS, mentre la scheda Bucket mostra i parametri per tutti i bucket. Ogni scheda dimensione contiene un layout identico costituito da quattro sezioni:

- Un grafico delle tendenze che mostra i primi N elementi all'interno della dimensione negli ultimi 30 giorni per il parametro selezionato. Per impostazione predefinita, questo grafico visualizza i primi 10 elementi, ma è possibile ridurli ad almeno 3 elementi o aumentarli fino a 50 elementi.

- Un istogramma mostra un grafico a barre verticali per la data e il parametro selezionati. Se è presente un numero molto elevato di elementi da visualizzare in questo grafico, potrebbe essere necessario scorrerlo orizzontalmente.
- Un diagramma di analisi a bolle che riporta tutti gli elementi che rientrano in quella dimensione. Questo grafico rappresenta il primo parametro sull'asse x e il secondo parametro sull'asse y. Il terzo parametro è rappresentato dalla dimensione della bolla.
- Una visualizzazione a griglia dei parametri che contiene ogni elemento della dimensione elencata nelle righe. Le colonne rappresentano ogni parametro disponibile, disposti in schede delle categorie di parametri per facilitare la navigazione.

Visualizzazione dei parametri di Amazon S3 Storage Lens utilizzando una esportazione di dati

Le metriche di Amazon S3 Storage Lens vengono generate giornalmente in file di esportazione delle metriche in formato CSV o in Apache Parquet formato CSV e inserite in un bucket S3 generico nel tuo account. Da lì, puoi importare le metriche esportate negli strumenti di analisi di tua scelta, come Amazon Quick e Amazon Athena, dove puoi analizzare l'utilizzo dello storage e le tendenze delle attività. Puoi anche inviare le esportazioni giornaliere delle metriche a un bucket di tabelle S3 AWS gestito per eseguire query immediate, utilizzando servizi di analisi o strumenti di terze parti. AWS

Argomenti

- [Utilizzando un AWS KMS key per crittografare le esportazioni delle metriche](#)
- [Cos'è un manifest di esportazione di S3 Storage Lens?](#)
- [Informazioni sugli schemi di esportazione di Amazon S3 Storage Lens](#)

Utilizzando un AWS KMS key per crittografare le esportazioni delle metriche

Per concedere ad Amazon S3 Storage Lens l'autorizzazione alla crittografia delle esportazioni dei parametri mediante una chiave gestita dal cliente, devi utilizzare una policy di chiave. Per aggiornare la policy di chiave in modo da poter utilizzare una chiave KMS per crittografare le esportazioni dei parametri di S3 Storage Lens, segui la seguente procedura.

Per concedere le autorizzazioni di S3 Storage Lens per eseguire la crittografia dei dati utilizzando la chiave KMS

1. Accedi utilizzando la chiave Console di gestione AWS gestita dal cliente Account AWS che possiede la chiave gestita dal cliente.
2. Apri la AWS KMS console all'indirizzo <https://console.aws.amazon.com/kms>.
3. Per modificare il Regione AWS, usa il selettore di regione.
4. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
5. In Chiavi gestite dal cliente, scegli la chiave che desideri utilizzare per crittografare le esportazioni delle metriche. AWS KMS keys si trovano Region-specific e devono trovarsi nella stessa regione del bucket S3 di destinazione per l'esportazione delle metriche.
6. In Policy chiave, seleziona Passa alla visualizzazione della policy.
7. Per aggiornare la policy chiave, seleziona Modifica.
8. In Modifica policy della chiave, aggiungi la policy chiave seguente alla policy chiave esistente. Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Sid": "Allow Amazon S3 Storage Lens use of the KMS key",
  "Effect": "Allow",
  "Principal": {
    "Service": "storage-lens.s3.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceArn": "arn:aws:s3:us-east-1:source-account-id:storage-lens/your-dashboard-name",
      "aws:SourceAccount": "source-account-id"
    }
  }
}
```

9. Scegli Save changes (Salva modifiche).

Per ulteriori informazioni sulla creazione di chiavi gestite dal cliente e sull'utilizzo delle policy delle chiavi, consulta i seguenti argomenti nella Guida per Developer di AWS Key Management Service :

- [Crea una chiave KMS](#)
- [Politiche chiave in AWS KMS](#)

Puoi anche utilizzare l'operazione API della policy AWS KMS PUT chiave ([PutKeyPolicy](#)) per copiare la policy chiave nelle chiavi gestite dal cliente che desideri utilizzare per crittografare le esportazioni delle metriche utilizzando l'API REST e gli AWS CLI SDK.

Cos'è un manifest di esportazione di S3 Storage Lens?

Le esportazioni giornaliere delle metriche di S3 Storage Lens in bucket generici possono essere suddivise in più file a causa della grande quantità di dati aggregati. Il file manifest `manifest.json` descrive dove si trovano i file di esportazione dei parametri quel giorno. Ogni volta che viene consegnata una nuova esportazione, è accompagnata da un nuovo manifesto. Ogni manifest contenuto nel file `manifest.json` fornisce i metadati e altre informazioni di base riguardanti un inventario.

Le informazioni sul manifest includono le seguenti proprietà:

- `sourceAccountId`: l'ID account del proprietario della configurazione.
- `configId`: un identificativo univoco per il pannello di controllo.
- `destinationBucket`: il nome della risorsa Amazon (ARN) del bucket di destinazione in cui viene inserita l'esportazione delle metriche.
- `reportVersion`: la versione dell'esportazione.
- `reportDate`: la data del report.
- `reportFormat`: il formato del report.
- `reportSchema`: lo schema del report.
- `reportFiles`: l'elenco reale dei file di report di esportazione presenti nel bucket di destinazione.

Esempio di percorso di destinazione del manifesto:

```
user-defined-prefix/StorageLens/111122223333/example-dashboard-configuration-id/V_1/  
manifests/dt=2025-03-18/manifest.json
```

L'esempio seguente mostra un `manifest.json` file per un rapporto sulle metriche predefinite di CSV-formatted Storage Lens:

```
{
  "sourceAccountId": "111122223333",
  "configId": "example-dashboard-configuration-id",
  "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
  "reportVersion": "V_1",
  "reportDate": "2025-07-15",
  "reportFormat": "CSV",
  "reportSchema":
    "version_number,configuration_id,report_date,aws_account_number,aws_region,storage_class,record_count",
  "reportFiles": [
    {
      "key": "DestinationPrefix/StorageLens/111122223333/example-dashboard-configuration-id/V_1/reports/dt=2025-07-15/12345678-1234-1234-1234-123456789012.csv",
      "size": 1603959,
      "md5Checksum": "2177e775870def72b8d84febe1ad3574"
    }
  ]
}
```

L'esempio seguente mostra un `manifest.json` file per un rapporto sulle metriche dei prefissi espansi di CSV-formatted Storage Lens:

```
{
  "sourceAccountId": "111122223333",
  "configId": "example-dashboard-configuration-id",
  "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
  "reportVersion": "V_1",
  "reportDate": "2025-11-03",
  "reportFormat": "CSV",
  "reportSchema":
    "version_number,configuration_id,report_date,aws_account_number,aws_region,storage_class,record_count",
  "reportFiles": [
    {
      "key": "DestinationPrefix/StorageLensExpandedPrefixes/111122223333/example-dashboard-configuration-id/V_1/reports/dt=2025-11-03/EXAMPLE1234-56ab-78cd-90ef-EXAMPLE11111.csv",
      "size": 1603959,
      "md5Checksum": "2177e775870def72b8d84febe1ad3574"
    }
  ]
}
```



```

    }
  ]
}

```

L'esempio seguente mostra un `manifest.json` file per un rapporto sulle metriche predefinite di Storage Parquet Lens formattato in formato:

```

{
  "sourceAccountId": "111122223333",
  "configId": "example-dashboard-configuration-id",
  "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
  "reportVersion": "V_1",
  "reportDate": "2025-11-03",
  "reportFormat": "Parquet",
  "reportSchema": "message s3.storage.lens { required string version_number;
required string configuration_id; required string report_date; required string
aws_account_number; required string aws_region; required string storage_class;
required string record_type; required string record_value; required string
bucket_name; required string metric_name; required long metric_value; }",
  "reportFiles": [
    {
      "key": "DestinationPrefix/StorageLens/111122223333/example-dashboard-
configuration-id/V_1/reports/dt=2025-11-03/bd23de7c-b46a-4cf4-bcc5-b21aac5be0f5.par",
      "size": 14714,
      "md5Checksum": "b5c741ee0251cd99b90b3e8eff50b944"
    }
  ]
}

```

L'esempio seguente mostra un `manifest.json` file per un rapporto sulle metriche dei prefissi espansi Parquet di Storage Lens formattato in formato:

```

{
  "sourceAccountId": "111122223333",
  "configId": "example-dashboard-configuration-id",
  "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
  "reportVersion": "V_1",
  "reportDate": "2025-11-03",
  "reportFormat": "Parquet",
  "reportSchema": "message s3.storage.lens { required string version_number;
required string configuration_id; required string report_date; required string
aws_account_number; required string aws_region; required string storage_class;

```

```
required string record_type; required string record_value; required string
bucket_name; required string metric_name; required long metric_value; }",
  "reportFiles": [
    {
      "key": "DestinationPrefix/StorageLensExpandedPrefixes/111122223333/example-
dashboard-configuration-id/V_1/reports/dt=2025-11-03/bd23de7c-b46a-4cf4-bcc5-
b21aac5be0f5.par",
      "size": 14714,
      "md5Checksum": "b5c741ee0251cd99b90b3e8eff50b944"
    }
  ]
}
```

Puoi configurare l'esportazione delle metriche in modo che venga generata come parte della configurazione del dashboard nella console Amazon S3 o utilizzando l'API REST e gli SDK di Amazon S3. AWS CLI

Informazioni sugli schemi di esportazione di Amazon S3 Storage Lens

Gli schemi di esportazione di S3 Storage Lens variano a seconda della destinazione di esportazione. Scegliete lo schema appropriato in base al fatto che stiate esportando in bucket S3 per uso generico o tabelle S3.

Argomenti

- [Schema di esportazione per bucket S3 per uso generico](#)
- [Schemi di esportazione per tabelle S3](#)

Schema di esportazione per bucket S3 per uso generico

La tabella seguente contiene lo schema dell'esportazione delle metriche di S3 Storage Lens durante l'esportazione in bucket S3 per uso generico.

Nome attributo	Tipo di dati	Nome colonna	Descrizione
VersionNumber	Stringa	version_number	La versione dei parametri di S3 Storage Lens in uso.
ConfigurationId	Stringa	configura tion_id	configura tion_id della

Nome attributo	Tipo di dati	Nome colonna	Descrizione
			configurazione di S3 Storage Lens.
ReportDate	Stringa	report_date	Data in cui sono stati tracciati i parametri.
AwsAccountNumber	Stringa	aws_account_number	Account AWS Il tuo numero.
AwsRegion	Stringa	aws_region	Il valore Regione AWS per il quale vengono monitorate le metriche.
StorageClass	Stringa	storage_class	La classe di storage del bucket in questione.
RecordType	ENUM	record_type	Il tipo di artefatto che viene segnalato (ACCOUNT,, BUCKET o). PREFIX
RecordValue	Stringa	record_value	Il valore dell'arte fatto RecordType . <div><div><div><div></div><div>Note</div></div><div>Lo record_value è URL-encoded</div></div></div>

Nome attributo	Tipo di dati	Nome colonna	Descrizione
MetricName	Stringa	metric_name	Il nome del parametro che viene riportato.
MetricValue	Lungo	metric_value	Il valore del parametro che viene riportato.

Esempio di esportazione dei parametri di S3 Storage Lens

Di seguito è riportato un esempio di esportazione dei parametri di S3 Storage Lens basata su questo schema.



Note

Per identificare i parametri per i gruppi Storage Lens, cerca il valore `STORAGE_LENS_GROUP_BUCKET` o `STORAGE_LENS_GROUP_ACCOUNT` nella colonna `record_type`. La colonna `record_value` mostra il nome della risorsa Amazon (ARN) per il gruppo Storage Lens, ad esempio, `arn:aws:s3:us-east-1:123456789012:storage-lens-group/slg-1`.

version_configuration_id	report_date	aws_account_number	aws_region	storage_class	record_type	record_value	bucket_name	metric_name	metric_value
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		StorageBytes	2478830621
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		ObjectCount	1598962
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		ReplicatedStorageBytes	20000
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		ReplicatedObjectCount	20
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		EncryptedStorageBytes	2478828742
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		EncryptedObjectCount	1598961
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		DeleteMarkerObjectCount	1500
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		ObjectLockEnabledStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		ObjectLockEnabledObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		CurrentVersionStorageBytes	2478830621
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		CurrentVersionObjectCount	1598962
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		NonCurrentVersionStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		NonCurrentVersionObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		IncompleteMultipartUploadStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT		IncompleteMultipartUploadObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	StorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	ObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	ReplicatedStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	ReplicatedObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	EncryptedStorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	EncryptedObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	DeleteMarkerObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	ObjectLockEnabledStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	ObjectLockEnabledObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	CurrentVersionStorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	CurrentVersionObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	NonCurrentVersionStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	NonCurrentVersionObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	IncompleteMultipartUploadStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus-west-1%2Fcloudtrail-log-sf%2F	IncompleteMultipartUploadObjectCount	0

Di seguito è riportato un esempio di esportazione dei parametri di S3 Storage Lens con i dati dei gruppi di Storage Lens.

version_numbe	configuration_id	report_date	aws_account_num	aws_region	storage_class	record_type	record_value	bucket_name	metric_name	metric_value
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		StorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		EncryptedStorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		EncryptedObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		DeleteMarkerObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectLockEnabledStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectLockEnabledObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		CurrentVersionStorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		CurrentVersionObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		NonCurrentVersionStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		NonCurrentVersionObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMultipartUploadStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMultipartUploadObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		DeleteMarkerStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedStorageBytesSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedObjectCountSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMPUStorageBytesOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMPUObjectCountOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	StorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	EncryptedStorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	EncryptedObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	DeleteMarkerObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectLockEnabledStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectLockEnabledObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	CurrentVersionStorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	CurrentVersionObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	NonCurrentVersionStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	NonCurrentVersionObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMultipartUploadStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMultipartUploadObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	DeleteMarkerStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedObjectCountSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedStorageBytesOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMPUObjectCountOlderThan7Days	0

Schemi di esportazione per tabelle S3

Quando si esportano le metriche di S3 Storage Lens in tabelle S3, i dati vengono organizzati in tre schemi di tabella separati: metriche di archiviazione, metriche delle proprietà del bucket e metriche di attività.

Argomenti

- [Schema della tabella delle metriche di archiviazione](#)
- [Schema della tabella delle metriche delle proprietà del bucket](#)
- [Schema della tabella delle metriche delle attività](#)

Schema della tabella delle metriche di archiviazione

Nome	Tipo	Description
version_number	stringa	Identificatore della versione dello schema della tabella
configuration_id	stringa	Nome di configurazione S3 Storage Lens
report_time	timestamptz	Data a cui si riferisce il rapporto S3 Storage Lens
aws_account_id	stringa	ID account a cui si riferisce la voce

Nome	Tipo	Description
aws_region	stringa	Region
storage_class	stringa	Classe di storage
record_type	stringa	Tipo di record, related a che cosa corrisponde il livello di aggregazione dei dati. Valori: ACCOUNT, BUCKET, PREFIX, LENS GROUP.
record_value	stringa	Disambiguatore per i tipi di record che contengono più di un record. Viene utilizzato per fare riferimento al prefisso
bucket_name	stringa	Nome bucket
object_count	Long	Numero di oggetti memorizzati per l'elemento di riferimento corrente
storage_bytes	DECIMALE (38,0)	Numero di byte memorizzati per l'elemento di riferimento corrente
bucket_key_sse_kms_object_count	Long	Numero di oggetti crittografati con una chiave gestita dal cliente memorizzata per l'elemento di riferimento corrente
bucket_key_sse_kms_storage_bytes	DECIMALE (38,0)	Numero di byte crittografati con una chiave gestita dal cliente memorizzata per l'elemento di riferimento corrente
current_version_object_count	Long	Numero di oggetti della versione corrente archiviati per l'elemento di riferimento corrente
current_version_storage_bytes	DECIMALE (38,0)	Numero di byte della versione corrente memorizzati per l'elemento di riferimento corrente

Nome	Tipo	Description
delete_marker_object_count	Long	Numero di oggetti marker di eliminazione memorizzati per l'elemento di riferimento corrente
delete_marker_storage_bytes	DECIMALE (38,0)	Numero di byte dell'indicatore di eliminazione memorizzati per l'elemento di riferimento corrente
encrypted_object_count	Long	Numero di oggetti crittografati archiviati per l'elemento di riferimento corrente
encrypted_storage_bytes	DECIMALE (38,0)	Numero di byte crittografati memorizzati per l'elemento di riferimento corrente
incomplete_mpu_object_older_than_7_days_count	Long	Numero di oggetti caricati in più parti incompleti più vecchi di 7 giorni e archiviati per l'elemento attualmente referenziato
incomplete_mpu_storage_older_than_7_days_bytes	DECIMALE (38,0)	Numero di byte di caricamento in più parti incompleti archiviati più vecchi di 7 giorni per l'elemento di riferimento corrente
incomplete_mpu_object_count	Long	Numero di oggetti di caricamento in più parti incompleti archiviati per l'elemento attualmente referenziato
incomplete_mpu_storage_bytes	DECIMALE (38,0)	Numero di byte di caricamento in più parti incompleti memorizzati per l'elemento di riferimento corrente

Nome	Tipo	Description
non_current_version_object_count	Long	Numero di oggetti della versione non corrente memorizzati per l'elemento di riferimento corrente
non_current_version_storage_bytes	DECIMALE (38,0)	Numero di byte della versione non corrente memorizzati per l'elemento di riferimento corrente
object_lock_enabled_object_count	Long	Numero di oggetti archiviati per gli oggetti con blocco abilitato nell'elemento di riferimento corrente
object_lock_enabled_storage_bytes	DECIMALE (38,0)	Numero di byte memorizzati per gli oggetti con blocco abilitato nell'elemento di riferimento corrente
replicated_object_count	Long	Numero di oggetti replicati per l'elemento di riferimento corrente
replicated_storage_bytes	DECIMALE (38,0)	Numero di byte replicati per l'elemento di riferimento corrente
replicated_object_source_count	Long	Numero di oggetti replicati come origine archiviata per l'elemento di riferimento corrente
replicated_storage_source_bytes	DECIMALE (38,0)	Numero di byte replicati come origine per l'elemento di riferimento corrente
sse_kms_object_count	Long	Numero di oggetti crittografati con chiave SSE memorizzata per l'elemento di riferimento corrente

Nome	Tipo	Description
sse_kms_storage_bytes	DECIMALE (38,0)	Numero di byte crittografati con chiave SSE memorizzati per l'elemento di riferimento corrente
object_0kb_count	Long	Numero di oggetti con dimensioni pari a 0 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_0kb_to_128kb_count	Long	Numero di oggetti con dimensioni superiori a 0 KB e inferiori o uguali a 128 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_128kb_to_256kb_count	Long	Numero di oggetti con dimensioni superiori a 128 KB e inferiori o uguali a 256 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_256kb_to_512kb_count	Long	Numero di oggetti con dimensioni superiori a 256 KB e inferiori o uguali a 512 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_512kb_to_1mb_count	Long	Numero di oggetti con dimensioni superiori a 512 KB e inferiori o uguali a 1 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_1mb_to_2mb_count	Long	Numero di oggetti con dimensioni superiori a 1 MB e inferiori o uguali a 2 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_2mb_to_4mb_count	Long	Numero di oggetti con dimensioni superiori a 2 MB e inferiori o uguali a 4 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione

Nome	Tipo	Description
object_4mb_to_8mb_count	Long	Numero di oggetti con dimensioni superiori a 4 MB e inferiori o uguali a 8 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_8mb_to_16mb_count	Long	Numero di oggetti con dimensioni superiori a 8 MB e inferiori o uguali a 16 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_16mb_to_32mb_count	Long	Numero di oggetti con dimensioni superiori a 16 MB e inferiori o uguali a 32 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_32mb_to_64mb_count	Long	Numero di oggetti con dimensioni superiori a 32 MB e inferiori o uguali a 64 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_64mb_to_128mb_count	Long	Numero di oggetti con dimensioni superiori a 64 MB e inferiori o uguali a 128 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_128mb_to_256mb_count	Long	Numero di oggetti con dimensioni superiori a 128 MB e inferiori o uguali a 256 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_256mb_to_512mb_count	Long	Numero di oggetti con dimensioni superiori a 256 MB e inferiori o uguali a 512 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione

Nome	Tipo	Description
object_512mb_to_1gb_count	Long	Numero di oggetti con dimensioni superiori a 512 MB e inferiori o uguali a 1 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_1gb_to_2gb_count	Long	Numero di oggetti con dimensioni superiori a 1 GB e inferiori o uguali a 2 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_2gb_to_4gb_count	Long	Numero di oggetti con dimensioni superiori a 2 GB e inferiori o uguali a 4 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_larger_than_4gb_count	Long	Numero di oggetti con dimensioni superiori a 4 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione

Schema della tabella delle metriche delle proprietà del bucket

Nome	Tipo	Description
version_number	stringa	Identificatore di versione dello schema della tabella
configuration_id	stringa	Nome di configurazione S3 Storage Lens
report_time	timestamp	Data a cui si riferisce il rapporto S3 Storage Lens
aws_account_id	stringa	ID account a cui si riferisce la voce
record_type	stringa	Tipo di record, correlato al livello di aggregazione dei dati. Valori: ACCOUNT, BUCKET, PREFIX, LENS GROUP.

Nome	Tipo	Description
<code>record_value</code>	stringa	Disambiguatore per i tipi di record che contengono più di un record. Viene utilizzato per fare riferimento al prefisso.
<code>aws_region</code>	stringa	Region
<code>storage_class</code>	stringa	Classe di storage
<code>bucket_name</code>	stringa	Nome bucket
<code>versioning_enabled_bucket_count</code>	Long	Numero di bucket con controllo delle versioni abilitato per l'elemento di riferimento corrente
<code>mfa_delete_enabled_bucket_count</code>	Long	Numero di bucket con eliminazione MFA abilitata per l'elemento di riferimento corrente
<code>sse_kms_enabled_bucket_count</code>	Long	Numero di bucket con KMS abilitato per l'elemento di riferimento corrente
<code>object_ownership_bucket_owner_enforced_bucket_count</code>	Long	Numero di bucket con proprietario del bucket Object Ownership applicato all'elemento di riferimento corrente
<code>object_ownership_bucket_owner_preferred_bucket_count</code>	Long	Numero di bucket con il proprietario del bucket Object Ownership preferito per l'elemento di riferimento corrente

Nome	Tipo	Description
object_ownership_object_writer_bucket_count	Long	Numero di bucket con autore di oggetti Object Ownership per l'elemento di riferimento corrente
transfer_acceleration_enabled_bucket_count	Long	Numero di bucket con accelerazione di trasferimento abilitata per l'elemento di riferimento corrente
event_notification_enabled_bucket_count	Long	Numero di bucket con notifica degli eventi abilitata per l'elemento di riferimento corrente
transition_lifecycle_rule_count	Long	Numero di regole del ciclo di vita di transizione per l'elemento di riferimento corrente
expiration_lifecycle_rule_count	Long	Numero di regole del ciclo di vita di scadenza per l'articolo di riferimento corrente
non_current_version_transition_lifecycle_rule_count	Long	Numero di regole del ciclo di vita della transizione di versione non correnti per l'articolo di riferimento corrente

Nome	Tipo	Description
non_current_version_expiration_lifecycle_rule_count	Long	Numero di regole del ciclo di vita di scadenza della versione non corrente per l'elemento di riferimento corrente
abort_incomplete_multipart_upload_lifecycle_rule_count	Long	Numero di regole del ciclo di vita del caricamento multipart non completo per l'elemento di riferimento corrente
expired_object_delete_marker_lifecycle_rule_count	Long	Numero di regole del ciclo di vita degli indicatori di eliminazione degli oggetti in scadenza per l'elemento di riferimento corrente
same_region_replication_rule_count	Long	Numero di regole di Same-Region replica conteggiate per l'elemento di riferimento corrente
cross_region_replication_rule_count	Long	Numero di conteggi delle regole Cross-Region di replica per l'elemento di riferimento corrente
same_account_replication_rule_count	Long	Numero di conteggi delle regole Same-account di replica per l'elemento di riferimento corrente

Nome	Tipo	Description
cross_account_replication_rule_count	Long	Numero di regole di Cross-account replica conteggiate per l'elemento di riferimento corrente
invalid_destination_replication_rule_count	Long	Numero di bucket con replica di destinazione non valida per l'elemento di riferimento corrente

Schema della tabella delle metriche delle attività

Nome	Tipo	Description
version_number	stringa	Identificatore della versione dello schema della tabella
configuration_id	stringa	Nome di configurazione S3 Storage Lens
report_time	timestamp tz	Data a cui si riferisce il rapporto S3 Storage Lens
aws_account_id	stringa	ID account a cui si riferisce la voce
aws_region	stringa	Region
storage_class	stringa	Classe di storage
record_type	stringa	Tipo di record, correlato al livello di aggregazione dei dati. Valori: ACCOUNT, BUCKET, PREFIX.
record_value	stringa	Disambiguatore per i tipi di record che contengono più di un record. Viene utilizzato per fare riferimento al prefisso
bucket_name	stringa	Nome bucket

Nome	Tipo	Description
all_request_count	Long	Numero di _tutte_ richieste per l'elemento di riferimento corrente
all_sse_kms_encrypted_request_count	Long	Numero di richieste crittografate KMS per l'elemento di riferimento corrente
all_unsupported_signature_request_count	Long	Numero di richieste di firma non supportate per l'elemento di riferimento corrente
all_unsupported_tls_request_count	Long	Numero di richieste TLS non supportate per l'elemento di riferimento corrente
bad_request_error_400_count	Long	Numero di 400 errori di richiesta errata per l'elemento di riferimento corrente
delete_request_count	Long	Numero di richieste di eliminazione per l'elemento attualmente referenziato
downloaded_bytes	decimale (0,0)	Numero di byte scaricati per l'elemento di riferimento corrente
error_4xx_count	Long	Numero di errori 4xx per l'elemento di riferimento corrente
error_5xx_count	Long	Numero di errori 5xx per l'elemento di riferimento corrente
forbidden_error_403_count	Long	Numero di 403 errori proibiti per l'articolo a cui si fa riferimento attualmente

Nome	Tipo	Description
get_reque st_count	Long	Numero di richieste get per l'articolo a cui si fa riferimento attualmente
head_requ est_count	Long	Numero di richieste principali per l'articolo a cui si fa riferimento attualmente
internal_ server_er ror_500_count	Long	Numero di 500 errori interni del server per l'elemento di riferimento corrente
list_requ est_count	Long	Numero di richieste di elenco per l'elemento attualmente referenziato
not_found _error_40 4_count	Long	Numero di 404 errori non trovati per l'elemento di riferimento corrente
ok_status _200_count	Long	Numero di 200 richieste OK per l'elemento di riferimento corrente
partial_c ontent_st atus_206_count	Long	Numero di 206 richieste di contenuto parziale per l'elemento di riferimento corrente
post_requ est_count	Long	Numero di richieste di post per l'elemento a cui si fa riferimento attualmente
put_reque st_count	Long	Numero di richieste put per l'articolo a cui si fa riferimento attualmente
select_re quest_count	Long	Numero di richieste di selezione per l'articolo a cui si fa riferimento attualmente
select_re turned_bytes	decimale (0,0)	Numero di byte restituiti dalle richieste di selezione per l'elemento di riferimento corrente

Nome	Tipo	Description
select_scanned_bytes	decimale (0,0)	Numero di byte scansionati da richieste selezionate per l'elemento di riferimento corrente
service_unavailable_error_503_count	Long	Numero di 503 errori di servizio non disponibili per l'elemento di riferimento corrente
uploaded_bytes	decimale (0,0)	Numero di byte caricati per l'elemento di riferimento corrente
average_first_byte_latency	Long	Tempo medio per richiesta che intercorre tra il momento in cui un bucket S3 riceve una richiesta completa e il momento in cui inizia a restituire la risposta, misurato nelle ultime 24 ore
average_total_request_latency	Long	Tempo medio trascorso per richiesta tra il primo byte ricevuto e l'ultimo byte inviato a un bucket S3, misurato nelle ultime 24 ore
read_0kb_request_count	Long	Numero di GetObject richieste con dimensioni di dati di 0 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_0kb_to_128kb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 0 KB e fino a 128 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_128kb_to_256kb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 128 KB e fino a 256 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto

Nome	Tipo	Description
read_256k_b_to_512k_b_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 256 KB e fino a 512 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_512k_b_to_1mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 512 KB e fino a 1 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_1mb_to_2mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 1 MB e fino a 2 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_2mb_to_4mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 2 MB e fino a 4 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_4mb_to_8mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 4 MB e fino a 8 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_8mb_to_16mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 8 MB e fino a 16 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_16mb_to_32mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 16 MB e fino a 32 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_32mb_to_64mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 32 MB e fino a 64 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_64mb_to_128mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 64 MB e fino a 128 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto

Nome	Tipo	Description
read_128mb_to_256mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 128 MB e fino a 256 MB, incluse le richieste basate sull'intervallo e le richieste per l'intero oggetto
read_256mb_to_512mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 256 MB e fino a 512 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_512mb_to_1gb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 512 MB e fino a 1 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_1gb_to_2gb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 1 GB e fino a 2 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_2gb_to_4gb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 2 GB e fino a 4 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_larger_than_4gb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 4 GB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
write_0kb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati di 0 KB
write_0kb_to_128kb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 0 KB e fino a 128 KB

Nome	Tipo	Description
write_128 kb_to_256 kb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 128 KB e fino a 256 KB
write_256 kb_to_512 kb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 256 KB e fino a 512 KB
write_512 kb_to_1mb _request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 512 KB e fino a 1 MB
write_1mb _to_2mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 1 MB e fino a 2 MB
write_2mb _to_4mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 2 MB e fino a 4 MB
write_4mb _to_8mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 4 MB e fino a 8 MB
write_8mb _to_16mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 8 MB e fino a 16 MB
write_16mb _to_32mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 16 MB e fino a 32 MB

Nome	Tipo	Description
write_32mb_to_64mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 32 MB e fino a 64 MB
write_64mb_to_128mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 64 MB e fino a 128 MB
write_128mb_to_256mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 128 MB e fino a 256 MB
write_256mb_to_512mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 256 MB e fino a 512 MB
write_512mb_to_1gb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 512 MB e fino a 1 GB
write_1gb_to_2gb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 1 GB e fino a 2 GB
write_2gb_to_4gb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 2 GB e fino a 4 GB
write_larger_than_4gb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 4 GB

Nome	Tipo	Description
concurrent_put_503_error_count	Long	Numero di 503 errori generati a causa di scritture simultanee sullo stesso oggetto
cross_region_request_count	Long	Numero di richieste che provengono da un client in una regione diversa da quella di origine del bucket
cross_region_transferred_bytes	decimale (0,0)	Numero di byte trasferiti da chiamate in una regione diversa da quella di origine del bucket
cross_region_without_replication_request_count	Long	Numero di richieste provenienti da un client in una regione diversa da quella di origine del bucket, escluse le richieste di replica tra regioni
cross_region_without_replication_transferred_bytes	decimale (0,0)	Numero di byte trasferiti da chiamate in una regione diversa da quella di origine del bucket, esclusi i byte di replica tra regioni
inregion_request_count	Long	Numero di richieste provenienti da un cliente nella stessa regione della regione di origine del bucket
inregion_transferred_bytes	decimale (0,0)	Numero di byte trasferiti dalle chiamate dalla stessa regione della regione di origine del bucket
unique_objects_accessed_daily_count	Long	Numero di oggetti a cui è stato effettuato l'accesso almeno una volta nelle ultime 24 ore

Monitora le metriche di S3 Storage Lens in CloudWatch

Puoi pubblicare le metriche di S3 Storage Lens su Amazon per CloudWatch creare una visione unificata dello stato operativo nelle dashboard. [CloudWatch](#) Puoi anche utilizzare CloudWatch funzionalità, come allarmi e azioni attivate, calcoli metrici e rilevamento delle anomalie, per monitorare e intervenire sulle metriche di S3 Storage Lens. Inoltre, le operazioni CloudWatch API consentono alle applicazioni, compresi i provider di terze parti, di accedere alle metriche di S3 Storage Lens. Per ulteriori informazioni sulle CloudWatch funzionalità, consulta la [Amazon CloudWatch User Guide](#).

Puoi abilitare l'opzione di CloudWatch pubblicazione per configurazioni di dashboard nuove o esistenti utilizzando la console Amazon S3, l'API REST di Amazon S3 e gli SDK AWS CLI. AWS Le dashboard aggiornate alle metriche e ai consigli avanzati di S3 Storage Lens possono utilizzare l'opzione di pubblicazione. CloudWatch Per i prezzi relativi all'opzione Advanced metrics and recommendations (Parametri e suggerimenti avanzati), consulta [Prezzi di Amazon S3](#). Non si applicano costi aggiuntivi per la pubblicazione CloudWatch delle metriche; tuttavia, si applicano altri CloudWatch costi, come dashboard, allarmi e chiamate API. Per ulteriori informazioni, consulta [i prezzi di Amazon. CloudWatch](#)

Le metriche di S3 Storage Lens vengono pubblicate CloudWatch nell'account proprietario della configurazione S3 Storage Lens. Dopo aver abilitato l'opzione di CloudWatch pubblicazione all'interno delle metriche avanzate, puoi accedere alle metriche a livello di account e bucket in base all'ID di configurazione, all'account, al bucket (solo per le metriche a livello di bucket), alla regione e alla classe di archiviazione in. CloudWatch Prefix-level CloudWatchle metriche non sono disponibili in.

Note

Le metriche di S3 Storage Lens sono metriche giornaliere e vengono pubblicate una volta al CloudWatch giorno. Quando si interrogano le metriche di S3 Storage Lens in CloudWatch, il periodo di interrogazione deve essere di 1 giorno (86400 secondi). Dopo la visualizzazione delle metriche giornaliere di S3 Storage Lens nella dashboard di S3 Storage Lens nella console Amazon S3, possono essere necessarie alcune ore prima che queste stesse metriche vengano visualizzate. CloudWatch Quando abiliti l'opzione di CloudWatch pubblicazione per le metriche di S3 Storage Lens per la prima volta, possono essere necessarie fino a 24 ore per la pubblicazione delle metriche. CloudWatch

Dopo aver abilitato l'opzione di CloudWatch pubblicazione, puoi utilizzare le seguenti CloudWatch funzionalità per monitorare e analizzare i dati di S3 Storage Lens: LensStorage

- [Dashboard](#): utilizza le CloudWatch dashboard per creare dashboard S3 Storage Lens personalizzate. Condividi la tua CloudWatch dashboard con persone che non hanno accesso diretto alla tua Account AWS, con tutti i team, con le parti interessate e con persone esterne alle tue organizzazioni.
- [Allarmi e operazioni attivate](#) – Configura gli allarmi che controllano i parametri e si attivano quando viene violata una soglia. Ad esempio, è possibile configurare un allarme che invia una notifica di Amazon SNS quando il valore del parametro Incomplete Multipart Upload Bytes (Byte caricamenti in più parti incompleti) supera 1 GB per tre giorni consecutivi.
- [Rilevamento di anomalie](#) – Abilita il rilevamento delle anomalie per analizzare continuamente i parametri, determinare le normali linee di base e le anomalie superficiali. Puoi creare allarmi di rilevamento delle anomalie basati sul valore previsto di un parametro. Ad esempio, è possibile monitorare le anomalie del parametro Object Lock Enabled Bytes (Byte con blocco oggetti abilitato) per rilevare una rimozione non autorizzata delle impostazioni di Object Lock.
- [Matematica dei parametri](#) – permette di eseguire query di più parametri S3 Storage Lens e di utilizzare espressioni matematiche per creare nuove serie temporali in base a tali parametri. Ad esempio, è possibile creare un nuovo parametro per ottenere la dimensione media dell'oggetto dividendo StorageBytes per ObjectCount.

Per ulteriori informazioni sull'opzione di CloudWatch pubblicazione per le metriche di S3 Storage Lens, consulta i seguenti argomenti.

Argomenti

- [Dimensioni e parametri di S3 Storage Lens](#)
- [Abilitazione della CloudWatch pubblicazione per S3 Storage Lens](#)
- [Utilizzo delle metriche di S3 Storage Lens in CloudWatch](#)

Dimensioni e parametri di S3 Storage Lens

Per inviare le metriche di S3 Storage Lens a CloudWatch, devi abilitare l'opzione di CloudWatch pubblicazione all'interno delle metriche avanzate di S3 Storage Lens. Dopo aver abilitato le metriche avanzate, puoi utilizzare le [CloudWatch dashboard](#) per monitorare le metriche di S3 Storage Lens insieme ad altre metriche dell'applicazione e creare una visione unificata dello stato operativo. Puoi

utilizzare le dimensioni per filtrare le metriche di S3 Storage Lens per organizzazione, account, bucket, classe CloudWatch di archiviazione, regione e ID di configurazione delle metriche.

Le metriche di S3 Storage Lens vengono pubblicate CloudWatch nell'account proprietario della configurazione S3 Storage Lens. Dopo aver abilitato l'opzione di CloudWatch pubblicazione all'interno delle metriche avanzate, puoi accedere alle metriche a livello di account e bucket in base all'ID di configurazione, all'account, al bucket (solo per le metriche a livello di bucket), alla regione e alla classe di archiviazione in. CloudWatch Prefix-level CloudWatchle metriche non sono disponibili in.

Note

Le metriche di S3 Storage Lens sono metriche giornaliere e vengono pubblicate una volta al CloudWatch giorno. Quando si interrogano le metriche di S3 Storage Lens in CloudWatch, il periodo di interrogazione deve essere di 1 giorno (86400 secondi). Dopo la visualizzazione delle metriche giornaliere di S3 Storage Lens nella dashboard di S3 Storage Lens nella console Amazon S3, possono essere necessarie alcune ore prima che queste stesse metriche vengano visualizzate. CloudWatch Quando abiliti l'opzione di CloudWatch pubblicazione per le metriche di S3 Storage Lens per la prima volta, possono essere necessarie fino a 24 ore per la pubblicazione delle metriche. CloudWatch

Per ulteriori informazioni sulle metriche e sulle dimensioni di S3 Storage Lens in CloudWatch, consulta i seguenti argomenti.

Argomenti

- [Metriche](#)
- [Dimensioni](#)

Metriche

Le metriche di S3 Storage Lens sono disponibili come metriche all'interno. CloudWatch I parametri di S3 Storage Lens sono pubblicati nello spazio dei nomi AWS/S3/Storage-Lens. Questo spazio dei nomi è solo per i parametri di S3 Storage Lens. I parametri bucket, richiesta e replica di Amazon S3 vengono pubblicati nello spazio dei nomi AWS/S3.

Le metriche di S3 Storage Lens vengono pubblicate CloudWatch nell'account che possiede la configurazione S3 Storage Lens. Dopo aver abilitato l'opzione di CloudWatch pubblicazione all'interno

delle metriche avanzate, puoi accedere alle metriche a livello di account e bucket in base all'ID di configurazione, all'account, al bucket (solo per le metriche a livello di bucket), alla regione e alla classe di archiviazione in. CloudWatch Prefix-level CloudWatchle metriche non sono disponibili in.

In S3 Storage Lens, i parametri vengono aggregati e memorizzati solo nella Regione di origine designata. Le metriche di S3 Storage Lens vengono pubblicate anche CloudWatch nella regione principale specificata nella configurazione di S3 Storage Lens.

Per un elenco completo delle metriche di S3 Storage Lens, incluso un elenco delle metriche disponibili in, consulta. CloudWatch [Glossario dei parametri di Amazon S3 Storage Lens](#)

Note

La statistica valida per le metriche di S3 Storage Lens in è Average. CloudWatch Per ulteriori informazioni sulle statistiche in CloudWatch, consulta le definizioni delle [CloudWatch statistiche](#) nella Amazon CloudWatch User Guide.

Granularità delle metriche di S3 Storage Lens in CloudWatch

S3 Storage Lens offre parametri sulla granularità dell'organizzazione, dell'account, del bucket e del prefisso. S3 Storage Lens pubblica le metriche di S3 Storage Lens a livello di organizzazione, account e bucket su. CloudWatch Prefix-level Le metriche di S3 Storage Lens non sono disponibili in. CloudWatch

Per ulteriori informazioni sulla granularità delle metriche di S3 Storage Lens disponibili in CloudWatch, consulta il seguente elenco:

- Organizzazione – Parametri aggregati tra gli account membri della tua organizzazione. S3 Storage Lens pubblica le metriche relative agli account dei membri nell'account di gestione. CloudWatch
 - Organizzazione e account – Parametri per gli account membri della tua organizzazione.
 - Organizzazione e account – Parametri per i bucket Amazon S3 buckets negli account membri della tua organizzazione.
- Account (Non-organization livello): metriche aggregate tra i bucket del tuo account.
- Bucket (Non-organization livello): metriche per un bucket specifico. In CloudWatch, S3 Storage Lens pubblica queste metriche per chi ha creato la Account AWS configurazione di S3 Storage Lens. S3 Storage Lens pubblica questi parametri solo per configurazioni non organizzative.

Dimensioni

Quando S3 Storage Lens invia dati a CloudWatch, le dimensioni vengono allegare a ciascuna metrica. Le dimensioni sono categorie che descrivono le caratteristiche dei parametri. È possibile utilizzare le dimensioni per filtrare i risultati restituiti CloudWatch .

Ad esempio, tutte le metriche di S3 Storage Lens CloudWatch hanno la `configuration_id` dimensione. È possibile utilizzare questa dimensione per distinguere tra i parametri associati con una configurazione specifica di S3 Storage Lens. L'`organization_id` identifica i parametri a livello organizzativo. Per ulteriori informazioni sulle dimensioni in CloudWatch, consulta [Dimensioni](#) nella Guida per l'CloudWatch utente.

Sono disponibili diverse dimensioni per i parametri S3 Storage Lens a seconda della granularità dei parametri. Ad esempio, puoi utilizzare la `organization_id` dimensione per filtrare le metriche a livello di organizzazione in base all'ID. AWS Organizations Tuttavia, non è possibile utilizzare questa dimensione per parametri a livello di bucket e account. Per ulteriori informazioni, consulta [Filtraggio dei parametri utilizzando le dimensioni](#).

Per vedere quali dimensioni sono disponibili per la configurazione di S3 Storage Lens, vedi la tabella seguente.

Dimensione	Descrizione	Bucket	Organizzazione	Organizzazione e bucket	Organizzazione e account
<code>configuration_id</code>	Nome del pannello di controllo per la configurazione di S3 Storage Lens riportato nei parametri	✔	✔	✔	✔
<code>metrics_version</code>	Versione dei parametri di S3 Storage Lens in uso. La versione dei parametri ha un valore fisso di 1.0.	✔	✔	✔	✔
<code>organization_id</code>	L' AWS Organizations ID per le metriche	✖	✖	✔	✔
<code>aws_account_number</code>	Account AWS Quello associato alle metriche	✔	✔	✖	✔

Dimensione	Descrizione	Bucket	Account	Organizzazione	Organizzazione e bucket	Organizzazione e bucket
aws_region	Il Regione AWS per le metriche	✓	✓	✓	✓	✓
bucket_name	Nome del bucket S3 riportato nei parametri	✓	✗	✗	✓	✗
storage_class	Classe di archiviazione per il bucket riportato nei parametri	✓	✓	✓	✓	✓
record_type	Granularità dei parametri: ORGANIZZAZIONE, ACCOUNT, BUCKET	✓	✓	✗	ORGANIZZAZIONE	BUCKET

Abilitazione della CloudWatch pubblicazione per S3 Storage Lens

Puoi pubblicare le metriche di S3 Storage Lens su Amazon CloudWatch per creare una visione unificata dello stato operativo in dashboard. [CloudWatch](#) Puoi anche utilizzare CloudWatch funzionalità, come allarmi e azioni attivate, calcoli metrici e rilevamento delle anomalie, per monitorare e intervenire sulle metriche di S3 Storage Lens. Inoltre, le operazioni CloudWatch API consentono alle applicazioni, compresi i provider di terze parti, di accedere alle metriche di S3 Storage Lens. Per ulteriori informazioni sulle CloudWatch funzionalità, consulta la [Amazon CloudWatch User Guide](#).

Le metriche di S3 Storage Lens vengono pubblicate CloudWatch nell'account che possiede la configurazione S3 Storage Lens. Dopo aver abilitato l'opzione di CloudWatch pubblicazione all'interno delle metriche avanzate, puoi accedere alle metriche a livello di account e bucket in base all'ID di configurazione, all'account, al bucket (solo per le metriche a livello di bucket), alla regione e alla classe di archiviazione in. CloudWatch Prefix-level CloudWatchle metriche non sono disponibili in.

Puoi abilitare CloudWatch il supporto per configurazioni di dashboard nuove o esistenti utilizzando la console S3, le API REST di Amazon S3 e gli SDK. AWS CLI AWS L'opzione di CloudWatch pubblicazione è disponibile per le dashboard aggiornate alle metriche e ai consigli avanzati di S3 Storage Lens. Per i prezzi relativi all'opzione Advanced metrics and recommendations (Parametri e suggerimenti avanzati), consulta [Prezzi di Amazon S3](#). Non si applicano costi aggiuntivi per

la pubblicazione CloudWatch delle metriche; tuttavia, si applicano altri CloudWatch costi, come dashboard, allarmi e chiamate API.

Per abilitare l'opzione di CloudWatch pubblicazione per le metriche di S3 Storage Lens, consulta i seguenti argomenti.

Note

Le metriche di S3 Storage Lens sono metriche giornaliere e vengono pubblicate una volta al giorno. CloudWatch Quando si interrogano le metriche di S3 Storage Lens in CloudWatch, il periodo di interrogazione deve essere di 1 giorno (86400 secondi). Dopo che le metriche giornaliere di S3 Storage Lens vengono visualizzate nella dashboard di S3 Storage Lens nella console Amazon S3, possono essere necessarie alcune ore prima che queste stesse metriche vengano visualizzate. CloudWatch Quando abiliti l'opzione di CloudWatch pubblicazione per le metriche di S3 Storage Lens per la prima volta, possono essere necessarie fino a 24 ore per la pubblicazione delle metriche. CloudWatch Attualmente, le metriche di S3 Storage Lens non possono essere utilizzate tramite stream. CloudWatch

Utilizzo della console S3

Quando viene aggiornato un pannello di controllo S3 Storage Lens, non è possibile modificare il nome del pannello di controllo o la regione di origine. Non è inoltre possibile cambiare l'ambito del pannello di controllo predefinito, che viene inserito nell'ambito dell'intera archiviazione dell'account.

Per aggiornare una dashboard di S3 Storage Lens per abilitare la pubblicazione CloudWatch

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli S3 Storage Lens, Dashboards.(Pannelli di controllo).
3. Scegli il pannello di controllo che desideri modificare, quindi seleziona Edit (Modifica).
4. Sotto Metrics selection (Selezione dei parametri), scegli Advanced metrics and recommendations (Raccomandazioni e parametri avanzati).

Le raccomandazioni e i parametri avanzati sono disponibili a un costo aggiuntivo. Le metriche e i consigli avanzati includono un periodo di 15 mesi per le query sui dati, metriche di utilizzo

aggregate a livello di prefisso, metriche di attività aggregate per bucket, l'opzione di CloudWatch pubblicazione e consigli contestuali che aiutano a ottimizzare i costi di storage e ad applicare le migliori pratiche di protezione dei dati. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

5. In Seleziona le funzionalità di metriche e raccomandazioni avanzate, seleziona Pubblicazione. CloudWatch

 Important

Se la configurazione abilita l'aggregazione dei prefissi per le metriche di utilizzo, le metriche a livello di prefisso non verranno pubblicate su. CloudWatch Vengono pubblicate solo le metriche di S3 Storage Lens a livello di bucket, account e organizzazione. CloudWatch

6. Scegli Save changes (Salva modifiche).

Per creare una nuova dashboard S3 Storage Lens che abiliti il supporto CloudWatch

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Seleziona Crea pannello di controllo.
4. In General (Generale), definire le opzioni di configurazione seguenti:
 - a. In Dashborard name (Nome pannello di controllo), inserisci il nome del pannello di controllo.

I nomi del pannello di controllo devono contenere meno di 65 caratteri e non possono contenere caratteri speciali o spazi. Il nome del pannello di controllo dopo la creazione non potrà più essere modificato.
 - b. Seleziona la Regione di origine del tuo pannello di controllo.

I parametri per tutte le Regioni incluse nell'ambito di questo pannello di controllo vengono archiviati centralmente in questa Regione di origine designata. In CloudWatch, le metriche di S3 Storage Lens sono disponibili anche nella regione principale. Non è possibile modificare la regione di origine dopo aver creato il pannello di controllo.
5. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.

 Note

Puoi aggiungere fino a 50 tag alla configurazione del pannello di controllo.

6. Definisci l'ambito della tua configurazione:

- a. Se stai creando una configurazione a livello di organizzazione, scegli gli account da includere nella configurazione: Include all accounts in your configuration (Includi tutti gli account nella configurazione) o Limit the scope to your signed-in account (Limita l'ambito al tuo account con accesso).

 Note

Quando si crea una configurazione a livello di organizzazione che include tutti gli account, è possibile includere o escludere solo regioni e non bucket.

- b. Seleziona le regioni e i bucket da includere in o escludere dalla configurazione del pannello di controllo eseguendo le seguenti operazioni:
- Per includere tutte le Regioni, seleziona Include Regions and buckets (Includi Regioni e bucket).
 - Per includere Regioni specifiche, spunta Include all regions (Includi tutte le Regioni). Sotto Choose regions to include (Scegli le Regioni da includere), scegli le Regioni che desideri siano incluse nel pannello di controllo di S3 Storage Lens.
 - Per includere bucket specifici, spunta Include all buckets (Includi tutti i bucket). Sotto Choose buckets to include (Scegli i bucket da includere), scegli i bucket che desideri siano inclusi da S3 Storage Lens nel pannello di controllo.

 Note

Puoi scegliere fino a 50 bucket.

7. In Metrics selection (Selezione dei parametri), scegli Advanced metrics and recommendations (Parametri e suggerimenti avanzati).

Per ulteriori informazioni sui prezzi avanzati e parametri avanzati, consulta [Prezzi di Amazon S3](#).

8. In Advanced metrics and recommendations features (Parametri avanzati e funzioni di suggerimento), seleziona le opzioni da abilitare:

- Advanced metrics (Parametri avanzati)
- CloudWatch pubblicazione

 Important

Se abiliti l'aggregazione dei prefissi per la configurazione di S3 Storage Lens, le metriche a livello di prefisso non verranno pubblicate su CloudWatch. Vengono pubblicate solo le metriche di S3 Storage Lens a livello di bucket, account e organizzazione in CloudWatch.

- Aggregazione di prefisso

 Note

Per ulteriori informazioni sui parametri avanzati e sulle funzioni di suggerimento, consulta [Selezione delle metriche](#).

9. Se hai abilitato Advanced metrics (Parametri avanzati), in Advanced metrics categories (Categorie parametri avanzati) seleziona le categorie che desideri visualizzare nel pannello di controllo di S3 Storage Lens:

- Parametri delle attività
- Detailed status code metrics (Parametri dettagliati codice di stato)
- Advanced cost optimization metrics (Parametri avanzati ottimizzazione costi)
- Advanced data protection metrics (Parametri avanzati protezione dati)

Per ulteriori informazioni sulle categorie di parametri, consulta [Categorie di parametri](#). Per un elenco completo di parametri, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

10. (Facoltativo) Configura l'esportazione dei parametri.

Per ulteriori informazioni su come configurare l'esportazione dei parametri, consulta la sezione [Utilizzo della console S3](#).

11. Seleziona Crea pannello di controllo.

Utilizzo di AWS CLI

L' AWS CLI esempio seguente abilita l'opzione di CloudWatch pubblicazione utilizzando una configurazione avanzata di metriche e raccomandazioni S3 Storage Lens a livello di organizzazione. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control put-storage-lens-configuration --account-id=555555555555 --config-id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file:///./config.json
```

config.json

```
{
  "Id": "SampleS3StorageLensConfiguration",
  "AwsOrg": {
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled": true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled": true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled": true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled": true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled": true
      },
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled": true
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled": true
      },
      "PrefixLevel": {
        "StorageMetrics": {
          "IsEnabled": true,
```

```

        "SelectionCriteria":{
            "MaxDepth":5,
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
        }
    },
    "Exclude": {
        "Regions": [
            "eu-west-1"
        ],
        "Buckets": [
            "arn:aws:s3:::amzn-s3-demo-source-bucket "
        ]
    },
    "IsEnabled": true,
    "DataExport": {
        "S3BucketDestination": {
            "OutputSchemaVersion": "V_1",
            "Format": "CSV",
            "AccountId": "111122223333",
            "Arn": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Prefix": "prefix-for-your-export-destination",
            "Encryption": {
                "SSES3": {}
            }
        },
        "CloudWatchMetrics": {
            "IsEnabled": true
        }
    }
}

```

Utilizzo di AWS SDK per Java

```

package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;

```

```
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSE3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "Source Account ID";
        String exportAccountId = "Destination Account ID";
        String exportBucketArn = "arn:aws:s3:::amzn-s3-demo-destination-bucket"; //
        The destination bucket for your metrics export must be in the same Region as your S3
        Storage Lens configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
        abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                .withDelimiter("/")
                .withMaxDepth(5)
                .withMinStorageBytesPercentage(10.0);
```

```

    PrefixLevelStorageMetrics prefixStorageMetrics = new
PrefixLevelStorageMetrics()
    .withIsEnabled(true)
    .withSelectionCriteria(selectionCriteria);
    BucketLevel bucketLevel = new BucketLevel()
    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
    .withAdvancedCostOptimizationMetrics(new
AdvancedCostOptimizationMetrics().withIsEnabled(true))
    .withAdvancedDataProtectionMetrics(new
AdvancedDataProtectionMetrics().withIsEnabled(true))
    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
    .withPrefixLevel(new
PrefixLevel().withStorageMetrics(prefixStorageMetrics));
    AccountLevel accountLevel = new AccountLevel()
    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
    .withAdvancedCostOptimizationMetrics(new
AdvancedCostOptimizationMetrics().withIsEnabled(true))
    .withAdvancedDataProtectionMetrics(new
AdvancedDataProtectionMetrics().withIsEnabled(true))
    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
    .withBucketLevel(bucketLevel);

    Include include = new Include()
    .withBuckets(Arrays.asList("arn:aws:s3:::amzn-s3-demo-bucket"))
    .withRegions(Arrays.asList(us-west-2));

    StorageLensDataExportEncryption exportEncryption = new
StorageLensDataExportEncryption()
    .withSSES3(new SSES3());
    S3BucketDestination s3BucketDestination = new S3BucketDestination()
    .withAccountId(exportAccountId)
    .withArn(exportBucketArn)
    .withEncryption(exportEncryption)
    .withFormat(exportFormat)
    .withOutputSchemaVersion(OutputSchemaVersion.V_1)
    .withPrefix("Prefix");
    CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
    .withIsEnabled(true);
    StorageLensDataExport dataExport = new StorageLensDataExport()
    .withCloudWatchMetrics(cloudWatchMetrics)
    .withS3BucketDestination(s3BucketDestination);

```

```
StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
    .withArn(awsOrgARN);

StorageLensConfiguration configuration = new StorageLensConfiguration()
    .withId(configurationId)
    .withAccountLevel(accountLevel)
    .withInclude(include)
    .withDataExport(dataExport)
    .withAwsOrg(awsOrg)
    .withIsEnabled(true);

List<StorageLensTag> tags = Arrays.asList(
    new StorageLensTag().withKey("key-1").withValue("value-1"),
    new StorageLensTag().withKey("key-2").withValue("value-2")
);

AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
    .withCredentials(new ProfileCredentialsProvider())
    .withRegion(US_WEST_2)
    .build();

s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
    .withAccountId(sourceAccountId)
    .withConfigId(configurationId)
    .withStorageLensConfiguration(configuration)
    .withTags(tags)
);
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
```

Utilizzo della REST API

Per abilitare l'opzione di CloudWatch pubblicazione utilizzando l'API REST di Amazon S3, puoi utilizzare. [PutStorageLensConfiguration](#)

Fasi successive

Dopo aver abilitato l'opzione di CloudWatch pubblicazione, puoi accedere alle metriche di S3 Storage Lens in. CloudWatch Puoi anche sfruttare CloudWatch le funzionalità per monitorare e analizzare i dati di S3 Storage Lens in. CloudWatch Per ulteriori informazioni, consulta i seguenti argomenti:

- [Dimensioni e parametri di S3 Storage Lens](#)
- [Utilizzo delle metriche di S3 Storage Lens in CloudWatch](#)

Utilizzo delle metriche di S3 Storage Lens in CloudWatch

Puoi pubblicare le metriche di S3 Storage Lens su Amazon CloudWatch per creare una visione unificata dello stato operativo in dashboard. [CloudWatch](#) Puoi anche utilizzare CloudWatch funzionalità, come allarmi e azioni attivate, calcoli metrici e rilevamento delle anomalie, per monitorare e intervenire sulle metriche di S3 Storage Lens. Inoltre, le operazioni CloudWatch API consentono alle applicazioni, compresi i provider di terze parti, di accedere alle metriche di S3 Storage Lens. Per ulteriori informazioni sulle CloudWatch funzionalità, consulta la [Amazon CloudWatch User Guide](#).

Puoi abilitare l'opzione di CloudWatch pubblicazione per configurazioni di dashboard nuove o esistenti utilizzando la console Amazon S3, le API REST di Amazon S3 e gli SDK. AWS CLI AWS L'opzione di CloudWatch pubblicazione è disponibile per le dashboard aggiornate alle metriche e ai consigli avanzati di S3 Storage Lens. Per i prezzi relativi all'opzione Advanced metrics and recommendations (Parametri e suggerimenti avanzati), consulta [Prezzi di Amazon S3](#). Non si applicano costi aggiuntivi per la pubblicazione CloudWatch delle metriche; tuttavia, si applicano altri CloudWatch costi, come dashboard, allarmi e chiamate API. Per ulteriori informazioni, consulta [i prezzi di Amazon. CloudWatch](#)

Le metriche di S3 Storage Lens vengono pubblicate CloudWatch nell'account proprietario della configurazione S3 Storage Lens. Dopo aver abilitato l'opzione di CloudWatch pubblicazione all'interno delle metriche avanzate, puoi accedere alle metriche a livello di account e bucket in base all'ID di configurazione, all'account, al bucket (solo per le metriche a livello di bucket), alla regione e alla classe di archiviazione in. CloudWatch Prefix-level CloudWatchle metriche non sono disponibili in.

 Note

Le metriche di S3 Storage Lens sono metriche giornaliere e vengono pubblicate una volta al CloudWatch giorno. Quando si interrogano le metriche di S3 Storage Lens in CloudWatch, il periodo di interrogazione deve essere di 1 giorno (86400 secondi). Dopo la visualizzazione delle metriche giornaliere di S3 Storage Lens nella dashboard di S3 Storage Lens nella console Amazon S3, possono essere necessarie alcune ore prima che queste stesse metriche vengano visualizzate. CloudWatch Quando abiliti l'opzione di CloudWatch pubblicazione per le metriche di S3 Storage Lens per la prima volta, possono essere necessarie fino a 24 ore per la pubblicazione delle metriche. CloudWatch Attualmente, le metriche di S3 Storage Lens non possono essere utilizzate tramite stream. CloudWatch

Per ulteriori informazioni sull'utilizzo delle metriche di S3 Storage Lens in CloudWatch, consulta i seguenti argomenti.

Argomenti

- [Lavorare con i dashboard CloudWatch](#)
- [Impostazione di allarmi, attivazione di azioni e utilizzo del rilevamento delle anomalie](#)
- [Filtraggio dei parametri utilizzando le dimensioni](#)
- [Calcolo di nuovi parametri con matematica dei parametri](#)
- [Utilizzo delle espressioni di ricerca nei grafici](#)

Lavorare con i dashboard CloudWatch

Puoi utilizzare CloudWatch le dashboard per monitorare le metriche di S3 Storage Lens insieme ad altre metriche delle applicazioni e creare una visione unificata dello stato operativo. Le dashboard sono home page personalizzabili nella CloudWatch console che puoi utilizzare per monitorare le tue risorse in un'unica visualizzazione.

CloudWatch dispone di un ampio controllo delle autorizzazioni che non supporta la limitazione dell'accesso a un set specifico di metriche o dimensioni. Gli utenti del tuo account o della tua organizzazione che hanno accesso a CloudWatch avranno accesso alle metriche per tutte le configurazioni di S3 Storage Lens in cui l'opzione di supporto è abilitata. CloudWatch Non è possibile gestire autorizzazioni per pannelli di controllo specifici come è possibile in S3 Storage Lens. Per

ulteriori informazioni sulle CloudWatch autorizzazioni, consulta [Gestire le autorizzazioni di accesso alle tue CloudWatch risorse](#) nella Amazon User Guide. CloudWatch

Per ulteriori informazioni sull'uso delle CloudWatch dashboard e sulla configurazione delle autorizzazioni, consulta [Using Amazon CloudWatch Dashboards](#) and [Sharing CloudWatch Dashboards nella Amazon User Guide](#). CloudWatch

Impostazione di allarmi, attivazione di azioni e utilizzo del rilevamento delle anomalie

Puoi configurare CloudWatch allarmi che controllano le metriche di S3 Storage Lens CloudWatch e agiscono quando viene superata una soglia. Ad esempio, è possibile configurare un allarme che invia una notifica di Amazon SNS quando il valore del parametro Incomplete Multipart Upload Bytes (Byte caricamenti in più parti incompleti) supera 1 GB per tre giorni consecutivi.

È inoltre possibile abilitare il rilevamento delle anomalie per analizzare continuamente i parametri di S3 Storage Lens, determinare le normali linee di base e le anomalie superficiali. Puoi creare allarmi di rilevamento delle anomalie basati sul valore previsto di un parametro. Ad esempio, è possibile monitorare le anomalie del parametro Object Lock Enabled Bytes (Byte con blocco oggetti abilitato) per rilevare una rimozione non autorizzata delle impostazioni di Blocco oggetti.

Per ulteriori informazioni ed esempi, consulta [Usare gli CloudWatch allarmi Amazon](#) e [Creare un allarme da una metrica su un grafico](#) nella Amazon User Guide. CloudWatch

Filtraggio dei parametri utilizzando le dimensioni

Puoi utilizzare le dimensioni per filtrare le metriche di S3 Storage Lens nella console. CloudWatch Ad esempio, è possibile filtrare per `configuration_id`, `aws_account_number`, `aws_region`, `bucket_name` e altri.

S3 Storage Lens supporta più configurazioni di pannello di controllo per account. Ciò significa che diverse configurazioni possono includere lo stesso bucket. Quando queste metriche vengono pubblicate su CloudWatch, il bucket conterrà metriche duplicate. CloudWatch Per visualizzare le metriche solo per una specifica configurazione di S3 Storage Lens in CloudWatch, puoi utilizzare la dimensione. `configuration_id` Quando si filtra per `configuration_id`, vengono visualizzati solo i parametri associati alla configurazione identificata.

Per ulteriori informazioni sul filtraggio per ID di configurazione, consulta [Searching for available metrics](#) nella Amazon User Guide. CloudWatch

Calcolo di nuovi parametri con matematica dei parametri

La matematica dei parametri permette di eseguire query di più parametri S3 Storage Lens e di utilizzare espressioni matematiche per creare nuove serie temporali in base a tali parametri. Ad esempio, è possibile creare un nuovo parametro per oggetti non crittografati sottraendo oggetti crittografati dal Conteggio oggetti. È inoltre possibile creare un parametro per ottenere la dimensione media dell'oggetto dividendo `StorageBytes` per `ObjectCount`, o i byte numerici a cui si accede in un giorno dividendo `BytesDownloaded` per `StorageBytes`.

Per ulteriori informazioni, consulta [Using metric math](#) nella Amazon User Guide. CloudWatch

Utilizzo delle espressioni di ricerca nei grafici

Con i parametri di S3 Storage Lens, puoi creare un'espressione di ricerca. Ad esempio, puoi creare un'espressione di ricerca per tutte le metriche denominate `IncompleteMultipartUploadStorageBytes` e `SUM` aggiungerle. Con questa espressione di ricerca, è possibile visualizzare il valore del parametro `Incomplete Multipart Upload Bytes` (Byte caricamenti in più parti incompleti) per tutte le dimensioni dell'archiviazione in un unico parametro.

Questo esempio mostra la sintassi da utilizzare per creare un'espressione di ricerca per tutte le metriche denominate. `IncompleteMultipartUploadStorageBytes`

```
SUM(SEARCH( '{AWS/S3/Storage-Lens,aws_account_number,aws_region,configuration_id,metrics_version,record_type,storage_class} MetricName="IncompleteMultipartUploadStorageBytes"', 'Average',86400))
```

Per ulteriori informazioni su questa sintassi, consulta la sintassi delle espressioni [CloudWatch di ricerca](#) nella Amazon User Guide. CloudWatch Per creare un CloudWatch grafico con un'espressione di ricerca, consulta [Creazione di un CloudWatch grafico con un'espressione di ricerca](#) nella Amazon CloudWatch User Guide.

Casi d'uso relativi ai parametri di Amazon S3 Storage Lens

Puoi utilizzare il pannello di controllo di Amazon S3 Storage Lens per visualizzare informazioni dettagliate e tendenze, contrassegnare le anomalie e ricevere suggerimenti. I parametri di S3 Storage Lens sono organizzati in categorie conformi ai principali casi di utilizzo. Puoi utilizzare questi parametri per effettuare le seguenti operazioni:

- Individuare le opportunità di ottimizzazione dei costi
- Applicare le best practice per la protezione dei dati

- Applica le best practice per la gestione degli accessi
- Migliorare le prestazioni dei carichi di lavoro delle applicazioni

Ad esempio, con i parametri relativi alla ottimizzazione dei costi, è possibile individuare le opportunità di riduzione dei costi di archiviazione di Amazon S3. Puoi individuare i bucket con caricamenti in più parti che risalgono a più di 7 giorni o i bucket che accumulano versioni non correnti.

Allo stesso modo, puoi utilizzare i parametri relativi alla protezione dei dati per individuare i bucket non conformi alle best practice di protezione dei dati all'interno dell'organizzazione. Ad esempio, puoi identificare i bucket che non utilizzano AWS Key Management Service keys (SSE-KMS) per la crittografia predefinita o che non hanno S3 Versioning abilitato.

Con i parametri relativi alla gestione degli accessi di S3 Storage Lens, puoi identificare le impostazioni della caratteristica S3 Object Ownership per i bucket in modo da poter eseguire la migrazione delle autorizzazioni delle liste di controllo degli accessi (ACL) alle policy di bucket e disabilitare le ACL.

Se hai abilitato l'opzione [Advanced metrics \(Parametri avanzati\) di S3 Storage Lens](#), puoi utilizzare i parametri dei codici di stato dettagliati per ottenere i numeri delle richieste riuscite o non riuscite per la risoluzione dei problemi relativi ad accessi e prestazioni.

Con i parametri avanzati, puoi anche accedere a parametri aggiuntivi relativi all'ottimizzazione dei costi e alla protezione dei dati che puoi utilizzare per individuare le opportunità per ridurre ulteriormente i costi complessivi dell'archiviazione S3 e allinearti meglio alle best practice per la protezione dei dati. Ad esempio, i parametri avanzati relativi all'ottimizzazione dei costi includono i conteggi delle regole del ciclo di vita che puoi utilizzare per identificare i bucket senza regole del ciclo di vita per far scadere i caricamenti in più parti incompleti che risalgono a più di 7 giorni. I parametri avanzati relativi alla protezione dei dati includono il conteggio delle regole di replica.

Per ulteriori informazioni sulle categorie di parametri, consulta [Categorie di parametri](#). Per un elenco completo dei parametri di S3 Storage Lens, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

Argomenti

- [Utilizzo di Amazon S3 Storage Lens per ottimizzare i costi di archiviazione](#)
- [Utilizzo di S3 Storage Lens per proteggere i tuoi dati](#)
- [Utilizzo di S3 Storage Lens per controllare le impostazioni di Object Ownership](#)
- [Utilizzo dei parametri di S3 Storage Lens per migliorare le prestazioni](#)

Utilizzo di Amazon S3 Storage Lens per ottimizzare i costi di archiviazione

Puoi utilizzare le metriche di ottimizzazione dei costi di S3 Storage Lens per ridurre il costo complessivo dello storage S3. Cost-optimization le metriche possono aiutarti a confermare di aver configurato Amazon S3 in modo conveniente e secondo le best practice. Ad esempio, è possibile individuare le seguenti opportunità di ottimizzazione dei costi:

- Bucket con caricamenti in più parti incompleti più vecchi di 7 giorni
- Bucket che accumulano numerose versioni non correnti
- Bucket che non hanno regole del ciclo di vita per l'interruzione dei caricamenti in più parti incompleti
- Bucket che non dispongono di regole del ciclo di vita per far scadere gli oggetti delle versioni non correnti
- Bucket che non dispongono di regole del ciclo di vita per trasferire gli oggetti a una classe di archiviazione diversa

È quindi possibile utilizzare questi dati per aggiungere ulteriori regole del ciclo di vita ai bucket.

Di seguito sono riportati esempi che mostrano come utilizzare i parametri di ottimizzazione dei costi nel pannello di controllo di S3 Storage Lens per ottimizzare i costi di archiviazione.

Argomenti

- [Identificare i bucket S3 più grandi](#)
- [Scoperta dei bucket Amazon S3 freddi](#)
- [Individuazione di caricamenti in più parti incompleti](#)
- [Riduzione del numero di versioni non correnti conservate](#)
- [Identificare i bucket senza regole del ciclo di vita ed esaminare i conteggi delle regole del ciclo di vita](#)

Identificare i bucket S3 più grandi

L'archiviazione degli oggetti nei bucket S3 è a pagamento. La tariffa che ti viene addebitata dipende dalle dimensioni degli oggetti, dalla durata di archiviazione degli oggetti e dalle relative classi di archiviazione. Con S3 Storage Lens, ottieni una vista centralizzata di tutti i bucket nel tuo account. Per visualizzare tutti i bucket in tutti gli account della tua organizzazione, puoi configurare una

dashboard S3 Storage AWS Organizations Lens a livello. Da questa vista del pannello di controllo è possibile identificare i bucket più grandi.

Fase 1: identificare i bucket più grandi

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.

Quando il pannello di controllo si apre, puoi vedere l'ultima data in cui S3 Storage Lens ha raccolto i parametri. Il pannello di controllo viene sempre caricato alla data più recente per la quale sono disponibili i parametri.

4. Per visualizzare una classifica dei bucket più grandi in base al parametro Total storage (Archiviazione totale) per un intervallo di date selezionato, scorri verso il basso fino alla sezione Top N overview for date (Panoramica primi N per [data]).

È possibile modificare l'ordinamento per mostrare i bucket più piccoli. Puoi anche modificare la selezione in Metric (Parametro) per classificare i tuoi bucket in base a uno qualsiasi dei parametri disponibili. La sezione Top N overview for date (Panoramica primi N per [data]) mostra anche la variazione percentuale rispetto al giorno o alla settimana precedente e un grafico sparkline per visualizzare la tendenza. Questa tendenza è valida per 14 giorni per i parametri gratuiti e per 30 giorni per i parametri e i suggerimenti avanzati.

Note

Con i parametri avanzati e i suggerimenti di S3 Storage Lens, i parametri sono disponibili per le query per 15 mesi. Per ulteriori informazioni, consulta [Selezione delle metriche](#).

5. Per informazioni più dettagliate sui bucket, scorri fino alla parte superiore della pagina, quindi scegli la scheda Bucket.

Nella scheda Bucket è possibile visualizzare dettagli quali il tasso di crescita recente, la dimensione media dell'oggetto, i prefissi più grandi e il numero di oggetti.

Fase 2: accedere ai bucket e analizzare

Per i bucket S3 più grandi, è quindi possibile passare a ciascun bucket all'interno della console S3 per analizzare i relativi oggetti e il carico di lavoro associato o per identificarne i proprietari interni. Puoi contattare i proprietari del bucket per scoprire se questa crescita è prevista o se necessita di ulteriore monitoraggio e controllo.

Scoperta dei bucket Amazon S3 freddi

Se hai l'opzione [Parametri avanzati di S3 Storage Lens](#) abilitata, puoi utilizzare i [parametri delle attività](#) per capire quanto sono freddi i tuoi bucket S3. Un bucket "freddo" è un bucket il cui spazio di archiviazione non è più utilizzato o è utilizzato molto raramente. Questa mancanza di attività indica in genere che gli oggetti del bucket non vengono utilizzati frequentemente.

Parametri di attività, quali Richieste GET e Byte di download, indicano la frequenza di accesso ai tuoi bucket ogni giorno. Per comprendere la coerenza del modello di accesso e individuare i bucket a cui non si accede più, è possibile seguire l'andamento di questi dati per diversi mesi. Il parametro Tasso di recupero, che viene calcolato come Byte di download/Spazio di archiviazione totale, indica la proporzione di spazio di archiviazione in un bucket a cui si accede quotidianamente.

Note

I byte di download vengono duplicati nei casi in cui lo stesso oggetto venga scaricato più volte durante il giorno.

Prerequisito

Per visualizzare i parametri relativi alle attività nel pannello di controllo di S3 Storage Lens, devi abilitare l'opzione S3 Storage Lens Advanced metrics and recommendations (Parametri e suggerimenti avanzati) e quindi selezionare Activity metrics (Parametri attività). Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

Fase 1: identificare i bucket attivi

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.

4. Seleziona la scheda Bucket e scorri verso il basso fino alla sezione grafici Bubble analysis by buckets for date (Analisi a bolle per bucket per [data]).

Nella sezione Bubble analysis by buckets for date, puoi tracciare i tuoi bucket su più dimensioni utilizzando tre metriche qualsiasi per rappresentare la X-axis Y-axis, e la dimensione della bolla.

5. Per trovare i bucket che sono andati esauriti, per e Size X-axis Y-axis , scegli le metriche Spazio di archiviazione totale,% di recupero e Dimensione media degli oggetti.
6. Nella sezione Bubble analysis by buckets for date (Analisi a bolle per bucket per [data]), individua tutti i bucket con frequenze di recupero pari a zero (o vicino a zero) e una dimensione di archiviazione relativa maggiore e quindi scegli la bolla che rappresenta il bucket.

Apparirà un riquadro con le scelte per visualizzare informazioni dettagliate più granulari. Esegui una delle seguenti operazioni:

- a. Per aggiornare la scheda Bucket in modo da visualizzare i parametri solo per il bucket selezionato, scegli Drill down (Esegui drill-down), quindi scegli Apply (Applica).
- b. Per aggregare i dati a livello di bucket per account, Regione AWS classe di archiviazione o bucket, scegli Analizza per, quindi scegli Dimension. Ad esempio, per eseguire l'aggregazione per classe di archiviazione, scegli Storage class (Classe di archiviazione) in Dimension (Dimensione).

Per trovare i bucket che si sono raffreddati, esegui un'analisi delle bolle utilizzando i parametri Archiviazione totale, % tasso di recupero e Dimensione media degli oggetti. Cerca tutti i bucket con tasso di recupero pari a zero (o vicino a zero) e una dimensione di archiviazione relativa maggiore.

La scheda Bucket del pannello di controllo viene aggiornata con i dati per l'aggregazione o il filtro selezionato. Se hai effettuato l'aggregazione per classe di archiviazione o un'altra dimensione, la nuova scheda, ad esempio la scheda Storage class (Classe di archiviazione), si apre nel pannello di controllo.

Fase 2: analizzare i bucket freddi

Da qui è possibile identificare i proprietari del bucket freddi nel tuo account o nella tua organizzazione e scoprire se lo spazio di archiviazione è ancora necessario. È quindi possibile ottimizzare i costi

impostando le [configurazioni della scadenza del ciclo di vita](#) per i bucket o archiviando i dati in una delle [classi di archiviazione Amazon Glacier](#).

Per evitare il problema dei cold bucket in futuro, puoi trasferire [automaticamente i dati utilizzando le configurazioni del ciclo di vita di S3](#) per i bucket oppure puoi abilitare l'archiviazione automatica con S3. [Intelligent-Tiering](#)

È inoltre possibile utilizzare la fase 1 per identificare i bucket "caldi". Quindi, puoi assicurarti che questi bucket utilizzino la [classe di archiviazione S3](#) corretta per garantire che soddisfino le loro richieste nel modo più efficace in termini di prestazioni e costi.

Individuazione di caricamenti in più parti incompleti

Puoi utilizzare i caricamenti in più parti per caricare oggetti di grandi dimensioni (fino a 50 TB) come set di parti per migliorare la produttività e velocizzare il ripristino dai problemi di rete. Nei casi in cui il processo di caricamento in più parti non venga portato a termine, le parti incomplete rimangono nel bucket (in uno stato inutilizzabile). Queste parti incomplete comportano costi di archiviazione fino al termine del processo di caricamento o fino alla rimozione delle parti incomplete. Per ulteriori informazioni, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

Con S3 Storage Lens, puoi identificare il numero di byte di un caricamento in più parti incompleto nel tuo account o nell'intera organizzazione, compresi i caricamenti in più parti incompleti che risalgono a più di 7 giorni. Per un elenco completo dei parametri relativi ai caricamenti in più parti incompleti, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

Come best practice, consigliamo di configurare le regole del ciclo di vita per far scadere i caricamenti in più parti incompleti più vecchi di un determinato numero di giorni. Quando crei la regola del ciclo di vita per far scadere i caricamenti in più parti incompleti, consigliamo il valore di 7 giorni come buon punto di partenza.

Fase 1: esaminare le tendenze generali relative ai caricamenti incompleti in più parti

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.
4. Nella sezione Snapshot for date (Snapshot per [data]), in Metrics categories (Categorie parametri), scegli Cost optimization (Ottimizzazione costi).

La sezione Snapshot for date (Snapshot per [data]) viene aggiornata per visualizzare i parametri Cost optimization (Ottimizzazione costi), che includono Incomplete multipart upload bytes greater than 7 days old (Byte caricamenti in più parti incompleti risalenti a più di 7 giorni).

In tutti i grafici del pannello di controllo di S3 Storage Lens, puoi vedere i parametri relativi ai caricamenti in più parti incompleti. Puoi utilizzare questi parametri per valutare ulteriormente l'impatto dei byte dei caricamenti in più parti incompleti nell'archiviazione, incluso il loro contributo alle tendenze generali di crescita. Puoi anche eseguire il drill-down sui livelli di aggregazione in dettaglio utilizzando le schede Account, Regione AWS, Bucket o Classe di archiviazione per un'analisi più approfondita dei dati. Per un esempio, consulta [Scoperta dei bucket Amazon S3 freddi](#).

Fase 2: identificare i bucket con i byte di caricamento in più parti più incompleti, ma che non dispongono di regole del ciclo di vita per interrompere i caricamenti in più parti incompleti

Prerequisito

Per visualizzare il parametro Abort incomplete multipart upload lifecycle rule count (Conteggio regole ciclo di vita interruzione caricamenti in più parti incompleti) nel pannello di controllo di S3 Storage Lens, devi abilitare l'opzione S3 Storage Lens Advanced metrics and recommendations (Parametri e suggerimenti avanzati) e quindi selezionare Advanced cost optimization metrics (Parametri avanzati ottimizzazione costi). Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.
4. Per identificare i bucket specifici che accumulano caricamenti in più parti incompleti risalenti a più di 7 giorni, vai alla sezione Top N overview for date (Panoramica primi N per [data]).

Per impostazione predefinita, la sezione Top N overview for date (Panoramica primi N per [data]) mostra i parametri per i primi 3 bucket. È possibile aumentare o diminuire il numero di bucket nel campo Top N (Primi N). La sezione Top N overview for date (Panoramica primi N per [data]) mostra anche la variazione percentuale rispetto al giorno o alla settimana precedente e un grafico sparkline per visualizzare la tendenza. Questa tendenza è valida per 14 giorni per i parametri gratuiti e per 30 giorni per i parametri e i suggerimenti avanzati.

 Note

Con i parametri avanzati e i suggerimenti di S3 Storage Lens, i parametri sono disponibili per le query per 15 mesi. Per ulteriori informazioni, consulta [Selezione delle metriche](#).

5. In Metric (Parametro), scegli Incomplete multipart upload bytes greater than 7 days old (Byte caricamenti in più parti incompleti risalenti a più di 7 giorni) nella categoria Cost optimization (Ottimizzazione costi).

Nella sezione Top number buckets (Primi [numero] bucket), puoi visualizzare i bucket con i byte di archiviazione per caricamenti in più parti incompleti che risalgono a più di 7 giorni.

6. Per visualizzare metriche più dettagliate a livello di bucket per i caricamenti multiparte incompleti, scegli la scheda Bucket.
7. Scorri fino alla sezione Buckets (Bucket). In Metrics categories (Categorie parametri), seleziona Cost optimization (Ottimizzazione dei costi). Quindi deseleziona Summary (Riepilogo).

L'elenco Buckets (Bucket) viene aggiornato per visualizzare tutti i parametri di ottimizzazione dei costi disponibili per i bucket visualizzati.

8. Per filtrare l'elenco Buckets (Bucket) in modo da visualizzare solo i parametri relativi all'ottimizzazione dei costi, scegli l'icona delle preferenze



).

9. Deseleziona tutti i parametri per l'ottimizzazione dei costi e lascia selezionati solo i parametri Incomplete multipart upload bytes greater than 7 days old (Byte caricamenti in più parti incompleti risalenti a più di 7 giorni) e Abort incomplete multipart upload lifecycle rule count (Conteggio regole ciclo di vita interruzione caricamenti in più parti incompleti).
10. (Facoltativo) In Page size (Dimensioni pagina), scegli il numero di bucket da visualizzare nell'elenco.
11. Scegli Confirm (Conferma).

L'elenco Buckets (Bucket) viene aggiornato con i parametri a livello di bucket per i conteggi dei caricamenti in più parti incompleti e per le regole del ciclo di vita. Puoi utilizzare questi dati per identificare i bucket con i byte di caricamenti in più parti più incompleti che risalgono a più di 7 giorni e che non presentano regole del ciclo di vita per interrompere i caricamenti in più parti incompleti. Quindi, puoi passare a questi bucket nella console S3 e aggiungere regole del ciclo di vita per eliminare i caricamenti in più parti incompleti abbandonati.

Fase 3: aggiungere una regola del ciclo di vita per eliminare i carichi in più parti incompleti dopo 7 giorni

Per gestire automaticamente i carichi in più parti incompleti, è possibile utilizzare la console S3 per creare una configurazione del ciclo di vita per far scadere byte di carichi in più parti incompleti da un bucket dopo un determinato numero di giorni. Per ulteriori informazioni, consulta [Configurazione del ciclo di vita del bucket per l'eliminazione dei carichi in più parti incompleti](#).

Riduzione del numero di versioni non correnti conservate

Se attivata, la funzionalità S3 di controllo delle versioni conserva più versioni dello stesso oggetto; tali versioni possono essere utilizzate per recuperare rapidamente i dati nel caso in cui un oggetto venga eliminato o sovrascritto accidentalmente. Se hai abilitato funzionalità S3 di controllo delle versioni senza configurare le regole del ciclo di vita per la transizione o la scadenza delle versioni non correnti, può accumularsi un gran numero di versioni precedenti non correnti, con ripercussioni sui costi di archiviazione. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Fase 1: identificare i bucket con il maggior numero di versioni di oggetti non correnti

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.
4. Nella sezione Snapshot for date (Snapshot per [data]), in Metric categories (Categorie parametri), scegli Cost optimization (Ottimizzazione costi).

La sezione Snapshot for date (Snapshot per [data]) viene aggiornata per visualizzare i parametri Cost optimization (Ottimizzazione costi), che includono il parametro % noncurrent version bytes (% byte versioni non correnti). Il parametro % noncurrent version bytes (% byte versioni non correnti) rappresenta la proporzione dei byte di archiviazione totali attribuita alle versioni non correnti nell'ambito del pannello di controllo e per la data selezionata.

Note

Se il valore del parametro % noncurrent version bytes (% byte versioni non correnti) è maggiore del 10% dell'archiviazione a livello di account, ciò può indicare che stai archiviando troppe versioni di oggetti.

5. Per identificare i bucket specifici che accumulano un numero elevato di versioni non correnti:
 - a. Scorri verso il basso fino alla sezione Top N overview for date (Panoramica primi N per [data]). In Top N (Primi N), inserisci il numero di bucket per i quali desideri visualizzare i dati.
 - b. In Metric (Parametro), scegli % noncurrent version bytes (% byte versioni non correnti).

In Top number buckets (Primi [numero] bucket), puoi visualizzare i bucket (per il numero specificato) con il valore più alto del parametro % noncurrent version bytes (% byte versioni non correnti). La sezione Top N overview for date (Panoramica primi N per [data]) mostra anche la variazione percentuale rispetto al giorno o alla settimana precedente e un grafico sparkline per visualizzare la tendenza. Questa tendenza è valida per 14 giorni per i parametri gratuiti e per 30 giorni per i parametri e i suggerimenti avanzati.

 Note

Con i parametri avanzati e i suggerimenti di S3 Storage Lens, i parametri sono disponibili per le query per 15 mesi. Per ulteriori informazioni, consulta [Selezione delle metriche](#).

- c. Per visualizzare metriche più dettagliate a livello di bucket per le versioni degli oggetti non correnti, scegli la scheda Bucket.

In qualsiasi grafico o visualizzazione della dashboard S3 Storage Lens, puoi approfondire i livelli di aggregazione utilizzando le schede Account, Regione AWS, Classe di archiviazione o Bucket. Per un esempio, consulta [Scoperta dei bucket Amazon S3 freddi](#).

- d. Nella sezione Buckets (Bucket), in Metric categories (Categorie parametri), seleziona Cost optimization (Ottimizzazione dei costi). Quindi seleziona Summary (Riepilogo).

A questo punto puoi visualizzare il parametro % noncurrent version bytes (% byte versioni non correnti), insieme ad altri parametri relativi alle versioni non correnti.

Fase 2: identificare i bucket privi di regole del ciclo di vita di transizione e scadenza per la gestione delle versioni non correnti

Prerequisito

Per visualizzare i parametri Noncurrent version transition lifecycle rule count (Conteggio regole ciclo di vita transizioni versione non corrente) e Noncurrent version expiration lifecycle rule count

(Conteggio regole ciclo di vita scadenza versione non corrente) nel pannello di controllo di S3 Storage Lens, devi abilitare l'opzione S3 Storage Lens Advanced metrics and recommendations (Parametri e suggerimenti avanzati) e quindi selezionare Advanced cost optimization metrics (Parametri avanzati ottimizzazione costi). Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.
4. Nel pannello di controllo di Storage Lens, scegli la scheda Bucket.
5. Scorri fino alla sezione Buckets (Bucket). In Metrics categories (Categorie parametri), seleziona Cost optimization (Ottimizzazione dei costi). Quindi deseleziona Summary (Riepilogo).

L'elenco Buckets (Bucket) viene aggiornato per visualizzare tutti i parametri di ottimizzazione dei costi disponibili per i bucket visualizzati.

6. Per filtrare l'elenco Buckets (Bucket) in modo da visualizzare solo i parametri relativi all'ottimizzazione dei costi, scegli l'icona delle preferenze



).

7. Deseleziona tutti i parametri di ottimizzazione dei costi finché non rimangono selezionati solo i seguenti parametri:
 - % noncurrent version bytes (% byte versioni non correnti)
 - Noncurrent version transition lifecycle rule count (Conteggio regole ciclo di vita transizione versioni non correnti)
 - Noncurrent version expiration lifecycle rule count (Conteggio regole ciclo di vita scadenza versioni non correnti)
8. (Facoltativo) In Page size (Dimensioni pagina), scegli il numero di bucket da visualizzare nell'elenco.
9. Scegli Confirm (Conferma).

L'elenco Buckets (Bucket) viene aggiornato con i parametri relativi ai byte di versioni non correnti e ai conteggi delle regole del ciclo di vita delle versioni non correnti. È possibile utilizzare questi dati per identificare i bucket che hanno un'alta percentuale di byte di versioni non correnti, ma sono privi di regole del ciclo di vita di transizione e scadenza. Quindi, puoi accedere a questi bucket nella console S3 e aggiungervi regole del ciclo di vita.

Fase 3: aggiungere regole del ciclo di vita per eseguire la transizione o la scadenza delle versioni degli oggetti non correnti

Dopo aver determinato quali bucket richiedono ulteriori indagini, puoi passare ai bucket all'interno della console S3 e aggiungere una regola del ciclo di vita per far scadere le versioni non correnti dopo un numero specificato di giorni. In alternativa, per ridurre i costi pur mantenendo le versioni non correnti, puoi configurare una regola del ciclo di vita per la transizione delle versioni non correnti a una delle classi di storage. Amazon Glacier Per ulteriori informazioni, consulta [Specifica di una regola del ciclo di vita per un bucket che supporta la funzionalità Controllo delle versioni](#).

Identificare i bucket senza regole del ciclo di vita ed esaminare i conteggi delle regole del ciclo di vita

S3 Storage Lens fornisce parametri relativi al numero di regole del ciclo di vita S3 che puoi utilizzare per identificare i bucket senza regole del ciclo di vita. Per trovare i bucket senza regole del ciclo di vita, puoi utilizzare il parametro Total buckets without lifecycle rules (Totale bucket senza regole ciclo di vita). Un bucket senza una configurazione S3 del ciclo di vita potrebbe disporre di un'archiviazione non più necessaria o che può essere trasferita a una classe di archiviazione a basso costo. Puoi anche utilizzare i parametri relativi al conteggio delle regole del ciclo di vita per identificare i bucket senza tipi specifici di regole del ciclo di vita, come le regole di scadenza o di transizione.

Prerequisito

Per visualizzare i parametri relativi ai conteggi delle regole ciclo di vita e il parametro Total buckets without lifecycle rules (Totale bucket senza regole ciclo di vita) nel pannello di controllo di S3 Storage Lens, devi abilitare l'opzione S3 Storage Lens Advanced metrics and recommendations (Parametri e suggerimenti avanzati) e quindi selezionare Advanced cost optimization metrics (Parametri avanzati ottimizzazione costi). Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

Fase 1: identificare i bucket senza regole del ciclo di vita

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.
4. Per identificare i bucket specifici senza regole del ciclo di vita, scorri verso il basso fino alla sezione Top N overview for date (Panoramica primi N per [data]).

Per impostazione predefinita, la sezione Top N overview for date (Panoramica primi N per [data]) mostra i parametri per i primi 3 bucket. Nel campo Top N (Primi N) è possibile aumentare il

numero di bucket. La sezione Top N overview for date (Panoramica primi N per [data]) mostra anche la variazione percentuale rispetto al giorno o alla settimana precedente e un grafico sparkline per visualizzare la tendenza. Questa tendenza è valida per 14 giorni per i parametri gratuiti e per 30 giorni per i parametri e i suggerimenti avanzati.

Note

Con i parametri avanzati e i suggerimenti di S3 Storage Lens, i parametri sono disponibili per le query per 15 mesi. Per ulteriori informazioni, consulta [Selezione delle metriche](#).

5. In Metric (Parametro), scegli Total buckets without lifecycle rules (Totale bucket senza regole ciclo di vita) nella categoria Cost optimization (Ottimizzazione costi).
6. Esamina i seguenti dati per il parametro Total buckets without lifecycle rules (Totale bucket senza regole ciclo di vita):
 - Top number accounts (Primi [numero] account): visualizza gli account con il maggior numero di bucket senza regole del ciclo di vita.
 - Top number Regions (Prime [numero] regioni): visualizza un'analisi dettagliata dei bucket senza regole del ciclo di vita per regione.
 - Top number buckets (Primi [numero] bucket): visualizza i bucket senza regole del ciclo di vita.

In qualsiasi grafico o visualizzazione della dashboard S3 Storage Lens, puoi approfondire i livelli di aggregazione utilizzando le schede Account, Regione AWS, Classe di archiviazione o Bucket. Per un esempio, consulta [Scoperta dei bucket Amazon S3 freddi](#).

Dopo aver identificato i bucket senza regole del ciclo di vita, puoi anche esaminare i conteggi specifici delle regole del ciclo di vita per i tuoi bucket.

Fase 2: rivedere i conteggi delle regole del ciclo di vita per i bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboard, scegli la dashboard da visualizzare.
4. Nel pannello di controllo di S3 Storage Lens, scegli la scheda Bucket.

5. Scorri fino alla sezione Buckets (Bucket). In Metrics categories (Categorie parametri), seleziona Cost optimization (Ottimizzazione dei costi). Quindi deseleziona Summary (Riepilogo).

L'elenco Buckets (Bucket) viene aggiornato per visualizzare tutti i parametri di ottimizzazione dei costi disponibili per i bucket visualizzati.

6. Per filtrare l'elenco Buckets (Bucket) in modo da visualizzare solo i parametri relativi all'ottimizzazione dei costi, scegli l'icona delle preferenze



).

7. Deseleziona tutti i parametri di ottimizzazione dei costi finché non rimangono selezionati solo i seguenti parametri:

- Transition lifecycle rule count (Conteggio regole ciclo di vita transizione)
- Expiration lifecycle rule count (Conteggio regole ciclo di vita scadenza)
- Noncurrent version transition lifecycle rule count (Conteggio regole ciclo di vita transizione versioni non correnti)
- Noncurrent version expiration lifecycle rule count (Conteggio regole ciclo di vita scadenza versioni non correnti)
- Abort incomplete multipart upload lifecycle rule count (Conteggio regole ciclo di vita interruzione caricamenti in più parti incompleti)
- Total lifecycle rule count (Conteggio totale regole ciclo di vita)

8. (Facoltativo) In Page size (Dimensioni pagina), scegli il numero di bucket da visualizzare nell'elenco.

9. Scegli Confirm (Conferma).

L'elenco Buckets (Bucket) viene aggiornato con i parametri relativi al conteggio delle regole del ciclo di vita per i bucket. È possibile utilizzare questi dati per identificare i bucket senza regole del ciclo di vita o i bucket a cui mancano tipi specifici di regole del ciclo di vita, ad esempio regole di scadenza o di transizione. Quindi, puoi accedere a questi bucket nella console S3 e aggiungervi regole del ciclo di vita.

Fase 3: aggiungere regole del ciclo di vita

Dopo aver identificato i bucket privi di regole del ciclo di vita, puoi aggiungere tali regole. Per ulteriori informazioni, consulta [Impostazione di una configurazione del ciclo di vita S3 in un bucket](#) e [Esempi di configurazioni del ciclo di vita S3](#).

Utilizzo di S3 Storage Lens per proteggere i tuoi dati

Puoi utilizzare i parametri per la protezione dei dati di Amazon S3 Storage Lens per identificare i bucket in cui non sono state applicate le best practice per la protezione dei dati. Puoi utilizzare questi parametri per definire e applicare impostazioni standard in linea con le best practice per proteggere i dati nei bucket del tuo account o della tua organizzazione. Ad esempio, puoi utilizzare le metriche di protezione dei dati per identificare i bucket che non utilizzano AWS Key Management Service (AWS KMS) keys (SSE-KMS) per la crittografia predefinita o le richieste che utilizzano AWS Signature Version 2 (Sigv2).

I seguenti casi d'uso forniscono strategie per l'utilizzo del pannello di controllo di S3 Storage Lens al fine di identificare i valori anomali e applicare le best practice per la protezione dei dati tra i bucket S3.

Argomenti

- [Identifica i bucket che non utilizzano la crittografia lato server con AWS KMS per la crittografia predefinita \(\) SSE-KMS](#)
- [Identificare i bucket con il controllo delle versioni S3 abilitato](#)
- [Identifica le richieste che utilizzano AWS Signature versione 2 \(Sigv2\)](#)
- [Conteggiare il numero totale di regole di replica per ogni bucket](#)
- [Identificare la percentuale di byte con blocco degli oggetti](#)

Identifica i bucket che non utilizzano la crittografia lato server con AWS KMS per la crittografia predefinita () SSE-KMS

La crittografia predefinita di Amazon S3 consente di impostare il comportamento di crittografia predefinito di un bucket S3. Per ulteriori informazioni, consulta [the section called “Impostazione della crittografia predefinita del bucket”](#).

Puoi utilizzare le metriche SSE-KMS Enabled bucket count e % bucket SSE-KMS enabled per identificare i bucket che utilizzano la crittografia lato server con AWS KMS keys () per la crittografia predefinita. SSE-KMS S3 Storage Lens fornisce anche parametri per byte non crittografati, oggetti non crittografati, byte crittografati e oggetti crittografati. Per un elenco completo di parametri, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

Puoi analizzare le metriche di SSE-KMS crittografia nel contesto delle metriche di crittografia generali per identificare i bucket che non vengono utilizzati. SSE-KMS Se desideri utilizzarlo SSE-KMS per tutti i bucket del tuo account o della tua organizzazione, puoi aggiornare le impostazioni di crittografia

predefinite da utilizzare per questi bucket. SSE-KMS Inoltre SSE-KMS, puoi utilizzare la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) o chiavi fornite dal cliente (). SSE-C Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia](#).

Fase 1: Identifica quali bucket vengono utilizzati per la crittografia predefinita SSE-KMS

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Nella sezione Tendenze e distribuzioni, scegli% numero di bucket SSE-KMS abilitato per la metrica principale e% byte crittografati per la metrica secondaria.

Il grafico Trend for date si aggiorna per visualizzare le tendenze e i byte crittografati. SSE-KMS

5. Per visualizzare approfondimenti più granulari a livello di bucket per: SSE-KMS
 - a. Scegli un punto sul grafico. Apparirà un riquadro con le scelte per visualizzare informazioni dettagliate più granulari.
 - b. Scegli la dimensione Buckets (Bucket). Quindi, scegliere Apply (Applica).
6. Nel grafico Distribuzione per bucket per data, scegli la metrica SSE-KMS abilitata per il conteggio dei bucket.
7. Ora puoi vedere quali bucket sono SSE-KMS abilitati e quali no.

Fase 2: aggiornare le impostazioni predefinite di crittografia dei bucket

Ora che hai determinato quali bucket vengono utilizzati SSE-KMS nel contesto dei tuoi% byte crittografati, puoi identificare i bucket che non utilizzano. SSE-KMS Facoltativamente, puoi quindi accedere a questi bucket all'interno della console S3 e aggiornare le loro impostazioni di crittografia predefinite per utilizzare o. SSE-KMS SSE-S3 Per ulteriori informazioni, consulta [Configurazione della crittografia predefinita](#).

Identificare i bucket con il controllo delle versioni S3 abilitato

Se attivata, la funzionalità Controllo versioni S3 conserva più versioni dello stesso oggetto che possono essere utilizzate per recuperare rapidamente i dati nel caso in cui un oggetto venga

eliminato o sovrascritto accidentalmente. Puoi utilizzare la metrica del conteggio dei Versioning-enabled bucket per vedere quali bucket utilizzano S3 Versioning. Quindi, puoi usare la console S3 per abilitare la funzionalità S3 di controllo delle versioni per altri bucket.

Fase 1: identificare i bucket con il controllo delle versioni S3 abilitato

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Storage Lens, Pannelli di controllo.
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Nella sezione Tendenze e distribuzioni, scegli il numero di Versioning-enabled bucket per la metrica principale e i bucket per la metrica secondaria.

Il grafico Trend for date (Tendenza per [data]) viene aggiornato con le tendenze per i bucket con la funzionalità S3 di controllo delle versioni abilitata. Subito sotto la riga delle tendenze, puoi vedere le sottosezioni Storage class distribution (Distribuzione classi di archiviazione) e Region distribution (Distribuzione regionale).

5. Per visualizzare informazioni dettagliate più granulari per tutti i bucket visualizzati nel grafico Trend for date (Tendenza per [data]) in modo da poter eseguire un'analisi più approfondita, procedi come segue:
 - a. Scegli un punto sul grafico. Apparirà un riquadro con le scelte per visualizzare informazioni dettagliate più granulari.
 - b. Scegli una dimensione da applicare ai tuoi dati per un'analisi più approfondita: Account, Regione AWS, Storage class (Classe di archiviazione) o Bucket. Quindi, scegliere Apply (Applica).
6. Nella sezione Bubble analysis per bucket per data, scegli le metriche del numero di bucket, dei bucket e dei Versioning-enabled bucket attivi.

La sezione Bubble analysis by buckets for date (Analisi a bolle per bucket per [data]) viene aggiornata per visualizzare i dati relativi ai parametri selezionati. Puoi utilizzare questi dati per vedere quali bucket hanno la funzionalità S3 di controllo delle versioni abilitata nel contesto del numero totale di bucket. Nella sezione Bubble analysis by buckets for date, puoi tracciare i tuoi bucket su più dimensioni utilizzando tre metriche qualsiasi per rappresentare la,, e la dimensione della bolla. X-axis Y-axis

Fase 2: abilitare il controllo delle versioni S3

Dopo aver identificato i bucket in cui è abilitata la funzionalità S3 del controllo delle versioni, puoi identificare i bucket in cui il controllo delle versioni S3 non è mai stato abilitato o il cui controllo delle versioni è sospeso. Facoltativamente, puoi quindi abilitare il controllo delle versioni per questi bucket nella console S3. Per ulteriori informazioni, consulta [Abilitazione della funzione Controllo delle versioni sui bucket](#).

Identifica le richieste che utilizzano AWS Signature versione 2 (Sigv2)

Puoi utilizzare la metrica Tutte le richieste di firma non supportate per identificare le richieste che utilizzano la versione AWS Signature 2 (Sigv2). Questi dati possono aiutarti a identificare applicazioni specifiche che utilizzano SigV2. È quindi possibile migrare queste applicazioni alla AWS Signature Version 4 (Sigv4).

SigV4 è il metodo di firma consigliato per tutte le nuove applicazioni S3. SigV4 offre una maggiore sicurezza ed è supportato in tutto. Regioni AWS Per ulteriori informazioni, consulta la sezione relativa all'[aggiornamento di Amazon S3 e all'estensione e alla modifica del periodo di obsolescenza di SigV2](#).

Prerequisito

Per visualizzare tutte le richieste di firma non supportate nel pannello di controllo di S3 Storage Lens, devi abilitare l'opzione S3 Storage Lens Advanced metrics and recommendations (Parametri e suggerimenti avanzati) e quindi selezionare Advanced data protection metrics (Parametri avanzati protezione dati). Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

Fase 1: Esamina le tendenze in materia di firma Sigv2 entro Account AWS, Regione e bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Per identificare bucket, account e regioni specifici con richieste che utilizzano SigV2:
 - a. Nella sezione Top N overview for date (Panoramica primi N per [data]), in Top N (Primi N), inserisci il numero di bucket per i quali desideri visualizzare i dati.
 - b. In Metric (Parametro), scegli All unsupported signature requests (Tutte le richieste di firma non supportate) nella categoria Data protection (Protezione dati).

La panoramica Top N per gli aggiornamenti delle date per visualizzare i dati relativi alle richieste Sigv2 per account e bucket Regione AWS. La sezione Top N overview for date (Panoramica primi N per [data]) mostra anche la variazione percentuale rispetto al giorno o alla settimana precedente e un grafico sparkline per visualizzare la tendenza. Questa tendenza è valida per 14 giorni per i parametri gratuiti e per 30 giorni per i parametri e i suggerimenti avanzati.

 Note

Con i parametri avanzati e i suggerimenti di S3 Storage Lens, i parametri sono disponibili per le query per 15 mesi. Per ulteriori informazioni, consulta [Selezione delle metriche](#).

Fase 2: identificare i bucket a cui le applicazioni accedono tramite richieste SigV2

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Nel pannello di controllo di Storage Lens, scegli la scheda Bucket.
5. Scorri fino alla sezione Buckets (Bucket). In Metrics categories (Categorie parametri), scegli Data protection (Protezione dati). Quindi deseleziona Summary (Riepilogo).

L'elenco Buckets (Bucket) viene aggiornato per visualizzare tutti i parametri di protezione dei dati disponibili per i bucket visualizzati.

6. Per filtrare l'elenco Buckets (Bucket) in modo da visualizzare solo i parametri specifici di protezione dei dati, scegli l'icona delle preferenze



).

7. Deseleziona tutti i parametri di protezione dei dati finché non rimangono selezionati solo i seguenti parametri:

- All unsupported signature requests (Tutte le richieste di firma non supportate)
- % all unsupported signature requests (% tutte le richieste di firma non supportate)

8. (Facoltativo) In Page size (Dimensioni pagina), scegli il numero di bucket da visualizzare nell'elenco.
9. Scegli Confirm (Conferma).

L'elenco Buckets (Bucket) viene aggiornato con i parametri a livello di bucket per le richieste SigV2. È possibile utilizzare questi dati per identificare bucket specifici con richieste SigV2. Quindi, puoi utilizzare queste informazioni per eseguire la migrazione delle tue applicazioni a SigV4. Per ulteriori informazioni, consulta [Authenticating Requests \(AWS Signature Version 4\)](#) nel Amazon Simple Storage Service API Reference.

Conteggiare il numero totale di regole di replica per ogni bucket

La replica S3 consente di eseguire la copia asincrona e automatica di oggetti tra bucket Amazon S3. I bucket configurati per la replica di oggetti possono essere di proprietà dello stesso Account AWS o di account diversi. Per ulteriori informazioni, consulta [Replica di oggetti all'interno e tra le Regioni](#).

Puoi utilizzare i parametri relativi al conteggio delle regole di replica di S3 Storage Lens per ottenere informazioni dettagliate per bucket sui bucket configurati per la replica. Queste informazioni includono le regole di replica all'interno di e tra bucket e regioni.

Prerequisito

Per visualizzare i parametri relativi al conteggio delle regole di replica nel pannello di controllo di S3 Storage Lens, devi abilitare l'opzione S3 Storage Lens Advanced metrics and recommendations (Parametri e suggerimenti avanzati) e quindi selezionare Advanced data protection metrics (Parametri avanzati protezione dati). Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

Fase 1: contare il numero totale di regole di replica per ogni bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Nel pannello di controllo di Storage Lens, scegli la scheda Bucket.
5. Scorri fino alla sezione Buckets (Bucket). In Metrics categories (Categorie parametri), scegli Data protection (Protezione dati). Quindi deseleziona Summary (Riepilogo).

6. Per filtrare l'elenco Buckets (Bucket) in modo da visualizzare solo i parametri relativi al conteggio delle regole di replica, scegli l'icona delle preferenze



).

7. Deseleziona tutti i parametri di protezione dei dati finché non rimangono selezionati solo i parametri relativi al conteggio delle regole di replica:
 - Same-Region Numero delle regole di replica
 - Cross-Region Conteggio delle regole di replica
 - Same-account conteggio delle regole di replica
 - Cross-account conteggio delle regole di replica
 - Total replication rule count (Conteggio totale regole di replica)
8. (Facoltativo) In Page size (Dimensioni pagina), scegli il numero di bucket da visualizzare nell'elenco.
9. Scegli Confirm (Conferma).

Fase 2: aggiungere regole di replica

Dopo aver creato il conteggio delle regole di replica per bucket, facoltativamente è possibile creare altre regole di replica. Per ulteriori informazioni, consulta [Esempi di configurazione della replica in tempo reale](#).

Identificare la percentuale di byte con blocco degli oggetti

La funzionalità S3 di blocco degli oggetti consente di archiviare gli oggetti utilizzando il modello write-once-read-many (WORM). Puoi usare il blocco degli oggetti per impedire che gli oggetti vengano eliminati o sovrascritti per un periodo di tempo fisso o indefinito. Puoi abilitare il blocco degli oggetti solo quando crei un bucket e abiliti anche la funzionalità S3 di controllo delle versioni. Tuttavia, puoi modificare il periodo di conservazione per le versioni dei singoli oggetti o applicare il blocco a fini legali per i bucket in cui è abilitato il blocco degli oggetti. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).

Puoi utilizzare i parametri di blocco degli oggetti in S3 Storage Lens per visualizzare il parametro % Object Lock in bytes (% blocco oggetti in byte) per il tuo account o la tua organizzazione. Puoi utilizzare queste informazioni per identificare i bucket non conformi alle best practice di protezione dei dati nel tuo account o nella tua organizzazione.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Nella sezione Snapshot, in Metrics categories (Categorie parametri), scegli Data protection (Protezione dati).

La sezione Snapshot viene aggiornata per visualizzare i parametri di protezione dei dati, incluso il parametro % Object Lock in bytes (% blocco oggetti in byte). Puoi vedere la percentuale complessiva di byte con blocco degli oggetti per il tuo account o la tua organizzazione.

5. Per visualizzare il valore del parametro % Object Lock bytes (% blocco oggetti in byte) per bucket, scorri verso il basso fino alla sezione Top N overview (Panoramica primi N).

Per ottenere dati a livello di oggetto per il blocco degli oggetti, puoi anche utilizzare i parametri Object Lock object count (Conteggio oggetti con blocco oggetti) e % Object Lock objects (% oggetti con blocco oggetti).

6. In Metric (Parametro), scegli % Object Lock bytes (% blocco oggetti in byte) nella categoria Data protection (Protezione dati).

Per impostazione predefinita, la sezione Top N overview for date (Panoramica primi N per [data]) mostra i parametri per i primi 3 bucket. Nel campo Top N (Primi N) è possibile aumentare il numero di bucket. La sezione Top N overview for date (Panoramica primi N per [data]) mostra anche la variazione percentuale rispetto al giorno o alla settimana precedente e un grafico sparkline per visualizzare la tendenza. Questa tendenza è valida per 14 giorni per i parametri gratuiti e per 30 giorni per i parametri e i suggerimenti avanzati.

Note

Con i parametri avanzati e i suggerimenti di S3 Storage Lens, i parametri sono disponibili per le query per 15 mesi. Per ulteriori informazioni, consulta [Selezione delle metriche](#).

7. Controlla i seguenti dati per il parametro % Object Lock bytes (% blocco oggetti in byte):
 - Top number accounts (Primi [numero] account): verifica quali account hanno il valore più alto e il valore più basso per il parametro % Object Lock bytes (% blocco oggetti in byte).

- Top number Regions (Prime [numero] regioni): visualizza un'analisi dettagliata dei valori del parametro % Object Lock bytes (% blocco oggetti in byte) per regione.
- Top number buckets (Primi [numero] bucket): verifica quali bucket hanno il valore più alto e il valore più basso per il parametro % Object Lock bytes (% blocco oggetti in byte).

Utilizzo di S3 Storage Lens per controllare le impostazioni di Object Ownership

Amazon S3 Object Ownership è un'impostazione a livello di bucket S3 che puoi utilizzare per disabilitare le liste di controllo degli accessi (ACL) e controllare la proprietà degli oggetti nel bucket. Se la caratteristica Object Ownership è impostata su Bucket owner enforced (Applicata da proprietario bucket), puoi disabilitare le [liste di controllo accessi \(ACL\)](#) e assumere la proprietà di ogni oggetto incluso nel tuo bucket. Questo approccio semplifica la gestione degli accessi per i dati archiviati in Amazon S3.

Per impostazione predefinita, quando un altro Account AWS carica un oggetto nel tuo bucket S3, quell'account (l'object writer) possiede l'oggetto, vi ha accesso e può concedere ad altri utenti l'accesso ad esso tramite ACL. È possibile utilizzare Object Ownership per modificare questo comportamento di default.

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. Pertanto, è consigliabile disabilitare le ACL, tranne in circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Se la caratteristica Object Ownership è impostata su Bucket owner enforced (Applicata da proprietario bucket), è possibile disabilitare le ACL e usare le policy per il controllo degli accessi. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Con i parametri di gestione degli accessi di S3 Storage Lens, puoi identificare i bucket in cui le liste di controllo degli accessi non sono state disabilitate. Dopo aver identificato questi bucket, puoi eseguire la migrazione delle autorizzazioni ACL alle policy e disabilitare le ACL per questi bucket.

Argomenti

- [Fase 1: identificare le tendenze generali per le impostazioni di Object Ownership](#)
- [Fase 2: identificare le tendenze a livello di bucket per le impostazioni di Object Ownership](#)
- [Fase 3: aggiornare l'impostazione di Object Ownership su Bucket owner enforced \(Applicata da proprietario bucket\) per disabilitare le ACL](#)

Fase 1: identificare le tendenze generali per le impostazioni di Object Ownership

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Nella sezione Snapshot for date (Snapshot per [data]), in Metrics categories (Categorie parametri), scegli Access management (Gestione accessi).

La sezione Snapshot for date (Snapshot per [data]) viene aggiornata in modo da visualizzare il parametro % Object Ownership bucket owner enforced (% Object Ownership applicata da proprietario bucket). Puoi visualizzare la percentuale complessiva di bucket nell'account o organizzazione che usano l'impostazione Bucket owner enforced (Applicata da proprietario bucket) per Object Ownership per disabilitare le liste di controllo degli accessi.

Fase 2: identificare le tendenze a livello di bucket per le impostazioni di Object Ownership

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Per visualizzare parametri più dettagliati a livello di bucket, scegli la scheda Bucket.
5. Nella sezione Distribution by buckets for date (Distribuzione per bucket per [data]), scegli il parametro % Object Ownership bucket owner enforced (% Object Ownership applicata da proprietario bucket).

Il grafico viene aggiornato per mostrare una ripartizione per bucket per il parametro % Object Ownership bucket owner enforced (% Object Ownership applicata da proprietario bucket). Puoi vedere quali bucket utilizzano l'impostazione Bucket owner enforced (Applicata da proprietario bucket) per la caratteristica Object Ownership per disabilitare le ACL.

6. Per visualizzare le impostazioni per Bucket owner enforced (Applicata da proprietario bucket) nel contesto, scorri verso il basso fino alla sezione Buckets (Bucket). In Metrics categories (Categorie parametri), seleziona Access management (Gestione accessi). Quindi deselecta Summary (Riepilogo).

Nell'elenco Buckets (Bucket) sono visualizzati i dati di tutte e tre le impostazioni di Object Ownership: Bucket owner enforced (Proprietario del bucket imposto), Bucket Owner Preferred (Proprietario preferito del bucket) e Object Writer.

7. Per filtrare l'elenco Buckets (Bucket) in modo da visualizzare i parametri metriche solo per una specifica impostazione di Object Ownership, scegli l'icona delle preferenze



).

8. Cancella i parametri che non desideri visualizzare.
9. (Facoltativo) In Page size (Dimensioni pagina), scegli il numero di bucket da visualizzare nell'elenco.
10. Scegli Confirm (Conferma).

Fase 3: aggiornare l'impostazione di Object Ownership su Bucket owner enforced (Applicata da proprietario bucket) per disabilitare le ACL

Dopo aver identificato i bucket che utilizzano l'impostazione Object Writer e Bucket Owner Preferred (Preferita da proprietario bucket) per Object Ownership, puoi eseguire la migrazione delle autorizzazioni ACL alle policy di bucket. Dopo aver completato la migrazione delle autorizzazioni ACL, puoi aggiornare l'impostazione di Object Ownership su Bucket owner enforced (Applicata da proprietario bucket) per disabilitare le ACL. Per ulteriori informazioni, consulta [Prerequisiti per la disabilitazione delle ACL](#).

Utilizzo dei parametri di S3 Storage Lens per migliorare le prestazioni

Se hai abilitato l'opzione [Advanced metrics \(Parametri avanzati\) di S3 Storage Lens](#), puoi utilizzare i parametri dei codici di stato dettagliati per ottenere i numeri delle richieste riuscite o non riuscite. È possibile utilizzare queste informazioni per risolvere i problemi relativi ad accesso e prestazioni. I parametri dei codici di stato dettagliati mostrano i conteggi dei codici di stato HTTP, come 403 Forbidden (403 Accesso negato) e 503 Service Unavailable (503 Servizio non disponibile). Puoi esaminare le tendenze generali relative ai parametri dei codici di stato dettagliati a livello di bucket S3, account e organizzazioni. Puoi quindi eseguire il drill-down dei parametri a livello di bucket per identificare i carichi di lavoro che attualmente accedono a questi bucket e causano errori.

Ad esempio, puoi esaminare il parametro 403 Forbidden error count (Conteggio errori 403 Accesso negato) per identificare i carichi di lavoro che accedono ai bucket senza le autorizzazioni corrette applicate. Dopo aver identificato questi carichi di lavoro, puoi eseguire un'analisi approfondita all'esterno di S3 Storage Lens per risolvere gli errori 403 Forbidden (403 Accesso negato).

Questo esempio mostra come eseguire un'analisi delle tendenze per l'errore 403 Forbidden (403 Accesso negato) utilizzando i parametri 403 Forbidden error count (Conteggio errori 403 Accesso negato) e % 403 Forbidden errors (% errori 403 Accesso negato). Puoi utilizzare questi parametri per identificare i carichi di lavoro che accedono ai bucket senza le autorizzazioni corrette applicate. Puoi eseguire un'analisi delle tendenze simile per qualsiasi altro parametro dei codici di stato dettagliati. Per ulteriori informazioni, consulta [Glossario dei parametri di Amazon S3 Storage Lens](#).

Prerequisito

Per visualizzare il parametro Detailed status code metrics (Parametri codice di stato dettagliato) nel pannello di controllo di S3 Storage Lens, devi abilitare l'opzione S3 Storage Lens Advanced metrics and recommendations (Parametri e suggerimenti avanzati) e quindi selezionare Detailed status code metrics (Parametri codice di stato dettagliato). Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

Argomenti

- [Fase 1: eseguire un'analisi delle tendenze per un singolo codice di stato HTTP](#)
- [Fase 2: analizzare il conteggio degli errori per bucket](#)
- [Fase 3: correggere gli errori](#)

Fase 1: eseguire un'analisi delle tendenze per un singolo codice di stato HTTP

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Nella sezione Tendenze e distribuzioni, in Parametro primario, scegli Conteggio errori 403 Forbidden nella categoria Codici di stato dettagliati. In Secondary metric (Parametro secondario), scegli % 403 Forbidden errors (% errori 403 Accesso negato).
5. Scorri verso il basso fino alla sezione Top N overview for date (Panoramica primi N per [data]). In Parametri, scegli Conteggio errori 403 Forbidden o % errori 403 Forbidden nella categoria Codici di stato dettagliati.

La panoramica delle prime N per la sezione relativa alla data viene aggiornata per visualizzare i 403 principali numeri di errori proibiti suddivisi per account e Regione AWS bucket.

Fase 2: analizzare il conteggio degli errori per bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, Dashboards (Pannelli di controllo).
3. Nell'elenco Dashboards (Pannelli di controllo), scegli il pannello di controllo che desideri visualizzare.
4. Nel pannello di controllo di Storage Lens, scegli la scheda Bucket.
5. Scorri fino alla sezione Buckets (Bucket). In Metrics categories (Categorie parametri), seleziona il parametro Detailed status code (Codice di stato dettagliato). Quindi deseleziona Summary (Riepilogo).

L'elenco Buckets (Bucket) viene aggiornato per visualizzare tutti i parametri dei codici di stato dettagliati disponibili. È possibile utilizzare queste informazioni per individuare i bucket con una elevata percentuale di codici di stato HTTP specifici e i codici di stato comuni tra bucket.

6. Per filtrare l'elenco Buckets (Bucket) in modo da visualizzare solo i parametri relativi a codici di stato dettagliati specifici, scegli l'icona delle preferenze



).

7. Deseleziona i parametri dei codici di stato dettagliati che non desideri visualizzare nell'elenco Buckets (Bucket).
8. (Facoltativo) In Page size (Dimensioni pagina), scegli il numero di bucket da visualizzare nell'elenco.
9. Scegli Confirm (Conferma).

L'elenco Buckets (Bucket) mostra i parametri relativi al conteggio degli errori per il numero di bucket specificato. È possibile utilizzare queste informazioni per identificare bucket specifici che presentano molti errori e per risolvere gli errori per bucket.

Fase 3: correggere gli errori

Dopo aver identificato i bucket con una percentuale elevata di codici di stato HTTP specifici, è possibile risolvere questi errori. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Perché ricevo un errore 403 Forbidden \(403 Accesso negato\) quando tento di caricare file in Amazon S3?](#)

- [Perché ricevo un errore 403 Forbidden \(403 Accesso negato\) quando tento di modificare una policy di bucket in Amazon S3?](#)
- [Come posso correggere gli errori 403 Forbidden \(403 Accesso negato\) nel mio bucket Amazon S3 in cui tutte le risorse provengono dallo stesso Account AWS?](#)
- [Come posso risolvere un errore HTTP 500 o 503 in Amazon S3?](#)

Utilizzo dei dati di S3 Storage Lens nelle tabelle S3

Amazon S3 Storage Lens può esportare le analisi e le informazioni sullo storage in S3 Tables, consentendoti di interrogare le metriche di Storage Lens utilizzando SQL con servizi di AWS analisi come Amazon Athena, Amazon EMR, Amazon SageMaker Studio (SMStudio) e altri strumenti di analisi. AWS Quando configuri S3 Storage Lens per l'esportazione in tabelle S3, le metriche vengono automaticamente archiviate in tabelle Apache Iceberg di sola lettura nel bucket di tabelle gestite. AWSaws-s3

Questa integrazione fornisce l'accesso ai dati strutturati per l'interrogazione delle metriche di Storage Lens utilizzando SQL standard, l'integrazione delle analisi con AWS i servizi di analisi, le funzionalità di analisi storica e l'ottimizzazione dei costi senza costi aggiuntivi per l'esportazione in tabelle S3 gestite. AWS

Argomenti

- [Esportazione delle metriche di S3 Storage Lens in tabelle S3](#)
- [Denominazione della tabella per l'esportazione di S3 Storage Lens in tabelle S3](#)
- [Informazioni sugli schemi delle tabelle S3 Storage Lens](#)
- [Autorizzazioni per le tabelle S3 Storage Lens](#)
- [Interrogazione dei dati di S3 Storage Lens con strumenti di analisi](#)
- [Utilizzo degli assistenti AI con le tabelle S3 Storage Lens](#)

Esportazione delle metriche di S3 Storage Lens in tabelle S3

Puoi configurare Amazon S3 Storage Lens per esportare le analisi e le informazioni sullo storage in S3 Tables. Quando abiliti l'esportazione delle tabelle S3, le metriche vengono automaticamente archiviate in tabelle Apache Iceberg di sola lettura nel bucket di aws-s3 tabelle AWS gestite, rendendole interrogabili tramite SQL con servizi di AWS analisi come Amazon Athena, Amazon Redshift e Amazon EMR.

 Note

Non sono previsti costi aggiuntivi per l'esportazione delle metriche di S3 Storage Lens in tabelle S3 gestite. AWS Si applicano le tariffe standard per l'archiviazione delle tabelle, la gestione delle tabelle e le richieste sui tavoli. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Abilita l'esportazione delle tabelle S3 utilizzando la console

1. Accedi alla console di AWS gestione e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli Storage Lens, quindi scegli Storage Lens Dashboards.
3. Nell'elenco Storage Lens Dashboards, scegli la dashboard che desideri modificare.
4. Scegli Modifica.
5. Nella pagina Dashboard, vai alla sezione Esportazione e pubblicazione delle metriche.
6. Per abilitare l'esportazione della tabella per il rapporto sulle metriche predefinite, seleziona Table bucket nel tipo Bucket.
7. Per abilitare il report sulle metriche di Table Export for Expanded Prefixes, seleziona Table bucket nel tipo Bucket.
8. Rivedi la configurazione della dashboard e scegli Invia.

 Note

Dopo aver abilitato l'esportazione di S3 Tables, possono essere necessarie fino a 48 ore prima che i primi dati siano disponibili nelle tabelle.

 Note

Non sono previsti costi aggiuntivi per l'esportazione delle metriche di S3 Storage Lens in tabelle S3 gestite. AWS Si applicano le tariffe standard per l'archiviazione delle tabelle, la gestione delle tabelle, le richieste sulle tabelle e il monitoraggio. Puoi abilitare o disabilitare

l'esportazione in tabelle S3 utilizzando la console Amazon S3, l'API Amazon S3, il AWS CLI, o gli SDK. AWS

Note

Per impostazione predefinita, i record nelle tabelle S3 non scadono. Per ridurre al minimo i costi di archiviazione per le tabelle, puoi abilitare e configurare la scadenza dei record per le tabelle. Con questa opzione, Amazon S3 rimuove automaticamente i record da una tabella quando i record scadono. Per ulteriori informazioni, consulta [Scadenza del record per le tabelle](#).

Abilita l'esportazione delle tabelle S3 utilizzando AWS CLI

Note

Prima di eseguire i seguenti comandi, assicurati di disporre di una versione CLI aggiornata. Vedi [Installazione o aggiornamento alla versione più recente di AWS CLI](#).

L'esempio seguente abilita l'esportazione delle tabelle S3 per un «Rapporto sulle metriche predefinite» di una configurazione di S3 Storage Lens utilizzando il. AWS CLI Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws s3control put-storage-lens-configuration --account-id=555555555555 --config-id=your-configuration-id --storage-lens-configuration '{
  "Id":"your-configuration-id",
  "AccountLevel":{
    "ActivityMetrics":{
      "IsEnabled":true
    },
    "BucketLevel":{
      "ActivityMetrics":{
        "IsEnabled":true
      }
    }
  },
  "DataExport":{
```



```

    "S3BucketDestination":{
      "OutputSchemaVersion":"V_1",
      "Format":"CSV",
      "AccountId":"555555555555",
      "Arn":"arn:aws:s3::my-export-bucket",
      "Prefix":"storage-lens-exports/"
    },
    "StorageLensTableDestination":{
      "IsEnabled":true
    }
  },
  "IsEnabled":true
}'

```

Abilita l'esportazione delle tabelle S3 utilizzando il AWS SDK

L'esempio seguente abilita l'esportazione delle tabelle S3 per un «report sulle metriche predefinite» di una configurazione di S3 Storage Lens utilizzando l' AWS SDK per Python (Boto3). Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```

import boto3

s3control = boto3.client('s3control')

response = s3control.put_storage_lens_configuration( AccountId='555555555555',
  ConfigId='your-configuration-id', StorageLensConfiguration={
    'Id': 'your-configuration-id',
    'AccountLevel': {
      'ActivityMetrics': {
        'IsEnabled': True
      },
      'BucketLevel': {
        'ActivityMetrics': {
          'IsEnabled': True
        }
      }
    },
    'DataExport': {
      'S3BucketDestination': {
        'OutputSchemaVersion': 'V_1',
        'Format': 'CSV',
        'AccountId': '555555555555',

```

```
        'Arn': 'arn:aws:s3::my-export-bucket',  
        'Prefix': 'storage-lens-exports/'  
    },  
    'StorageLensTableDestination': {  
        'IsEnabled': True  
    }  
},  
'IsEnabled': True  
}  
)
```

Per ulteriori informazioni sull'uso degli SDK, consulta SDK e strumenti AWS . [AWS](#)

Fasi successive

Dopo aver abilitato l'esportazione delle tabelle S3, puoi:

- Ulteriori informazioni su [Denominazione della tabella per l'esportazione di S3 Storage Lens in tabelle S3](#)
- Ulteriori informazioni su [Informazioni sugli schemi delle tabelle S3 Storage Lens](#)

Denominazione della tabella per l'esportazione di S3 Storage Lens in tabelle S3

Quando si esportano le metriche di S3 Storage Lens in tabelle S3, le tabelle vengono organizzate utilizzando le convenzioni del catalogo Apache Iceberg con modelli di denominazione specifici per garantire compatibilità e organizzazione.

Struttura della posizione delle tabelle

La posizione completa della tabella segue questo schema:

```
s3tablescatalog/aws-s3/<namespace>/<table-name>
```

Nome del bucket della tabella

Secchio da tavolo: aws-s3

L'esportazione di S3 Storage Lens utilizza il bucket aws-s3 table, che è il bucket designato per le tabelle di sistema. AWS S3-related

Nome del catalogo

Catalogo: `s3tablescatalog/aws-s3`

Le tabelle S3 Storage Lens sono archiviate nel catalogo S3 perché Storage Lens fornisce informazioni su tre tipi di risorse S3:

- Metriche di archiviazione
- Proprietà dei bucket
- Metriche di utilizzo delle API

Convenzione di denominazione dei namespace

I namespace organizzano le tabelle all'interno del catalogo. Per S3 Storage Lens, lo spazio dei nomi è derivato dall'ID di configurazione di Storage Lens.

Formato standard dello spazio dei nomi

Per gli ID di configurazione di Storage Lens senza punti (.): .

```
lens_<configuration-id>_exp
```

Esempio: se l'ID di configurazione è `my-lens-config`, lo spazio dei nomi sarà:

```
lens_my-lens-config_exp
```

Formato dello spazio dei nomi con gestione dei caratteri a punti o delle lettere maiuscole

Gli ID di configurazione di Storage Lens possono contenere punti (.) o lettere maiuscole (A-Z), ma i namespace di S3 Tables supportano solo lettere minuscole, numeri, trattini () e caratteri di sottolineatura (). - _ Quando l'ID di configurazione contiene punti, questi vengono convertiti in trattini, le lettere maiuscole vengono convertite in lettere minuscole e viene aggiunto un suffisso cancelletto per l'unicità:

```
lens_<configuration-id-with-dots-or-uppercase-replaced>_exp_<7-char-hash>
```

Esempio: se l'ID di configurazione è `my.LENS.config`, lo spazio dei nomi sarà: `my.LENS.config`

```
lens_my-lens-config_exp_a1b2c3d
```

Dove a1b2c3d sono i primi 7 caratteri dell' SHA-1 hash dell'ID di configurazione originale.

Esempi completi

Per una configurazione Storage Lens con IDproduction-metrics:

- Secchio da tavolo: aws-s3
- Catalogo: s3tablescatalog/aws-s3
- Namespace: lens_production-metrics_exp
- Percorso completo: s3tablescatalog/aws-s3/lens_production-metrics_exp/<table-name>

Per una configurazione Storage Lens con IDprod.us.east.metrics:

- Secchio da tavolo: aws-s3
- Catalogo: s3tablescatalog/aws-s3
- Namespace: lens_prod-us-east-metrics_exp_f8e9a1b (con hash)
- Percorso completo: s3tablescatalog/aws-s3/lens_prod-us-east-metrics_exp_f8e9a1b/<table-name>

Tipo di tabella

La tabella seguente mostra i diversi tipi di tabelle create per le esportazioni di S3 Storage Lens:

Catalogo	Namespace	Nome della tabella S3	Description
s3tablescatalog/aws-s3	<conf_name><hash>obiettivo_ _exp [_]	metriche_di_storag e_default_default_	Questa tabella contiene le metriche di archiviazione per la configurazione di Storage Lens.
s3tablescatalog/aws-s3	<conf_name><hash>obiettivo_ _exp [_]	metriche_di_attivi tà_predefinite	Questa tabella contiene le metriche di attività per la configurazione di Storage Lens.
s3tablescatalog/aws-s3	<hash>obiettivo_<conf_name>_exp [_]	metriche_expanded_ prefixes_storage_m etrics	Questa tabella contiene le metriche di archiviazione per tutti

Catalogo	Namespace	Nome della tabella S3	Description
			i prefissi nella configurazione di Storage Lens.
s3tablescatalog/aw s-s3	<conf_name><hash>ob iettivo__exp [_]	metriche_di_attivi tà_espanse	Questa tabella contiene le metriche di attività per tutti i prefissi nella configurazione di Storage Lens.
s3tablescatalog/aw s-s3	<conf_name><hash>ob iettivo__exp [_]	bucket_property_me trics	Questa tabella contiene le metriche delle proprietà dei bucket per tutti i bucket nella configurazione di Storage Lens.

Fasi successive

- Ulteriori informazioni su [Informazioni sugli schemi delle tabelle S3 Storage Lens](#)
- Ulteriori informazioni su [Autorizzazioni per le tabelle S3 Storage Lens](#)

Informazioni sugli schemi delle tabelle S3 Storage Lens

Quando si esportano le metriche di S3 Storage Lens in tabelle S3, i dati vengono organizzati in tre schemi di tabella separati: metriche di archiviazione, metriche delle proprietà del bucket e metriche di attività.

Schema della tabella delle metriche di archiviazione

Nome	Tipo	Description
version_number	stringa	Identificatore della versione dello schema della tabella
configuration_id	stringa	Nome di configurazione S3 Storage Lens
report_time	timestamptz	Data a cui si riferisce il rapporto S3 Storage Lens
aws_account_id	stringa	ID account a cui si riferisce la voce

Nome	Tipo	Description
aws_region	stringa	Region
storage_class	stringa	Classe di storage
record_type	stringa	Tipo di record, correlato al livello di aggregazione dei dati. Valori:ACCOUNT,BUCKET,, PREFIXSTORAGE_LENS_GROUP_BUCKET ,STORAGE_LENS_GROUP_ACCOUNT .
record_value	stringa	Disambiguatore per i tipi di record che contengono più di un record. Viene utilizzato per fare riferimento al prefisso
bucket_name	stringa	Nome bucket
object_count	Long	Numero di oggetti memorizzati per l'elemento di riferimento corrente
storage_bytes	DECIMALE (38,0)	Numero di byte memorizzati per l'elemento di riferimento corrente
bucket_key_sse_kms_object_count	Long	Numero di oggetti crittografati con una chiave gestita dal cliente memorizzata per l'elemento di riferimento corrente
bucket_key_sse_kms_storage_bytes	DECIMALE (38,0)	Numero di byte crittografati con una chiave gestita dal cliente memorizzata per l'elemento di riferimento corrente
current_version_object_count	Long	Numero di oggetti della versione corrente archiviati per l'elemento di riferimento corrente
current_version_storage_bytes	DECIMALE (38,0)	Numero di byte della versione corrente memorizzati per l'elemento di riferimento corrente

Nome	Tipo	Description
delete_marker_object_count	Long	Numero di oggetti marker di eliminazione memorizzati per l'elemento di riferimento corrente
delete_marker_storage_bytes	DECIMALE (38,0)	Numero di byte dell'indicatore di eliminazione memorizzati per l'elemento di riferimento corrente
encrypted_object_count	Long	Numero di oggetti crittografati archiviati per l'elemento di riferimento corrente
encrypted_storage_bytes	DECIMALE (38,0)	Numero di byte crittografati memorizzati per l'elemento di riferimento corrente
incomplete_mpu_object_older_than_7_days_count	Long	Numero di oggetti caricati in più parti incompleti più vecchi di 7 giorni e archiviati per l'elemento attualmente referenziato
incomplete_mpu_storage_older_than_7_days_bytes	DECIMALE (38,0)	Numero di byte di caricamento in più parti incompleti archiviati più vecchi di 7 giorni per l'elemento di riferimento corrente
incomplete_mpu_object_count	Long	Numero di oggetti di caricamento in più parti incompleti archiviati per l'elemento attualmente referenziato
incomplete_mpu_storage_bytes	DECIMALE (38,0)	Numero di byte di caricamento in più parti incompleti memorizzati per l'elemento di riferimento corrente

Nome	Tipo	Description
non_current_version_object_count	Long	Numero di oggetti della versione non corrente memorizzati per l'elemento di riferimento corrente
non_current_version_storage_bytes	DECIMALE (38,0)	Numero di byte della versione non corrente memorizzati per l'elemento di riferimento corrente
object_lock_enabled_object_count	Long	Numero di oggetti memorizzati con il blocco abilitato per l'elemento di riferimento corrente
object_lock_enabled_storage_bytes	DECIMALE (38,0)	Numero di byte memorizzati per gli oggetti con blocco abilitato nell'elemento di riferimento corrente
replicated_object_count	Long	Numero di oggetti replicati per l'elemento di riferimento corrente
replicated_storage_bytes	DECIMALE (38,0)	Numero di byte replicati per l'elemento di riferimento corrente
replicated_object_source_count	Long	Numero di oggetti replicati come origine archiviata per l'elemento di riferimento corrente
replicated_storage_source_bytes	DECIMALE (38,0)	Numero di byte replicati come origine per l'elemento di riferimento corrente
sse_kms_object_count	Long	Numero di oggetti crittografati con chiave SSE memorizzata per l'elemento di riferimento corrente

Nome	Tipo	Description
sse_kms_storage_bytes	DECIMALE (38,0)	Numero di byte crittografati con chiave SSE memorizzati per l'elemento di riferimento corrente
object_0kb_count	Long	Numero di oggetti con dimensioni pari a 0 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_0kb_to_128kb_count	Long	Numero di oggetti con dimensioni superiori a 0 KB e inferiori o uguali a 128 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_128kb_to_256kb_count	Long	Numero di oggetti con dimensioni superiori a 128 KB e inferiori o uguali a 256 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_256kb_to_512kb_count	Long	Numero di oggetti con dimensioni superiori a 256 KB e inferiori o uguali a 512 KB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_512kb_to_1mb_count	Long	Numero di oggetti con dimensioni superiori a 512 KB e inferiori o uguali a 1 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_1mb_to_2mb_count	Long	Numero di oggetti con dimensioni superiori a 1 MB e inferiori o uguali a 2 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_2mb_to_4mb_count	Long	Numero di oggetti con dimensioni superiori a 2 MB e inferiori o uguali a 4 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione

Nome	Tipo	Description
object_4mb_to_8mb_count	Long	Numero di oggetti con dimensioni superiori a 4 MB e inferiori o uguali a 8 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_8mb_to_16mb_count	Long	Numero di oggetti con dimensioni superiori a 8 MB e inferiori o uguali a 16 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_16mb_to_32mb_count	Long	Numero di oggetti con dimensioni superiori a 16 MB e inferiori o uguali a 32 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_32mb_to_64mb_count	Long	Numero di oggetti con dimensioni superiori a 32 MB e inferiori o uguali a 64 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_64mb_to_128mb_count	Long	Numero di oggetti con dimensioni superiori a 64 MB e inferiori o uguali a 128 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_128mb_to_256mb_count	Long	Numero di oggetti con dimensioni superiori a 128 MB e inferiori o uguali a 256 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_256mb_to_512mb_count	Long	Numero di oggetti con dimensioni superiori a 256 MB e inferiori o uguali a 512 MB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione

Nome	Tipo	Description
object_512mb_to_1gb_count	Long	Numero di oggetti con dimensioni superiori a 512 MB e inferiori o uguali a 1 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_1gb_to_2gb_count	Long	Numero di oggetti con dimensioni superiori a 1 GB e inferiori o uguali a 2 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_2gb_to_4gb_count	Long	Numero di oggetti con dimensioni superiori a 2 GB e inferiori o uguali a 4 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione
object_larger_than_4gb_count	Long	Numero di oggetti con dimensioni superiori a 4 GB, inclusa la versione corrente, le versioni non correnti, i caricamenti multiparte incompleti e gli indicatori di eliminazione

Schema della tabella delle metriche delle proprietà del bucket

Nome	Tipo	Description
version_number	stringa	Identificatore di versione dello schema della tabella
configuration_id	stringa	Nome di configurazione S3 Storage Lens
report_time	timestamp	Data a cui si riferisce il rapporto S3 Storage Lens
aws_account_id	stringa	ID account a cui si riferisce la voce
record_type	stringa	Tipo di record, correlato al livello di aggregazione dei dati. Valori: ACCOUNT, BUCKET, PREFIXSTORAGE_L

Nome	Tipo	Description
		ENS_GROUP_BUCKET ,STORAGE_LENS_GROUP_ACCOUNT .
record_value	stringa	Disambiguatore per i tipi di record che contengono più di un record. Viene utilizzato per fare riferimento al prefisso.
aws_region	stringa	Region
storage_class	stringa	Classe di storage
bucket_name	stringa	Nome bucket
versioning_enabled_bucket_count	Long	Numero di bucket con controllo delle versioni abilitato per l'elemento di riferimento corrente
mfa_delete_enabled_bucket_count	Long	Numero di bucket con eliminazione MFA abilitata per l'elemento di riferimento corrente
sse_kms_enabled_bucket_count	Long	Numero di bucket con KMS abilitato per l'elemento di riferimento corrente
object_ownership_bucket_owner_enforced_bucket_count	Long	Numero di bucket con proprietario del bucket Object Ownership applicato all'elemento di riferimento corrente
object_ownership_bucket_owner_preferred_bucket_count	Long	Numero di bucket con il proprietario del bucket Object Ownership preferito per l'elemento di riferimento corrente

Nome	Tipo	Description
object_ownership_object_writer_bucket_count	Long	Numero di bucket con autore di oggetti Object Ownership per l'elemento di riferimento corrente
transfer_acceleration_enabled_bucket_count	Long	Numero di bucket con accelerazione di trasferimento abilitata per l'elemento di riferimento corrente
event_notification_enabled_bucket_count	Long	Numero di bucket con notifica degli eventi abilitata per l'elemento di riferimento corrente
transition_lifecycle_rule_count	Long	Numero di regole del ciclo di vita di transizione per l'elemento di riferimento corrente
expiration_lifecycle_rule_count	Long	Numero di regole del ciclo di vita di scadenza per l'articolo di riferimento corrente
non_current_version_transition_lifecycle_rule_count	Long	Numero di regole del ciclo di vita della transizione di versione non correnti per l'articolo di riferimento corrente

Nome	Tipo	Description
non_current_version_expiration_lifecycle_rule_count	Long	Numero di regole del ciclo di vita di scadenza della versione non corrente per l'elemento di riferimento corrente
abort_incomplete_multipart_upload_lifecycle_rule_count	Long	Numero di regole del ciclo di vita del caricamento multipart non completo per l'elemento di riferimento corrente
expired_object_delete_marker_lifecycle_rule_count	Long	Numero di regole del ciclo di vita degli indicatori di eliminazione degli oggetti in scadenza per l'elemento di riferimento corrente
same_region_replication_rule_count	Long	Numero di regole di Same-Region replica per l'elemento di riferimento corrente
cross_region_replication_rule_count	Long	Numero di regole di Cross-Region replica per l'elemento di riferimento corrente
same_account_replication_rule_count	Long	Numero di regole di replica per lo stesso account per l'elemento di riferimento corrente

Nome	Tipo	Description
cross_account_replication_rule_count	Long	Numero di regole di replica tra account per l'elemento di riferimento corrente
invalid_destination_replication_rule_count	Long	Numero di bucket con replica di destinazione non valida per l'elemento di riferimento corrente

Schema della tabella delle metriche delle attività

Nome	Tipo	Description
version_number	stringa	Identificatore della versione dello schema della tabella
configuration_id	stringa	Nome di configurazione S3 Storage Lens
report_time	timestampz	Data a cui si riferisce il rapporto S3 Storage Lens
aws_account_id	stringa	ID account a cui si riferisce la voce
aws_region	stringa	Region
storage_class	stringa	Classe di storage
record_type	stringa	Tipo di record, correlato al livello di aggregazione dei dati. Valori: ACCOUNT, BUCKET, PREFIX, STORAGE_LENS_GROUP_BUCKET, STORAGE_LENS_GROUP_ACCOUNT.
record_value	stringa	Disambiguatore per i tipi di record che contengono più di un record. Viene utilizzato per fare riferimento al prefisso

Nome	Tipo	Description
bucket_name	stringa	Nome bucket
all_request_count	Long	Numero di tutte le richieste per l'articolo a cui si fa riferimento attualmente
all_sse_kms_encrypted_request_count	Long	Numero di richieste crittografate KMS per l'elemento di riferimento corrente
all_unsupported_signature_request_count	Long	Numero di richieste di firma non supportate per l'elemento di riferimento corrente
all_unsupported_tls_request_count	Long	Numero di richieste TLS non supportate per l'elemento di riferimento corrente
bad_request_error_400_count	Long	Numero di 400 errori di richiesta errata per l'elemento di riferimento corrente
delete_request_count	Long	Numero di richieste di eliminazione per l'elemento attualmente referenziato
downloaded_bytes	decimale (38,0)	Numero di byte scaricati per l'elemento di riferimento corrente
error_4xx_count	Long	Numero di errori 4xx per l'elemento di riferimento corrente
error_5xx_count	Long	Numero di errori 5xx per l'elemento di riferimento corrente
forbidden_error_403_count	Long	Numero di 403 errori proibiti per l'articolo a cui si fa riferimento attualmente

Nome	Tipo	Description
get_reque st_count	Long	Numero di richieste get per l'articolo a cui si fa riferimento attualmente
head_requ est_count	Long	Numero di richieste principali per l'articolo a cui si fa riferimento attualmente
internal_ server_er ror_500_count	Long	Numero di 500 errori interni del server per l'elemento di riferimento corrente
list_requ est_count	Long	Numero di richieste di elenco per l'elemento attualmente referenziato
not_found _error_40 4_count	Long	Numero di 404 errori non trovati per l'elemento di riferimento corrente
ok_status _200_count	Long	Numero di 200 richieste OK per l'elemento di riferimento corrente
partial_c ontent_st atus_206_count	Long	Numero di 206 richieste di contenuto parziale per l'elemento di riferimento corrente
post_requ est_count	Long	Numero di richieste di post per l'elemento a cui si fa riferimento attualmente
put_reque st_count	Long	Numero di richieste put per l'articolo a cui si fa riferimento attualmente
select_re quest_count	Long	Numero di richieste di selezione per l'articolo a cui si fa riferimento attualmente
select_re turned_bytes	decimale (38,0)	Numero di byte restituiti dalle richieste di selezione per l'elemento di riferimento corrente

Nome	Tipo	Description
select_scanned_bytes	decimale (38,0)	Numero di byte scansionati da richieste selezionate per l'elemento di riferimento corrente
service_unavailable_error_503_count	Long	Numero di 503 errori di servizio non disponibili per l'elemento di riferimento corrente
uploaded_bytes	decimale (38,0)	Numero di byte caricati per l'elemento di riferimento corrente
average_first_byte_latency	Long	Tempo medio per richiesta che intercorre tra il momento in cui un bucket S3 riceve una richiesta completa e il momento in cui inizia a restituire la risposta, misurato nelle ultime 24 ore
average_total_request_latency	Long	Tempo medio trascorso per richiesta tra il primo byte ricevuto e l'ultimo byte inviato a un bucket S3, misurato nelle ultime 24 ore
read_0kb_request_count	Long	Numero di GetObject richieste con dimensioni di dati di 0 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_0kb_to_128kb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 0 KB e fino a 128 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_128kb_to_256kb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 128 KB e fino a 256 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto

Nome	Tipo	Description
read_256k_b_to_512k_b_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 256 KB e fino a 512 KB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_512k_b_to_1mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 512 KB e fino a 1 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_1mb_to_2mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 1 MB e fino a 2 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_2mb_to_4mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 2 MB e fino a 4 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_4mb_to_8mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 4 MB e fino a 8 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_8mb_to_16mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 8 MB e fino a 16 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_16mb_to_32mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 16 MB e fino a 32 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_32mb_to_64mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 32 MB e fino a 64 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
read_64mb_to_128mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 64 MB e fino a 128 MB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto

Nome	Tipo	Description
read_128mb_to_256mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 128 MB e fino a 256 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_256mb_to_512mb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 256 MB e fino a 512 MB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_512mb_to_1gb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 512 MB e fino a 1 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_1gb_to_2gb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 1 GB e fino a 2 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_2gb_to_4gb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 2 GB e fino a 4 GB, incluse le richieste basate sull'intervallo e le richieste relative all'intero oggetto
read_larger_than_4gb_request_count	Long	Numero di GetObject richieste con dimensioni dei dati superiori a 4 GB, incluse le richieste basate su intervalli e le richieste relative all'intero oggetto
write_0kb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati di 0 KB
write_0kb_to_128kb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 0 KB e fino a 128 KB

Nome	Tipo	Description
write_128 kb_to_256 kb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 128 KB e fino a 256 KB
write_256 kb_to_512 kb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 256 KB e fino a 512 KB
write_512 kb_to_1mb _request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 512 KB e fino a 1 MB
write_1mb _to_2mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 1 MB e fino a 2 MB
write_2mb _to_4mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 2 MB e fino a 4 MB
write_4mb _to_8mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 4 MB e fino a 8 MB
write_8mb _to_16mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 8 MB e fino a 16 MB
write_16mb _to_32mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 16 MB e fino a 32 MB

Nome	Tipo	Description
write_32mb_to_64mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 32 MB e fino a 64 MB
write_64mb_to_128mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 64 MB e fino a 128 MB
write_128mb_to_256mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 128 MB e fino a 256 MB
write_256mb_to_512mb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 256 MB e fino a 512 MB
write_512mb_to_1gb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 512 MB e fino a 1 GB
write_1gb_to_2gb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 1 GB e fino a 2 GB
write_2gb_to_4gb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 2 GB e fino a 4 GB
write_larger_than_4gb_request_count	Long	Numero di PutObject UploadPart, e CreateMultipartUpload richieste con dimensioni dei dati superiori a 4 GB

Nome	Tipo	Description
concurrent_put_503_error_count	Long	Numero di 503 errori generati a causa di scritture simultanee sullo stesso oggetto
cross_region_request_count	Long	Numero di richieste che provengono da un client in una regione diversa da quella di origine del bucket
cross_region_transferred_bytes	decimale (38,0)	Numero di byte trasferiti da chiamate in una regione diversa da quella di origine del bucket
cross_region_without_replication_request_count	Long	Numero di richieste provenienti da un client in una regione diversa da quella di origine del bucket, escluse le richieste di replica tra regioni
cross_region_without_replication_transferred_bytes	decimale (38,0)	Numero di byte trasferiti da chiamate in una regione diversa da quella di origine del bucket, esclusi i byte di replica tra regioni
inregion_request_count	Long	Numero di richieste provenienti da un cliente nella stessa regione della regione di origine del bucket
inregion_transferred_bytes	decimale (38,0)	Numero di byte trasferiti dalle chiamate dalla stessa regione della regione di origine del bucket
unique_objects_accessed_daily_count	Long	Numero di oggetti a cui è stato effettuato l'accesso almeno una volta nelle ultime 24 ore

Fasi successive

- Ulteriori informazioni su [Autorizzazioni per le tabelle S3 Storage Lens](#)
- Avvia [Interrogazione dei dati di S3 Storage Lens con strumenti di analisi](#)
- Consulta il [Glossario dei parametri di Amazon S3 Storage Lens](#) per le definizioni dettagliate delle metriche

Autorizzazioni per le tabelle S3 Storage Lens

Per lavorare con i dati S3 Storage Lens esportati in tabelle S3, sono necessarie le autorizzazioni (IAM) appropriate. AWS Identity and Access Management Questo argomento descrive le autorizzazioni necessarie per l'esportazione delle metriche e la gestione della crittografia.

Autorizzazioni per l'esportazione delle metriche nelle tabelle S3

Per creare e lavorare con tabelle e bucket di tabelle S3 Storage Lens, è necessario disporre di determinate autorizzazioni. `s3tables` Come minimo, per configurare S3 Storage Lens su S3 Tables, devi disporre delle seguenti autorizzazioni: `s3tables`

- `s3tables:CreateTableBucket`— Questa autorizzazione consente di creare un AWS bucket di tabelle gestito. Tutte le metriche di S3 Storage Lens nel tuo account sono archiviate in un unico AWS bucket di tabella gestito denominato. `aws-s3`
- `s3tables:PutTableBucketPolicy`— S3 Storage Lens utilizza questa autorizzazione per impostare una policy di table bucket che consenta `systemtables.s3.amazonaws.com` l'accesso al bucket in modo da poter inviare i log.

Important

Se rimuovi le autorizzazioni per l'entità del servizio `systemtables.s3.amazonaws.com`, S3 Storage Lens non sarà in grado di aggiornare le tabelle S3 con i dati in base alla tua configurazione. Ti consigliamo di aggiungere altre politiche di controllo degli accessi oltre alla policy già fornita, invece di modificare la policy predefinita che viene aggiunta quando il bucket della tabella è impostato.

 Note

Per ogni configurazione di Storage Lens viene creata una tabella S3 separata per ogni tipo di esportazione delle metriche. Se nella regione sono presenti più configurazioni di Storage Lens, vengono create tabelle separate per configurazioni aggiuntive. Ad esempio, sono disponibili tre tipi di tabelle per il bucket da tavolo S3.

Autorizzazioni per AWS Tabelle crittografate KMS

Tutti i dati nelle tabelle S3, incluse le metriche di S3 Storage Lens, sono crittografati con crittografia per impostazione predefinita. SSE-S3 Puoi scegliere di crittografare il rapporto sulle metriche di Storage Lens con le chiavi (). AWS KMS SSE-KMS Se scegli di crittografare i report metrici di S3 Storage Lens con chiavi KMS, devi disporre di autorizzazioni aggiuntive.

1. L'utente o il ruolo IAM necessita delle seguenti autorizzazioni. Puoi concedere queste autorizzazioni utilizzando la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>
 - kms:DescribeKeysulla AWS KMS chiave utilizzata
2. Per quanto riguarda la politica chiave per la AWS KMS chiave, sono necessarie le seguenti autorizzazioni. Puoi concedere queste autorizzazioni utilizzando la AWS KMS console all'indirizzo. <https://console.aws.amazon.com/kms/> Per utilizzare questa policy, sostituisci *user input placeholders* con le tue informazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnableSystemTablesKeyUsage",
      "Effect": "Allow",
      "Principal": {
        "Service": "systemtables.s3.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
      "Condition": {
        "StringEquals": {
```

```

        "aws:SourceAccount": "111122223333"
    }
}
},
{
    "Sid": "EnableKeyUsage",
    "Effect": "Allow",
    "Principal": {
        "Service": "maintenance.s3tables.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "<table-bucket-arn>/*"
        }
    }
}
]
}

```

Service-linked ruolo per S3 Storage Lens

S3 Storage Lens utilizza un ruolo collegato ai servizi per scrivere metriche su S3 Tables. Questo ruolo viene creato automaticamente quando abiliti l'esportazione di tabelle S3 per la prima volta nel tuo account. Il ruolo collegato al servizio dispone delle seguenti autorizzazioni:

- `s3tables:CreateTable`- Per creare tabelle nel bucket delle tabelle `aws-s3`
- `s3tables:PutTableData`- Scrivere i dati delle metriche nelle tabelle
- `s3tables:GetTable`- Per recuperare i metadati delle tabelle

Non è necessario creare o gestire manualmente questo ruolo collegato al servizio. Per ulteriori informazioni sui ruoli collegati al servizio, consulta [Utilizzo dei ruoli collegati al servizio](#) nella Guida per l'utente IAM.

Procedure consigliate per le autorizzazioni

Segui queste best practice per configurare le autorizzazioni per le tabelle S3 Storage Lens:

- Usa il privilegio minimo: concedi solo le autorizzazioni richieste per attività specifiche. Ad esempio, se gli utenti devono solo interrogare i dati, non concedere le autorizzazioni per modificare le configurazioni di Storage Lens.
- Usa i ruoli IAM: utilizza i ruoli IAM anziché le chiavi di accesso a lungo termine per le applicazioni e i servizi che accedono alle tabelle S3 Storage Lens.
- Abilita AWS CloudTrail: abilita la CloudTrail registrazione per monitorare l'accesso alle tabelle S3 Storage Lens e tenere traccia delle modifiche alle autorizzazioni.
- Utilizza politiche basate sulle risorse: quando possibile, utilizza politiche basate sulle risorse per controllare l'accesso a tabelle o namespace specifici.
- Rivedi regolarmente le autorizzazioni: rivedi e verifica periodicamente le politiche IAM e le autorizzazioni di Lake Formation per assicurarti che rispettino il principio del privilegio minimo.

Risoluzione dei problemi relativi alle autorizzazioni

Accesso negato quando si abilita l'esportazione di tabelle S3

Problema: viene visualizzato un errore di «accesso negato» quando si tenta di abilitare l'esportazione di tabelle S3.

Soluzione: verifica che il tuo utente o ruolo IAM disponga dell'`s3:PutStorageLensConfiguration` autorizzazione e delle autorizzazioni S3 Tables necessarie.

Accesso negato durante l'interrogazione delle tabelle

Problema: ricevi un errore di «accesso negato» quando esegui una query sulle tabelle S3 Storage Lens in Amazon Athena.

Soluzione: verifica che:

- L'integrazione di Analytics è abilitata nel aws-s3 bucket della tabella
- Le autorizzazioni di Lake Formation sono configurate correttamente
- Il tuo utente o ruolo IAM dispone delle autorizzazioni Amazon Athena necessarie

Errori di crittografia KMS

Problema: si KMS-related verificano errori quando si accede alle tabelle crittografate.

Soluzione: verifica che:

- La tua policy IAM include le autorizzazioni KMS richieste
- La policy chiave KMS concede le autorizzazioni al responsabile del servizio S3 Storage Lens
- La chiave KMS si trova nella stessa regione della configurazione di Storage Lens

Fasi successive

- Ulteriori informazioni su [Impostazione delle autorizzazioni di Amazon S3 Storage Lens](#)
- Ulteriori informazioni su [Interrogazione dei dati di S3 Storage Lens con strumenti di analisi](#)
- Ulteriori informazioni su [Utilizzo degli assistenti AI con le tabelle S3 Storage Lens](#)

Interrogazione dei dati di S3 Storage Lens con strumenti di analisi

Prima di poter interrogare i dati di S3 Storage Lens esportati in S3 Tables utilizzando servizi di AWS analisi come Amazon Athena o Amazon EMR, devi abilitare l'integrazione delle analisi nel bucket di tabelle AWS`aws-s3` gestito e configurare le autorizzazioni. AWS Lake Formation

Important

Abilitare l'integrazione delle analisi nel bucket da tabella «aws-s3" è un passaggio obbligatorio che spesso viene ignorato. Senza questa configurazione, non sarà possibile interrogare le tabelle S3 Storage Lens utilizzando i servizi di analisi. AWS

Prerequisiti

Prima di iniziare, assicurati di avere:

- Una configurazione S3 Storage Lens con esportazione S3 Tables abilitata. Per ulteriori informazioni, consulta [Esportazione delle metriche di S3 Storage Lens in tabelle S3](#).
- Accesso ad Amazon Athena o a un altro servizio di analisi.
- Sono state attese 24-48 ore dopo aver abilitato l'esportazione prima che i primi dati fossero disponibili.

Panoramica dell'integrazione

Per informazioni dettagliate sull'integrazione di S3 Tables con i servizi di AWS analisi, inclusi i prerequisiti, la configurazione del ruolo IAM e le procedure dettagliate, consulta [Integrazione di Amazon S3 Tables con i servizi di analisi. AWS](#)

Dopo aver abilitato l'esportazione di S3 Tables e configurato l'integrazione delle analisi, puoi interrogare i dati di S3 Storage Lens utilizzando servizi di AWS analisi come Amazon Athena, Amazon Redshift e Amazon EMR. Ciò consente di eseguire analisi personalizzate, creare dashboard e ricavare informazioni dettagliate dai dati di storage utilizzando SQL standard.

Interrogazione con Amazon Athena

Amazon Athena è un servizio di query interattivo senza server che semplifica l'analisi dei dati utilizzando SQL standard. Utilizza i seguenti passaggi per interrogare i dati di S3 Storage Lens in Athena.

Note

In tutti gli esempi di query, sostituisci `lens_my-config_exp` con il tuo namespace di configurazione Storage Lens effettivo. Per ulteriori informazioni sulla denominazione dei namespace, vedere [Denominazione della tabella per l'esportazione di S3 Storage Lens in tabelle S3](#)

Esempio: interroga i principali utenti di storage

La seguente query identifica i 10 bucket principali in base al consumo di spazio di archiviazione:

```
SELECT
    bucket_name,
    storage_class,
    SUM(storage_bytes) / POWER(1024, 3) AS storage_gb,
    SUM(object_count) AS objects
FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."default_storage_metrics"
WHERE report_time = (
    SELECT MAX(report_time)
    FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."default_storage_metrics"
)
AND record_type = 'BUCKET'
AND bucket_name != ''
```

```
GROUP BY bucket_name, storage_class
ORDER BY storage_gb DESC
LIMIT 10
```

Esempio: analizza la crescita dello storage nel tempo

La seguente query analizza la crescita dello storage negli ultimi 30 giorni:

```
SELECT
    CAST(report_time AS date) AS report_date,
    SUM(storage_bytes) / POWER(1024, 3) AS total_storage_gb
FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."default_storage_metrics"
WHERE report_time >= current_date - interval '30' day
    AND record_type = 'ACCOUNT'
GROUP BY CAST(report_time AS date)
ORDER BY report_date DESC;
```

Esempio: Identifica i caricamenti multipart incompleti

La seguente query trova i bucket con caricamenti multipart incompleti più vecchi di 7 giorni:

```
SELECT
    bucket_name,
    SUM(incomplete_mpu_storage_older_than_7_days_bytes) / POWER(1024, 3) AS
wasted_storage_gb,
    SUM(incomplete_mpu_object_older_than_7_days_count) AS wasted_objects
FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."default_storage_metrics"
WHERE report_time = (
    SELECT MAX(report_time)
    FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."default_storage_metrics"
)
    AND record_type = 'BUCKET'
    AND incomplete_mpu_storage_older_than_7_days_bytes > 0
GROUP BY bucket_name
ORDER BY wasted_storage_gb DESC;
```

Esempio: trova candidati con dati incompleti

La seguente query identifica i prefissi senza attività negli ultimi 100 giorni che sono stati archiviati in livelli di archiviazione a caldo:

```
WITH recent_activity AS (
    SELECT DISTINCT
```

```

        bucket_name,
        record_value AS prefix_path
    FROM "s3tablescatalog/aws-s3"."lens_my-
config_exp"."expanded_prefixes_activity_metrics"
    WHERE report_time >= current_date - interval '100' day
        AND record_type = 'PREFIX'
        AND all_request_count > 0
)
SELECT
    s.bucket_name,
    s.record_value AS prefix_path,
    s.storage_class,
    SUM(s.storage_bytes) / POWER(1024, 3) AS storage_gb
FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."expanded_prefixes_storage_metrics"
s
LEFT JOIN recent_activity r
    ON s.bucket_name = r.bucket_name
    AND s.record_value = r.prefix_path
WHERE s.report_time = (
    SELECT MAX(report_time)
    FROM "s3tablescatalog/aws-s3"."lens_my-
config_exp"."expanded_prefixes_storage_metrics"
)
    AND s.record_type = 'PREFIX'
    AND s.storage_class IN ('STANDARD', 'REDUCED_REDUNDANCY')
    AND s.storage_bytes > 1073741824 -- > 1GB
    AND r.prefix_path IS NULL -- No recent activity
GROUP BY s.bucket_name, s.record_value, s.storage_class
ORDER BY storage_gb DESC
LIMIT 20;

```

Esempio: analizza i modelli di richiesta

La seguente query analizza i modelli di richiesta per comprendere la frequenza di accesso:

```

SELECT
    bucket_name,
    SUM(all_request_count) AS total_requests,
    SUM(get_request_count) AS get_requests,
    SUM(put_request_count) AS put_requests,
    ROUND(100.0 * SUM(get_request_count) / NULLIF(SUM(all_request_count), 0), 2) AS
get_percentage,
    SUM(downloaded_bytes) / POWER(1024, 3) AS downloaded_gb
FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."default_activity_metrics"

```

```
WHERE report_time >= current_date - interval '7' day
      AND record_type = 'BUCKET'
      AND bucket_name != ''
GROUP BY bucket_name
HAVING SUM(all_request_count) > 0
ORDER BY total_requests DESC
LIMIT 10;
```

Interrogazione con Apache Spark su Amazon EMR

Amazon EMR fornisce un framework Hadoop gestito che semplifica l'elaborazione di grandi quantità di dati utilizzando Apache Spark. Puoi utilizzare il connettore Iceberg per leggere direttamente le tabelle di S3 Storage Lens.

Leggi le tabelle S3 con Spark

Usa il seguente codice Python per leggere i dati di S3 Storage Lens con Spark:

```
from pyspark.sql import SparkSession

spark = SparkSession.builder \
    .appName("S3StorageLensAnalysis") \
    .config("spark.sql.catalog.s3tablescatalog",
"org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablescatalog.catalog-impl",
"org.apache.iceberg.aws.glue.GlueCatalog") \
    .getOrCreate()

# Read S3 Storage Lens data
df = spark.read \
    .format("iceberg") \
    .load("s3tablescatalog/aws-s3.lens_my-config_exp.default_storage_metrics")

# Analyze data
df.filter("record_type = 'BUCKET'") \
    .groupBy("bucket_name", "storage_class") \
    .sum("storage_bytes") \
    .orderBy("sum(storage_bytes)", ascending=False) \
    .show(10)
```

Le migliori pratiche per l'ottimizzazione delle query

Segui queste best practice per ottimizzare le prestazioni delle query e ridurre i costi:

- Filtra per `report_time`: includi sempre filtri di data per ridurre la quantità di dati scansionati. Ciò è particolarmente importante per le tabelle con lunghi periodi di conservazione.

```
WHERE report_time >= current_date - interval '7' day
```

- Usa i filtri `record_type`: specifica il livello di aggregazione appropriato (ACCOUNT, BUCKET, PREFIX) per interrogare solo i dati di cui hai bisogno.

```
WHERE record_type = 'BUCKET'
```

- Includi clausole `LIMIT`: utilizza `LIMIT` per le query esplorative per controllare la dimensione dei risultati e ridurre i costi delle query.

```
LIMIT 100
```

- Filtra i record vuoti: utilizza le condizioni per escludere i record vuoti o con valore zero.

```
WHERE storage_bytes > 0
```

- Usa i dati più recenti: quando analizzi lo stato corrente, filtra in base al rapporto `report_time` più recente per evitare la scansione dei dati storici.

```
WHERE report_time = (SELECT MAX(report_time) FROM table_name)
```

Esempio di modello di interrogazione ottimizzato

La seguente query illustra le migliori pratiche per l'ottimizzazione:

```
SELECT
    bucket_name,
    SUM(storage_bytes) / POWER(1024, 3) AS storage_gb
FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."default_storage_metrics"
WHERE report_time >= current_date - interval '7' day -- Date filter
    AND record_type = 'BUCKET' -- Record type filter
    AND storage_bytes > 0 -- Non-empty filter
    AND bucket_name != '' -- Non-empty filter
GROUP BY bucket_name
ORDER BY storage_gb DESC
LIMIT 100; -- Result limit
```

Risoluzione dei problemi

La query non restituisce risultati

Problema: la query viene completata correttamente ma non restituisce risultati.

Soluzione::

- Verifica che i dati siano disponibili controllando l'ultima versione di `report_time`:

```
SELECT MAX(report_time) AS latest_data
FROM "s3tablescatalog/aws-s3"."lens_my-config_exp"."default_storage_metrics";
```

- Assicurati di utilizzare il nome corretto dello spazio dei nomi. Usalo `SHOW TABLES IN `lens_my-config_exp`` ; per elencare le tabelle disponibili.
- Attendi 24-48 ore dopo aver abilitato l'esportazione delle tabelle S3 affinché i primi dati siano disponibili.

Errori di accesso negato

Problema: ricevi errori di accesso negato durante l'esecuzione delle query.

Soluzione: verifica che AWS Lake Formation le autorizzazioni siano configurate correttamente. Per ulteriori informazioni, consulta [Integrazione delle tabelle Amazon S3 con AWS i servizi di analisi](#).

Fasi successive

- Ulteriori informazioni su [Utilizzo degli assistenti AI con le tabelle S3 Storage Lens](#)
- Consulta le quattro definizioni delle [Glossario dei parametri di Amazon S3 Storage Lens](#) metriche
- Esplora [Casi d'uso relativi ai parametri di Amazon S3 Storage Lens](#) per ulteriori idee di analisi
- Scopri [Amazon Athena](#) per le interrogazioni senza server

Utilizzo degli assistenti AI con le tabelle S3 Storage Lens

Puoi utilizzare assistenti AI e strumenti di intelligenza artificiale conversazionale per interagire con i dati di S3 Storage Lens esportati in tabelle S3 utilizzando il linguaggio naturale. Sfruttando il Model Context Protocol (MCP) e il server MCP per Amazon S3 Tables, puoi interrogare, analizzare e ottenere informazioni dettagliate dai tuoi dati di storage senza scrivere query SQL.

Panoramica di

Il Model Context Protocol (MCP) è un modo standardizzato per le applicazioni di intelligenza artificiale di accedere e utilizzare le informazioni contestuali. Il server MCP per Amazon S3 Tables fornisce strumenti che consentono agli assistenti AI di interagire con i dati di S3 Tables utilizzando interfacce in linguaggio naturale. Ciò democratizza l'accesso ai dati e consente alle persone con qualsiasi livello di competenza tecnica di lavorare con le metriche di S3 Storage Lens.

Con il server MCP per tabelle S3, puoi utilizzare il linguaggio naturale per:

- Elenca i bucket, i namespace e le tabelle S3
- Interroga le metriche di S3 Storage Lens e ottieni informazioni
- Analizza le tendenze e i modelli di storage
- Identifica le opportunità di ottimizzazione dei costi
- Genera report e visualizzazioni

Assistenti AI supportati

Il server MCP per tabelle S3 funziona con vari assistenti AI che supportano il Model Context Protocol, tra cui:

- Kiro: un assistente di codifica AI con supporto MCP integrato
- Amazon Q Developer: AWS assistente per AI-powered sviluppatori
- Cline - Un assistente di codifica AI con integrazione MCP
- Claude Desktop - Applicazione desktop di Anthropic con supporto MCP
- Cursor - Un editor di codice AI-powered

Important

AI-generated Le domande e i consigli SQL devono essere esaminati e convalidati prima dell'uso. Verifica che le query siano appropriate per la struttura dei dati, il caso d'uso e i requisiti prestazionali. Verifica sempre i consigli in un ambiente non di produzione prima di implementarli in produzione.

Configurare Kiro con le tabelle S3 Storage Lens

Kiro è un assistente di codifica AI che fornisce una perfetta integrazione con le tabelle S3 tramite il server MCP. Kiro può aiutarti a installare e configurare il server MCP direttamente tramite la sua interfaccia, semplificando il processo di configurazione.

Per ulteriori informazioni su Kiro, consulta Kiro AI. <https://kiro.ai/>

Prerequisiti

Prima di iniziare, assicurati di avere:

- Kiro è installato sul tuo sistema. Scarica da <https://kiro.ai/>
- AWS CLI configurato con le credenziali appropriate
- Una configurazione S3 Storage Lens con esportazione S3 Tables abilitata
- Autorizzazioni per interrogare le tabelle S3. Per ulteriori informazioni, consulta [Autorizzazioni per le tabelle S3 Storage Lens](#).

Passaggio 1: installare il server MCP S3 Tables

È possibile installare il server MCP S3 Tables in due modi:

Opzione 1: utilizzo della gestione del server MCP integrata di Kiro

Kiro può aiutarti a scoprire e installare i server MCP direttamente tramite la sua interfaccia:

1. Apri Kiro
2. Accedi all'interfaccia di gestione del server MCP (in genere tramite le impostazioni o la palette di comandi)
3. Cerca «S3 Tables» o «awslabs.s3-tables-mcp-server»
4. Segui le istruzioni di Kiro per installare e configurare il server

Opzione 2: installazione manuale tramite uvx

In alternativa, è possibile installare manualmente il server MCP utilizzando uvx un gestore di pacchetti Python:

```
uvx awslabs.s3-tables-mcp-server@latest
```

Per ulteriori informazioni sull'installazione del server MCP, consulta la documentazione del server MCP di [AWS S3 Tables](#).

Fase 2: Configurare le impostazioni MCP di Kiro

Crea o aggiorna il tuo file di configurazione Kiro MCP `~/.kiro/settings/mcp.json` con il seguente contenuto:

```
{
  "mcpServers": {
    "awslabs.s3-tables-mcp-server": {
      "command": "uvx",
      "args": ["awslabs.s3-tables-mcp-server@latest"],
      "env": {
        "AWS_PROFILE": "your-aws-profile",
        "AWS_REGION": "us-east-1"
      }
    }
  }
}
```

Sostituiscilo `your-aws-profile` con il nome AWS CLI del tuo profilo e `us-east-1` con la tua AWS regione.

Fase 3: Verifica la configurazione

Dopo aver configurato il server MCP, riavvia Kiro e verifica che gli strumenti di S3 Tables siano disponibili. Puoi controllare i server MCP disponibili nelle impostazioni di Kiro o chiedendo a Kiro di elencare gli strumenti disponibili.

Esempi di casi d'uso con assistenti AI

Gli esempi seguenti dimostrano come utilizzare i prompt in linguaggio naturale con gli assistenti AI per interagire con i dati di S3 Storage Lens.

Esempio 1: interroga i principali utenti di storage

Prompt: «Mostrami i 10 bucket principali in base al consumo di spazio di archiviazione dei dati del mio S3 Storage Lens».

L'assistente AI utilizzerà il server MCP per interrogare le tabelle S3 Storage Lens e restituire i risultati, inclusi i nomi dei bucket, le classi di archiviazione e le quantità di archiviazione.

Esempio 2: analizza la crescita dello storage

Richiesta: «Analizza la crescita dello storage negli ultimi 30 giorni e mostrami la tendenza».

L'assistente AI interrogherà la tabella delle metriche di archiviazione, calolerà i totali di storage giornalieri e presenterà il trend di crescita.

Esempio 3: Identifica le opportunità di ottimizzazione dei costi

Richiesta: «Trova i bucket con caricamenti multiparte incompleti più vecchi di 7 giorni che comportano uno spreco di spazio di archiviazione».

L'assistente AI interrogherà la tabella delle metriche di archiviazione per i caricamenti multiparte incompleti e fornirà un elenco di bucket con potenziali risparmi sui costi.

Esempio 4: Trova i dati disponibili per i cold data

Richiesta: «Identifica i prefissi senza attività negli ultimi 100 giorni che sono stati archiviati in livelli di archiviazione inattivi».

L'assistente AI analizzerà le metriche di archiviazione e di attività per identificare i dati che potrebbero essere spostati su livelli di storage più freddi per l'ottimizzazione dei costi.

Esempio 5: generazione di report di archiviazione

Prompt: «Crea un report riepilogativo del mio storage S3 che mostri lo storage totale, il numero di oggetti e i modelli di richiesta dell'ultima settimana».

L'assistente AI interrogherà più tabelle, aggregherà i dati e genererà un report completo.

Le migliori pratiche per l'utilizzo degli assistenti AI

Segui queste best practice quando utilizzi gli assistenti AI con i dati di S3 Storage Lens:

- Sii specifico nelle istruzioni: fornisci istruzioni chiare e specifiche su quali dati vuoi analizzare e quali approfondimenti stai cercando.
- Verifica AI-generated le query: rivedi e convalida sempre le query e i consigli SQL generati dall'assistente AI prima di eseguirli o agire. Gli assistenti AI possono occasionalmente produrre domande o consigli errati che devono essere verificati in base al caso d'uso e ai dati specifici.
- Utilizza le autorizzazioni appropriate: assicurati che le credenziali IAM utilizzate dall'assistente AI dispongano solo delle autorizzazioni necessarie. Per l'analisi di sola lettura, concedi solo le autorizzazioni SELECT.

- Monitora l'utilizzo: tieni traccia delle query eseguite dagli assistenti AI utilizzando AWS CloudTrail per mantenere gli audit trail.
- Inizia con domande semplici: inizia con domande semplici per capire come l'assistente AI interpreta i tuoi prompt, quindi passa ad analisi più complesse.

Registrazione e tracciabilità

Quando si utilizza il server MCP S3 Tables con assistenti AI, sono disponibili diversi modi per verificare le operazioni:

- Registri locali: il server MCP registra le richieste e le risposte localmente. È possibile specificare una directory di registro utilizzando l'opzione `--log-dir` di configurazione.
- AWS CloudTrail- Tutte le operazioni di S3 Tables tramite l'utilizzo del server MCP Pylceberg avranno `awslabs/mcp/s3-tables-mcp-server/<version>` come stringa user agent. È possibile filtrare CloudTrail i log di questo user agent per tracciare le azioni eseguite dagli assistenti AI.
- Cronologia degli assistenti AI: gli assistenti AI come Kiro e Cline conservano registri cronologici che registrano le richieste in linguaggio naturale, le risposte LLM e le istruzioni fornite al server MCP.

Considerazioni relative alla sicurezza

Quando utilizzi assistenti AI con dati S3 Storage Lens, segui queste best practice di sicurezza:

- Utilizza l'accesso con privilegi minimi: concedi agli assistenti AI solo le autorizzazioni minime richieste per le loro attività.
- Abilita MFA: utilizza l'autenticazione a più fattori per AWS gli account a cui accedono gli assistenti AI.
- Controlla regolarmente le autorizzazioni: verifica periodicamente le autorizzazioni concesse agli assistenti AI e revoca gli accessi non necessari.
- Usa credenziali separate: prendi in considerazione l'utilizzo di AWS credenziali separate per l'accesso agli assistenti AI per facilitare il monitoraggio e il controllo.
- Evita la condivisione di dati sensibili: fai attenzione quando condividi informazioni sensibili nelle richieste agli assistenti AI, soprattutto quando utilizzi servizi di intelligenza artificiale basati su cloud.

Risoluzione dei problemi

L'assistente AI non può connettersi a S3 Tables

Problema: l'assistente AI segnala che non può connettersi a S3 Tables o che il server MCP non risponde.

Soluzione::

- Verificare che il server MCP sia installato correttamente utilizzando `uvx awslabs.s3-tables-mcp-server@latest --version`
- Verifica che le tue AWS credenziali siano configurate correttamente
- Assicuratevi che il file di configurazione MCP abbia il AWS profilo e la regione corretti

Errori di accesso negato

Problema: l'assistente AI riceve errori di accesso negato durante l'interrogazione delle tabelle S3 Storage Lens.

Soluzione::

- Verifica che l'integrazione delle analisi sia abilitata nel bucket della tabella `aws-s3`
- Verifica che le autorizzazioni di Lake Formation siano configurate correttamente
- Assicurati che le AWS credenziali dispongano delle autorizzazioni IAM necessarie

Risultati errati o imprevisti

Problema: l'assistente AI restituisce risultati errati o imprevisti.

Soluzione::

- Esamina la query SQL generata dall'assistente AI
- Verifica di utilizzare il nome dello spazio dei nomi corretto per la configurazione di Storage Lens
- Verifica che i dati siano disponibili richiedendo l'ultima versione di `report_time`
- Perfeziona la richiesta per essere più specifici su ciò che desideri analizzare

Risorse aggiuntive

Per ulteriori informazioni sull'utilizzo degli assistenti AI con S3 Tables, consulta le seguenti risorse:

- [Kiro AI](#) - Assistente di codifica AI con supporto MCP integrato
- [Implementazione dell'IA conversazionale per le tabelle S3 utilizzando il Model Context Protocol \(MCP\) - Storage Blog](#) AWS
- [AWS Documentazione del server MCP di S3 Tables](#)
- [Specifiche del protocollo di contesto del modello](#)

Utilizzo di Amazon S3 Storage Lens con AWS Organizations

Amazon S3 Storage Lens è una funzionalità di analisi del cloud-storage che può essere utilizzata per ottenere visibilità a livello di organizzazione sull'utilizzo e l'attività dell'object-storage. È possibile utilizzare i parametri di S3 Storage Lens per generare approfondimenti, ad esempio per scoprire la quantità di spazio di archiviazione disponibile nell'intera organizzazione o quali sono i bucket e i prefissi caratterizzati da una crescita più rapida. Puoi anche utilizzare Amazon S3 Storage Lens per raccogliere metriche di storage e dati di utilizzo per tutto ciò Account AWS che fa parte della tua gerarchia. AWS Organizations A tale scopo, è necessario utilizzare AWS Organizations e abilitare l'accesso affidabile a S3 Storage Lens utilizzando il proprio account di gestione. AWS Organizations

Dopo aver abilitato l'accesso protetto, aggiungere l'accesso amministratore delegato agli account dell'organizzazione. Gli account di amministratore delegato vengono utilizzati per creare configurazioni e dashboard S3 Storage Lens che raccolgono le metriche di archiviazione e i dati degli utenti a livello di organizzazione. Per maggiori informazioni sull'abilitazione dell'accesso attendibile, consulta [Amazon S3 Storage Lens e AWS Organizations](#) nella Guida per l'utente AWS Organizations

Argomenti

- [Abilitazione dell'accesso attendibile per S3 Storage Lens](#)
- [Disabilitazione dell'accesso attendibile per S3 Storage Lens](#)
- [Registrazione di un amministratore delegato per S3 Storage Lens](#)
- [Annullamento della registrazione di un amministratore delegato per S3 Storage Lens](#)

Abilitazione dell'accesso attendibile per S3 Storage Lens

Abilitando l'accesso affidabile, consenti ad Amazon S3 Storage Lens di accedere alla tua AWS Organizations gerarchia, appartenenza e struttura tramite AWS Organizations operazioni API. S3 Storage Lens diventa in questo modo un servizio attendibile per l'intera struttura dell'organizzazione.

Ogni volta che viene creata una configurazione del pannello di controllo, S3 Storage Lens crea ruoli collegati ai servizi nella gestione o negli account dell'amministratore delegato. Il ruolo collegato al servizio concede a S3 Storage Lens l'autorizzazione a eseguire le seguenti azioni:

- Descrivere le organizzazioni
- Elencare gli account
- Verifica un elenco di Servizio AWS accessi per le organizzazioni
- Ottenere amministratori delegati per le organizzazioni

S3 Storage Lens può quindi garantire l'accesso alla raccolta delle metriche multi-account per gli account dell'organizzazione. Per ulteriori informazioni, consulta la sezione [Utilizzo dei ruoli collegati ai servizi per Amazon S3 Storage Lens](#).

Dopo aver abilitato l'accesso attendibile, potrai assegnare l'accesso da amministratore delegato agli account dell'organizzazione. Quando un account è contrassegnato come amministratore delegato per un servizio, l'account riceve l'autorizzazione ad accedere a tutte le operazioni API dell'organizzazione in sola lettura. Ciò fornisce visibilità di tipo amministratore delegato ai membri e alle strutture dell'organizzazione in modo che possano creare pannelli di controllo di S3 Storage Lens.

Note

- L'accesso attendibile può essere abilitato solo dall'[account di gestione](#).
- Solo l'account di gestione e gli amministratori delegati possono creare pannelli di controllo o configurazioni di S3 Storage Lens per l'organizzazione.

Utilizzo della console S3

Per consentire a S3 Storage Lens di avere AWS Organizations Accesso attendibile

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli le impostazioni di AWS Organizations . Viene visualizzata la pagina AWS Organizations access for Storage Lens.

4. In AWS Organizations Accesso attendibile, scegli Modifica.

Viene visualizzata la pagina di accesso a AWS Organizations .

5. Scegli Abilita per abilitare l'accesso protetto per la dashboard di S3 Storage Lens.

6. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Example

L'esempio seguente mostra come abilitare l'accesso AWS Organizations affidabile per S3 Storage Lens in AWS CLI

```
aws organizations enable-aws-service-access --service-principal storage-  
lens.s3.amazonaws.com
```

Utilizzo di AWS SDK per Java

Example— Abilita AWS Organizations accesso affidabile per S3 Storage Lens tramite SDK per Java

L'esempio seguente mostra come abilitare l'accesso attendibile per S3 Storage Lens in SDK per Java. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import com.amazonaws.auth.profile.ProfileCredentialsProvider;  
import com.amazonaws.regions.Regions;  
import com.amazonaws.services.organizations.AWSOrganizations;  
import com.amazonaws.services.organizations.AWSOrganizationsClient;  
import com.amazonaws.services.organizations.model.EnableAWSServiceAccessRequest;  
  
public class EnableOrganizationsTrustedAccess {  
    private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-  
lens.s3.amazonaws.com";  
  
    public static void main(String[] args) {  
        try {  
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()  
                .withCredentials(new ProfileCredentialsProvider())  
                .withRegion(Regions.US_EAST_1)
```

```
        .build();

        organizationsClient.enableAWSServiceAccess(new
EnableAWSServiceAccessRequest()
        .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but AWS Organizations couldn't
process
        // it and returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // AWS Organizations couldn't be contacted for a response, or the client
        // couldn't parse the response from AWS Organizations.
        e.printStackTrace();
    }
}
```

Disabilitazione dell'accesso attendibile per S3 Storage Lens

La rimozione di un account come amministratore delegato o la disabilitazione dell'accesso attendibile limita le metriche della dashboard S3 Storage Lens del proprietario dell'account al solo livello di account. Ogni titolare di account potrà quindi usufruire dei vantaggi di S3 Storage Lens solo nell'ambito limitato del proprio account, e non dell'intera organizzazione.

Quando si disabilita l'accesso attendibile in S3 Storage Lens, le dashboard che richiedono l'accesso attendibile non vengono più aggiornate. Anche le dashboard organizzative create non vengono più aggiornate. Invece, è possibile interrogare solo i [dati storici per la dashboard S3 Storage Lens](#), finché i dati sono ancora disponibili.

Note

- Inoltre, la disabilitazione dell'accesso attendibile per S3 Storage Lens impedisce automaticamente a tutti i pannelli di controllo a livello di organizzazione di raccogliere e aggregare i parametri di storage. Questo perché S3 Storage Lens non ha più accesso fidato agli account dell'organizzazione.
- Gli account di gestione e di amministratore delegato possono ancora consultare i dati storici di tutte le dashboard disattivate. Possono anche interrogare questi dati storici quando sono ancora disponibili.

Utilizzo della console S3

Per disabilitare l'accesso attendibile per S3 Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli le impostazioni di AWS Organizations . Viene visualizzata la pagina AWS Organizations access for Storage Lens.
4. In AWS Organizations Accesso attendibile, scegli Modifica.

Viene visualizzata la pagina di accesso a AWS Organizations .

5. Scegli Disabilita per disabilitare l'accesso attendibile per la dashboard S3 Storage Lens.
6. Scegli Save changes (Salva modifiche).

Utilizzo di AWS CLI

Example

L'esempio seguente disabilita l'accesso attendibile per S3 Storage Lens utilizzando AWS CLI.

```
aws organizations disable-aws-service-access --service-principal storage-lens.s3.amazonaws.com
```

Utilizzo di AWS SDK per Java

Example— Disabilita AWS Organizations accesso affidabile per S3 Storage Lens

L'esempio seguente mostra come disabilitare l'accesso AWS Organizations affidabile per S3 Storage Lens in SDK for Java. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.DisableAWSServiceAccessRequest;
```

```

public class DisableOrganizationsTrustedAccess {
    private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

    public static void main(String[] args) {
        try {
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            // Make sure to remove any existing delegated administrator for S3 Storage
            Lens
            // before disabling access; otherwise, the request will fail.
            organizationsClient.disableAWSServiceAccess(new
            DisableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
            process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
    }
}

```

Registrazione di un amministratore delegato per S3 Storage Lens

È possibile creare pannelli di controllo a livello di organizzazione utilizzando l'account di gestione dell'organizzazione o un account come amministratore delegato. Gli account amministratore delegati consentono ad altri account oltre all'account di gestione di creare pannelli di controllo a livello di organizzazione. Solo l'account di gestione di un'organizzazione può registrare e annullare la registrazione di altri account come amministratori delegati per l'organizzazione.

Dopo aver abilitato l'accesso affidabile, puoi registrare l'accesso amministratore delegato agli account della tua organizzazione utilizzando l'API AWS Organizations REST o gli SDK dell'account di gestione. AWS CLI <https://docs.aws.amazon.com/managedservices/latest/userguide/management->

[account.html](#) (Per ulteriori informazioni, consulta [RegisterDelegatedAdministrator](#) in AWS Organizations API Reference) Quando un account viene registrato come amministratore delegato, riceve l'autorizzazione ad accedere a tutte le operazioni API di sola lettura AWS Organizations . Ciò fornisce visibilità ai membri e alle strutture dell'organizzazione in modo che possano creare pannelli di controllo di S3 Storage Lens per conto dell'utente.

Note

Prima di poter designare un amministratore delegato utilizzando l'API AWS Organizations REST o gli SDK AWS CLI, è necessario chiamare l'operazione. [EnableAWSServiceAccess](#)

Utilizzo della console S3

Per registrare gli amministratori delegati per S3 Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli le impostazioni di AWS Organizations .
4. In Amministratori delegati, scegli Registra account.
5. Aggiungi un Account AWS ID per registrare l'account come amministratore delegato. L'amministratore delegato è in grado di creare dashboard a livello di organizzazione per tutti gli account e gli archivi dell'organizzazione.
6. Scegli Registra account.

Utilizzo di AWS CLI

Example

L'esempio seguente mostra come registrare gli amministratori delegati delle organizzazioni per S3 Storage Lens tramite AWS CLI. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
aws organizations register-delegated-administrator --service-principal storage-lens.s3.amazonaws.com --account-id 111122223333
```

Utilizzo di AWS SDK per Java

Example- Registrare gli amministratori delegati delle organizzazioni per S3 Storage Lens

L'esempio seguente mostra come registrare gli amministratori AWS Organizations delegati per S3 Storage Lens in SDK for Java. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
    com.amazonaws.services.organizations.model.RegisterDelegatedAdministratorRequest;

public class RegisterOrganizationsDelegatedAdministrator {
    private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

    public static void main(String[] args) {
        try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
delegated administrator.
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.registerDelegatedAdministrator(new
RegisterDelegatedAdministratorRequest()
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
    }
}
```



```
}  
}  
}
```

Annullamento della registrazione di un amministratore delegato per S3 Storage Lens

Dopo aver abilitato l'accesso attendibile, è possibile anche annullare la registrazione dell'accesso dell'amministratore delegato agli account dell'organizzazione. Gli account di amministratore delegato consentono ad altri account, oltre a quello [di gestione](#), di creare dashboard a livello di organizzazione. Solo l'account di gestione di un'organizzazione può annullare la registrazione degli account come amministratori delegati per l'organizzazione.

È possibile annullare la registrazione di un amministratore delegato utilizzando l'API REST o gli AWS Organizations Console di gestione AWS SDK dall'account di gestione AWS CLI. AWS Per ulteriori informazioni, consulta [DeregisterDelegatedAdministrator](#) nella documentazione di riferimento dell'API AWS Organizations .

Quando viene annullata la registrazione di un account come amministratore delegato, tale account perde l'accesso a quanto segue:

- Tutte le operazioni AWS Organizations API di sola lettura che forniscono visibilità ai membri e alle strutture dell'organizzazione.
- Tutte le dashboard a livello di organizzazione create dall'amministratore delegato. Questa azione interrompe automaticamente tutti i pannelli di controllo a livello di organizzazione creati dall'amministratore delegato dall'aggregazione di nuovi parametri di archiviazione.

Note

L'amministratore delegato con registrazione annullata sarà ancora in grado di consultare i dati storici delle dashboard disabilite che ha creato, se i dati sono ancora disponibili per l'esecuzione di query.

Utilizzo della console S3

Per cancellare gli amministratori delegati per S3 Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nel riquadro di navigazione sinistro, spostarsi su Storage Lens.
3. Scegli le impostazioni di AWS Organizations .
4. In Amministratori delegati, scegli l'account che si desidera cancellare.
5. Scegli un De-register account. L'account cancellato non è più un amministratore delegato e non è più in grado di creare dashboard a livello di organizzazione per tutti gli account e gli archivi dell'organizzazione.
6. Scegli Registra account.

Utilizzo di AWS CLI

Example

L'esempio seguente mostra come annullare la registrazione degli amministratori delegati delle organizzazioni per S3 Storage Lens tramite AWS CLI. Per utilizzare questo esempio, sostituisci **111122223333** con il tuo ID Account AWS .

```
aws organizations deregister-delegated-administrator --service-principal storage-lens.s3.amazonaws.com --account-id 111122223333
```

Utilizzo di AWS SDK per Java

Example- Cancellare gli amministratori delegati delle organizzazioni per S3 Storage Lens

L'esempio seguente mostra come annullare la registrazione degli amministratori delegati delle organizzazioni per S3 Storage Lens utilizzando SDK per Java. Per utilizzare questo esempio, sostituisci **user input placeholders** con le informazioni appropriate.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
    com.amazonaws.services.organizations.model.DeregisterDelegatedAdministratorRequest;

public class DeregisterOrganizationsDelegatedAdministrator {
    private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-lens.s3.amazonaws.com";
```

```
public static void main(String[] args) {
    try {
        String delegatedAdminAccountId = "111122223333"; // Account Id for the
        delegated administrator.
        AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
            .withCredentials(new ProfileCredentialsProvider())
            .withRegion(Regions.US_EAST_1)
            .build();

        organizationsClient.deregisterDelegatedAdministrator(new
        DeregisterDelegatedAdministratorRequest()
            .withAccountId(delegatedAdminAccountId)
            .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but AWS Organizations couldn't
        process
        // it and returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // AWS Organizations couldn't be contacted for a response, or the client
        // couldn't parse the response from AWS Organizations.
        e.printStackTrace();
    }
}
```

Operazioni con i gruppi S3 Storage Lens per filtrare e aggregare le metriche

Un gruppo Amazon S3 Storage Lens aggrega i parametri utilizzando filtri personalizzati basati sui metadati degli oggetti. I gruppi Storage Lens ti aiutano ad approfondire le caratteristiche dei tuoi dati, come la distribuzione degli oggetti per età, i tipi di file più comuni e altro ancora. Ad esempio, puoi filtrare le metriche per tag di oggetto per identificare i set di dati in più rapida crescita o visualizzare lo storage in base alla dimensione e all'età degli oggetti per definire la tua strategia di archiviazione dello storage. Di conseguenza, i gruppi Amazon S3 Storage Lens ti aiutano a comprendere e ottimizzare meglio la tua archiviazione S3.

Con i gruppi Storage Lens, puoi analizzare e filtrare i parametri di S3 Storage Lens utilizzando metadati degli oggetti come prefissi, suffissi, [tag degli oggetti](#), dimensioni o età degli oggetti. Puoi anche applicare una combinazione di questi filtri. Dopo aver collegato il gruppo Storage Lens al pannello di controllo di S3 Storage Lens, puoi visualizzare i parametri S3 Storage Lens aggregati in base ai gruppi Amazon S3 Storage Lens direttamente nel pannello di controllo.

Ad esempio, è anche possibile filtrare i parametri per dimensione degli oggetti o fasce di età per determinare quale parte dell'archiviazione è costituita da oggetti di piccole dimensioni. È quindi possibile utilizzare queste informazioni con S3 Intelligent-Tiering o S3 Lifecycle per trasferire piccoli oggetti a diverse classi di storage per l'ottimizzazione dei costi e dello storage.

Argomenti

- [Funzionamento dei gruppi S3 Storage Lens](#)
- [Utilizzo dei gruppi Storage Lens](#)

Funzionamento dei gruppi S3 Storage Lens

I gruppi Storage Lens consentono di aggregare i parametri utilizzando filtri personalizzati basati sui metadati degli oggetti. Quando si definisce un filtro personalizzato, è possibile utilizzare prefissi, suffissi, tag degli oggetti, dimensioni degli oggetti, età degli oggetti o una combinazione di questi filtri personalizzati. Durante la creazione del gruppo Storage Lens, puoi anche includere un singolo filtro o più condizioni di filtro. Per specificare più condizioni di filtro, utilizza gli operatori logici And oppure Or.

Quando crei e configuri un gruppo Storage Lens, questo opera da filtro personalizzato nel pannello di controllo al quale colleghi il gruppo. Nel pannello di controllo, puoi quindi utilizzare il filtro di gruppo Storage Lens per ottenere parametri di archiviazione basati sul filtro personalizzato che hai definito nel gruppo.

Per visualizzare i dati del gruppo Storage Lens nel pannello di controllo S3 Storage Lens, devi creare il gruppo e poi collegarlo al pannello di controllo. Dopo aver collegato il gruppo Storage Lens al pannello di controllo Storage Lens, quest'ultimo raccoglierà i parametri di utilizzo dell'archiviazione entro 48 ore. Potrai visualizzare questi dati nel pannello di controllo Storage Lens oppure esportarli tramite un'esportazione dei parametri. Se dimentichi di collegare un gruppo Storage Lens a un pannello di controllo, i dati del gruppo Storage Lens non verranno acquisiti e quindi neppure visualizzati.

Note

- Quando crei un gruppo S3 Storage Lens, stai creando una risorsa. AWS Pertanto, ogni gruppo Storage Lens ha il proprio nome della risorsa Amazon (ARN), che puoi specificare quando [lo colleghi o lo escludi da un pannello di controllo S3 Storage Lens](#).
- Se il tuo gruppo Storage Lens non è collegato a un pannello di controllo, non dovrai sostenere costi aggiuntivi per la creazione di un gruppo Storage Lens.

- S3 Storage Lens aggrega i parametri di utilizzo di un oggetto in tutti i gruppi Storage Lens corrispondenti. Pertanto, se un oggetto soddisfa le condizioni di filtro per due o più gruppi Storage Lens, i conteggi relativi all'utilizzo dell'archiviazione saranno visualizzati come ripetuti per lo stesso oggetto.

Puoi creare un gruppo Storage Lens a livello di account in una regione principale specificata (dall'elenco dei supportati Regioni AWS). Quindi, puoi collegare il tuo gruppo Storage Lens a più pannelli di controllo Storage Lens, purché tali pannelli si trovino nello stesso Account AWS e nella stessa regione. È possibile creare fino a 50 gruppi Storage Lens con la stessa regione di origine in ogni Account AWS.

Puoi creare e gestire i gruppi S3 Storage Lens utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), AWS gli SDK o l'API REST di Amazon S3.

Argomenti

- [Visualizzazione dei parametri aggregati del gruppo Storage Lens](#)
- [Autorizzazioni gruppi Storage Lens](#)
- [Configurazione dei gruppi Storage Lens](#)
- [AWS tag delle risorse](#)
- [Esportazione dei parametri dei gruppi Storage Lens](#)

Visualizzazione dei parametri aggregati del gruppo Storage Lens

È possibile visualizzare i parametri aggregati per i gruppi Storage Lens collegando i gruppi a un pannello di controllo. I gruppi Storage Lens che desideri collegare devono risiedere nella regione di origine designata nell'account del pannello di controllo.

Per collegare un gruppo Storage Lens a un pannello di controllo, è necessario specificare il gruppo nella sezione Aggregazione dei gruppi Storage Lens della configurazione del pannello di controllo. Se hai più gruppi Storage Lens, puoi filtrare i risultati in Aggregazione dei gruppi Storage Lens per includere o escludere solo i gruppi che desideri. Per ulteriori informazioni su come collegare gruppi ai pannelli di controllo, consulta [the section called “Collegare o rimuovere un gruppo Storage Lens”](#).

Dopo aver collegato i gruppi, i dati di aggregazione dei gruppi di Storage Lens ulteriori saranno visibili nel pannello di controllo entro 48 ore.

 Note

Per visualizzare i parametri aggregati relativi al tuo gruppo Storage Lens, devi collegare il gruppo a pannello di controllo S3 Storage Lens.

Autorizzazioni gruppi Storage Lens

I gruppi Storage Lens richiedono determinate autorizzazioni in AWS Identity and Access Management (IAM) per autorizzare l'accesso alle azioni del gruppo S3 Storage Lens. Per concedere queste autorizzazioni, puoi utilizzare una policy IAM basata sull'identità. Ti basterà collegare la policy agli utenti, ai gruppi o ai ruoli IAM ai quali devi concedere le autorizzazioni. Tali autorizzazioni possono includere la possibilità di creare o eliminare gruppi Storage Lens, visualizzarne le configurazioni o gestirne i tag.

L'utente o il ruolo IAM a cui concedi le autorizzazioni deve appartenere all'account che ha creato o possiede il gruppo Storage Lens.

Per utilizzare i gruppi Storage Lens e visualizzare i parametri dei gruppi Storage Lens, devi prima disporre delle autorizzazioni appropriate per utilizzare S3 Storage Lens. Per ulteriori informazioni, consulta [the section called “Impostazione delle autorizzazioni”](#).

Per creare e gestire gruppi S3 Storage Lens, devi disporre delle seguenti autorizzazioni IAM, a seconda delle azioni che desideri eseguire:

Azione	autorizzazioni IAM
Creare un nuovo gruppo Storage Lens	s3:CreateStorageLensGroup
Creare un nuovo gruppo Storage Lens con tag	s3:CreateStorageLensGroup , s3:TagResource
Aggiornare un gruppo Storage Lens esistente	s3:UpdateStorageLensGroup
Restituire i dettagli di una configurazione del gruppo Storage Lens	s3:GetStorageLensGroup
Elencare tutti i gruppi Storage Lens nella tua regione di origine	s3:ListStorageLensGroups

Azione	autorizzazioni IAM
Eliminare un gruppo Storage Lens	s3:DeleteStorageLensGroup
Elencare i tag aggiunti al tuo gruppo Storage Lens	s3:ListTagsForResource
Aggiungere o aggiornare un tag di gruppo Storage Lens per un gruppo Storage Lens esistente	s3:TagResource
Eliminare un tag da un gruppo Storage Lens	s3:UntagResource

Ecco un esempio di come configurare la policy IAM nell'account che crea il gruppo Storage Lens. Per utilizzare questa policy, sostituisci *us-east-1* con la regione di origine in cui si trova il gruppo Storage Lens. Sostituisci *111122223333* con l'ID del tuo Account AWS e sostituisci *example-storage-lens-group* con il nome del gruppo Storage Lens. Per applicare queste autorizzazioni a tutti i gruppi Storage Lens, sostituisci *example-storage-lens-group* con ***.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EXAMPLE-Statement-ID",
      "Effect": "Allow",
      "Action": [
        "s3:CreateStorageLensGroup",
        "s3:UpdateStorageLensGroup",
        "s3:GetStorageLensGroup",
        "s3:ListStorageLensGroups",
        "s3:DeleteStorageLensGroup",
        "s3:TagResource",
        "s3:UntagResource",
        "s3:ListTagsForResource"
      ],
      "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens-group/example-storage-lens-group"
    }
  ]
}
```

Per ulteriori informazioni sull'utilizzo di S3 Storage Lens, consulta [Impostazione delle autorizzazioni di Amazon S3 Storage Lens](#). Per informazioni sul linguaggio delle policy IAM, consulta [Policy e autorizzazioni in Amazon S3](#).

Configurazione dei gruppi Storage Lens

Nome dei gruppi S3 Storage Lens

Ti consigliamo di assegnare ai gruppi Storage Lens nomi che ne indichino lo scopo, in modo da poter determinare facilmente quali gruppi collegare ai pannelli di controllo. Per [collegare un gruppo Storage Lens a un pannello di controllo](#), è necessario specificare il gruppo nella sezione Aggregazione dei gruppi Storage Lens della configurazione del pannello di controllo.

I nomi dei gruppi Storage Lens devono essere univoci all'interno dell'account. Non devono superare i 64 caratteri e possono contenere solo lettere (a-z A-Z), numeri (0-9), trattini () e trattini bassi (-). _

Regione d'origine

La regione principale è la regione Regione AWS in cui viene creato e gestito il gruppo Storage Lens. Il gruppo Storage Lens viene creato nella stessa regione di origine del pannello di controllo Amazon S3 Storage Lens. Anche la configurazione e i parametri del gruppo Storage Lens vengono archiviati in questa regione. È possibile creare fino a 50 gruppi Storage Lens nella stessa regione di origine.

Dopo aver creato il gruppo Storage Lens, non sarà possibile modificarne la regione.

Scope

Affinché possano essere inclusi nel gruppo Storage Lens, gli oggetti devono rientrare nell'ambito del pannello di controllo Amazon S3 Storage Lens. L'ambito del pannello di controllo Storage Lens è determinato dai bucket che includi nell'ambito del pannello di controllo della configurazione del pannello di controllo di S3 Storage Lens.

Puoi utilizzare diversi filtri relativi agli oggetti per definire l'ambito del gruppo Storage Lens. Per visualizzare questi parametri del gruppo Storage Lens nel pannello di controllo di S3 Storage Lens, gli oggetti devono corrispondere ai filtri che includi nei gruppi Storage Lens. Ad esempio, supponiamo che il gruppo Storage Lens includa oggetti con il prefisso marketing e il suffisso .png, ma che nessun oggetto soddisfi tali criteri. In questo caso, i parametri per questo gruppo Storage Lens non verranno generati nell'esportazione giornaliera dei parametri e nessun parametro per questo gruppo sarà visibile nel pannello di controllo.

Filtri

Puoi utilizzare i seguenti filtri in un gruppo S3 Storage Lens:

- **Prefissi:** specifica il [prefisso](#) degli oggetti inclusi, ovvero una stringa di caratteri all'inizio del nome della chiave dell'oggetto. Ad esempio, il valore `images` per il filtro Prefissi include oggetti con uno dei seguenti prefissi: `images/`, `images-marketing` o `images/production`. La lunghezza massima di un prefisso è 1.024 byte.
- **Suffissi:** specifica il suffisso degli oggetti inclusi (ad esempio, `.png`, `.jpeg` o `.csv`). La lunghezza massima di un suffisso è 1.024 byte.
- **Tag degli oggetti:** specifica l'elenco dei [tag degli oggetti](#) che desideri filtrare. Una chiave di tag non può superare i 128 caratteri Unicode e il valore di un tag non può superare i 256 caratteri Unicode. Si noti che se il campo del valore del tag dell'oggetto è lasciato vuoto, S3 Storage Lens groups abbina l'oggetto solo ad altri oggetti che hanno anch'essi valori di tag vuoti.
- **Età:** specifica l'intervallo di età degli oggetti inclusi, che viene espressa in giorni. Sono supportati solo i numeri interi.
- **Dimensioni:** specifica l'intervallo di dimensioni degli oggetti inclusi, che viene espresso in byte. Sono supportati solo i numeri interi. Il valore massimo consentito è 50 TB.

Tag degli oggetti del gruppo Storage Lens

È possibile [Creazione di un gruppo Storage Lens](#) che includa fino a 10 filtri per tag di oggetti.

L'esempio seguente include due coppie chiave-valore di tag di oggetto che operano da filtri per un gruppo Storage Lens denominato *Marketing-Department*. Per utilizzare questo esempio, sostituisci *Marketing-Department* con il nome del gruppo e sostituisci *object-tag-key-1*, *object-tag-value-1* e così via con le coppie chiave-valore del tag dell'oggetto che desideri filtrare.

```
{
  "Name": "Marketing-Department",
  "Filter": {
    "MatchAnyTag": [
      {
        "Key": "object-tag-key-1",
        "Value": "object-tag-value-1"
      },
      {
        "Key": "object-tag-key-2",
```

```

        "Value": "object-tag-value-2"
      }
    ]
  }
}

```

Operatori logici (And o Or)

Per includere più condizioni di filtro nel gruppo Storage Lens, è possibile utilizzare operatori logici (And o Or). Nell'esempio seguente, il gruppo Storage Lens denominato *Marketing-Department* ha un operatore And che contiene i filtri Prefix, ObjectAge e ObjectSize. Poiché viene utilizzato un operatore And, solo gli oggetti che soddisfano tutte queste condizioni di filtro verranno inclusi nell'ambito del gruppo Storage Lens.

Per utilizzare questo esempio, sostituisci *user input placeholders* con i valori in base ai quali desideri filtrare.

```

{
  "Name": "Marketing-Department",
  "Filter": {
    "And": {
      "MatchAnyPrefix": [
        "prefix-1",
        "prefix-2",
        "prefix-3/sub-prefix-1"
      ],
      "MatchObjectAge": {
        "DaysGreaterThan": 10,
        "DaysLessThan": 60
      },
      "MatchObjectSize": {
        "BytesGreaterThan": 10,
        "BytesLessThan": 60
      }
    }
  }
}

```

 Note

Se desideri includere oggetti che soddisfano una qualsiasi delle condizioni di filtro, sostituisci l'operatore logico And con l'operatore logico Or in questo esempio.

AWS tag delle risorse

Ogni gruppo S3 Storage Lens viene conteggiato come AWS risorsa con il proprio Amazon Resource Name (ARN). Pertanto, quando configuri il gruppo Storage Lens, puoi aggiungere facoltativamente tag delle risorse AWS al gruppo. È possibile aggiungere fino a 50 tag per ogni gruppo Storage Lens. Per creare un gruppo Storage Lens con tag, devi disporre delle autorizzazioni `s3:CreateStorageLensGroup` e `s3:TagResource`.

Puoi utilizzare i tag AWS delle risorse per classificare le risorse in base al reparto, alla linea di business o al progetto. Ciò è utile quando si dispone di numerose risorse dello stesso tipo. Applicando i tag, è possibile individuare rapidamente un gruppo Storage Lens in base ai tag che hai assegnato loro. È possibile utilizzare i tag anche per monitorare e allocare i costi.

Inoltre, quando si aggiunge un tag di AWS risorsa al gruppo Storage Lens, si attiva il controllo degli accessi [basato sugli attributi \(ABAC\)](#). L'ABAC è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, in questo caso ai tag. Puoi anche utilizzare condizioni che specificano i tag delle risorse nelle tue policy IAM per [controllare l'accesso alle risorse. AWS](#)

Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Inoltre, tieni presente le limitazioni seguenti:

- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole.
- Se aggiungi un tag con la stessa chiave di un tag esistente su quella risorsa, il nuovo valore sovrascrive il vecchio valore.
- Se elimini una risorsa, verranno eliminati anche tutti i tag a essa associati.
- Non includere dati privati o sensibili nei tag delle AWS risorse.
- I tag di sistema (con chiavi di tag che iniziano con `aws:`) non sono supportati.
- La lunghezza di ogni chiave di tag non può superare i 128 caratteri. La lunghezza di ogni valore di tag non può superare i 256 caratteri.

Esportazione dei parametri dei gruppi Storage Lens

I parametri del gruppo S3 Storage Lens sono inclusi nell'esportazione [parametri di Amazon S3 Storage Lens](#) per il pannello di controllo a cui è collegato il gruppo Storage Lens. Per informazioni generali sulla funzionalità di esportazione dei parametri di Storage Lens, consulta [Visualizzazione dei parametri di Amazon S3 Storage Lens utilizzando una esportazione di dati](#).

L'esportazione dei parametri dei gruppi Storage Lens include tutti i parametri di S3 Storage Lens che rientrano nell'ambito del pannello di controllo che hai collegato al gruppo Storage Lens. L'esportazione include anche dati aggiuntivi relativi ai parametri per i gruppi Storage Lens.

Una volta creato il gruppo Storage Lens, l'esportazione dei parametri viene inviata quotidianamente al bucket che hai selezionato al momento di configurare l'esportazione dei parametri per il pannello di controllo a cui è collegato il gruppo. Per ricevere la prima esportazione dei parametri possono essere necessarie fino a 48 ore.

Per generare i parametri dell'esportazione quotidiana, gli oggetti devono corrispondere ai filtri che includi nei gruppi Storage Lens. Se nessun oggetto corrisponde ai filtri che hai incluso nel gruppo Storage Lens, non verrà generato alcun parametro. Tuttavia, se un oggetto corrisponde a due o più gruppi Storage Lens, l'oggetto viene elencato separatamente per ogni gruppo nell'esportazione dei parametri.

Per identificare i parametri per i gruppi Storage Lens cerca uno dei seguenti valori nella colonna `record_type` dell'esportazione dei parametri per il pannello di controllo:

- `STORAGE_LENS_GROUP_BUCKET`
- `STORAGE_LENS_GROUP_ACCOUNT`

La colonna `record_value` mostra l'ARN della risorsa per il gruppo Storage Lens (ad esempio, `arn:aws:s3:us-east-1:111122223333:storage-lens-group/Marketing-Department`).

Utilizzo dei gruppi Storage Lens

I gruppi Amazon S3 Storage Lens aggregano i parametri utilizzando filtri personalizzati basati sui metadati degli oggetti. È possibile analizzare e filtrare i parametri di S3 Storage Lens utilizzando prefissi, suffissi, tag degli oggetti, dimensioni o età degli oggetti. Con i gruppi Amazon S3 Storage Lens puoi anche classificare l'utilizzo all'interno di e tra bucket Amazon S3. Di conseguenza, sarai in grado di comprendere e ottimizzare meglio la tua archiviazione S3.

Per iniziare a visualizzare i dati per un gruppo Storage Lens, devi prima [collegare il gruppo Storage Lens a un pannello di controllo di S3 Storage Lens](#). Se devi gestire i gruppi di Storage Lens nel pannello di controllo, puoi modificare la configurazione del pannello di controllo. Per verificare quali gruppi Storage Lens sono presenti nel tuo account, elencali. Per verificare quali gruppi Storage Lens sono collegati al pannello di controllo, puoi controllare in qualsiasi momento la scheda Gruppi Storage Lens nel pannello di controllo. Accedi ai dettagli di un gruppo Storage Lens esistente per rivedere o aggiornare il suo ambito. È inoltre possibile eliminare definitivamente un gruppo Storage Lens.

Per gestire le autorizzazioni, puoi creare e aggiungere tag di AWS risorse definiti dall'utente ai tuoi gruppi Storage Lens. È possibile utilizzare i tag AWS delle risorse per classificare le risorse in base al reparto, alla linea di business o al progetto. Ciò è utile quando si dispone di numerose risorse dello stesso tipo. Applicando i tag, è possibile individuare rapidamente un gruppo Storage Lens in base ai tag che hai assegnato loro.

Inoltre, quando si aggiunge un tag di AWS risorsa al gruppo Storage Lens, si attiva il controllo degli accessi [basato sugli attributi \(ABAC\)](#). L'ABAC è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, in questo caso ai tag. Puoi anche utilizzare condizioni che specificano i tag delle risorse nelle tue policy IAM per [controllare l'accesso alle risorse. AWS](#)

Argomenti

- [Creazione di un gruppo Storage Lens](#)
- [Collegare o rimuovere gruppi S3 Storage Lens a o da un pannello di controllo](#)
- [Visualizzazione dei dati dei gruppi Storage Lens](#)
- [Aggiornamento di un gruppo Storage Lens](#)
- [Gestione AWS tag di risorse con gruppi Storage Lens](#)
- [Elenco di tutti i gruppi Storage Lens](#)
- [Visualizzazione dei dettagli del gruppo Storage Lens](#)
- [Eliminazione di un gruppo Storage Lens](#)

Creazione di un gruppo Storage Lens

Gli esempi seguenti dimostrano come creare un gruppo Amazon S3 Storage Lens utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e. AWS SDK per Java

Utilizzo della console S3

Per creare un gruppo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome della AWS regione attualmente visualizzata. Quindi, scegli la Regione a cui passare.
3. Nel riquadro di navigazione sinistro, scegli Gruppi Storage Lens.
4. Scegli Crea gruppo Storage Lens.
5. In Generale, visualizza la Regione di provenienza e inserisci il nome del gruppo Storage Lens.
6. In Ambito, scegli il filtro da applicare al gruppo Storage Lens. Per applicare più filtri, seleziona i filtri, quindi scegli l'operatore logico AND oppure OR.
 - Per il filtro Prefissi, scegli Prefissi e inserisci una stringa di prefisso. Per aggiungere più prefissi, scegli Aggiungi prefisso. Per rimuovere un prefisso, scegli Rimuovi accanto al prefisso che desideri eliminare.
 - Per il filtro Tag di oggetti, scegli Tag di oggetti e inserisci la coppia chiave-valore per l'oggetto. Quindi scegli Aggiungi tag. Per rimuovere un tag, scegli Rimuovi accanto al tag che desideri eliminare.
 - Per il filtro Suffissi, scegli Suffissi. e inserisci una stringa di suffisso. Per aggiungere più suffissi, scegli Aggiungi suffisso. Per rimuovere un suffisso, scegli Rimuovi accanto al suffisso che desideri eliminare.
 - Per il filtro Età, specifica l'intervallo di età dell'oggetto in giorni. Scegli Specifica l'età minima dell'oggetto e inserisci l'età minima dell'oggetto. Poi scegli Specifica l'età massima dell'oggetto e inserisci l'età massima dell'oggetto.
 - Per il filtro Dimensione, specifica l'intervallo di dimensioni dell'oggetto e l'unità di misura. Scegli Specifica la dimensione minima dell'oggetto e inserisci la dimensione minima dell'oggetto. Poi scegli Specifica la dimensione massima dell'oggetto e inserisci la dimensione dell'oggetto.
7. (Facoltativo) Per i tag AWS delle risorse, aggiungi la coppia chiave-valore, quindi scegli Aggiungi tag.
8. Scegli Crea gruppo Storage Lens.

Utilizzo di AWS CLI

Il AWS CLI comando di esempio seguente crea un gruppo Storage Lens. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control create-storage-lens-group --account-id 111122223333 \  
--region us-east-1 --storage-lens-group=file:///./marketing-department.json
```

Il AWS CLI comando di esempio seguente crea un gruppo Storage Lens con due tag di AWS risorse. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control create-storage-lens-group --account-id 111122223333 \  
--region us-east-1 --storage-lens-group=file:///./marketing-department.json \  
--tags Key=k1,Value=v1 Key=k2,Value=v2
```

Per esempi di configurazione JSON, consulta [Configurazione dei gruppi Storage Lens](#).

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente crea un gruppo Storage Lens. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

Example– Creare un gruppo Storage Lens con un solo filtro

Nel seguente esempio viene creato un gruppo Storage Lens denominato *Marketing-Department*. Questo gruppo dispone di un filtro relativo all'età degli oggetti che specifica una fascia di età compresa tra *30* e *90* giorni. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;  
  
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.s3control.S3ControlClient;  
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;  
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;  
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;  
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
```

```
public class CreateStorageLensGroupWithObjectAge {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupFilter objectAgeFilter = StorageLensGroupFilter.builder()
                .matchObjectAge(MatchObjectAge.builder()
                    .daysGreaterThan(30)
                    .daysLessThan(90)
                    .build())
                .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                .name(storageLensGroupName)
                .filter(objectAgeFilter)
                .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
                CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .build();

            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```


Example— Creare un gruppo Storage Lens con un operatore AND che include più filtri

Nel seguente esempio viene creato un gruppo Storage Lens denominato *Marketing-Department*. Per questo gruppo viene utilizzato l'operatore AND per indicare che gli oggetti devono soddisfare tutte le condizioni del filtro. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.S3Tag;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupAndOperator;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;

public class CreateStorageLensGroupWithAndFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create object tags.
            S3Tag tag1 = S3Tag.builder()
                .key("object-tag-key-1")
                .value("object-tag-value-1")
                .build();
            S3Tag tag2 = S3Tag.builder()
                .key("object-tag-key-2")
                .value("object-tag-value-2")
                .build();

            StorageLensGroupAndOperator andOperator =
                StorageLensGroupAndOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchAnySuffix(".png", ".gif", ".jpg")
```

```

        .matchAnyTag(tag1, tag2)
        .matchObjectAge(MatchObjectAge.builder()
            .daysGreaterThan(30)
            .daysLessThan(90).build())
        .matchObjectSize(MatchObjectSize.builder()
            .bytesGreaterThan(1000L)
            .bytesLessThan(6000L).build())
        .build();

StorageLensGroupFilter andFilter = StorageLensGroupFilter.builder()
    .and(andOperator)
    .build();

StorageLensGroup storageLensGroup = StorageLensGroup.builder()
    .name(storageLensGroupName)
    .filter(andFilter)
    .build();

CreateStorageLensGroupRequest createStorageLensGroupRequest =
CreateStorageLensGroupRequest.builder()
    .storageLensGroup(storageLensGroup)
    .accountId(accountId).build();

S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.US_WEST_2)
    .credentialsProvider(ProfileCredentialsProvider.create())
    .build();
s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
}

```

Example— Creare un gruppo Storage Lens con un operatore OR che include più filtri

Nel seguente esempio viene creato un gruppo Storage Lens denominato *Marketing-Department*. Per questo gruppo viene utilizzato un operatore OR per applicare un filtro di prefisso (*prefix-1*, *prefix-2*, *prefix3/sub-prefix-1*) o un filtro per le dimensioni degli oggetti con un intervallo di dimensioni compreso tra *1000* e *6000* byte. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupOrOperator;

public class CreateStorageLensGroupWithOrFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupOrOperator orOperator =
                StorageLensGroupOrOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchObjectSize(MatchObjectSize.builder()
                        .bytesGreaterThan(1000L)
                        .bytesLessThan(6000L)
                        .build())
                    .build();

            StorageLensGroupFilter orFilter = StorageLensGroupFilter.builder()
                .or(orOperator)
                .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                .name(storageLensGroupName)
                .filter(orFilter)
```

```

        .build();

        CreateStorageLensGroupRequest createStorageLensGroupRequest =
CreateStorageLensGroupRequest.builder()
        .storageLensGroup(storageLensGroup)
        .accountId(accountId).build();

        S3ControlClient s3ControlClient = S3ControlClient.builder()
        .region(Region.US_WEST_2)
        .credentialsProvider(ProfileCredentialsProvider.create())
        .build();
        s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it and returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
}
}

```

Example— Creare un gruppo Storage Lens con un solo filtro e due AWS tag delle risorse

Nel seguente esempio viene creato un gruppo Storage Lens denominato *Marketing-Department* e dotato di un filtro di suffisso. Questo esempio aggiunge anche due tag di AWS risorse al gruppo Storage Lens. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```

package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.Tag;

```

```
public class CreateStorageLensGroupWithResourceTags {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create AWS resource tags.
            Tag resourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-value-1")
                .build();
            Tag resourceTag2 = Tag.builder()
                .key("resource-tag-key-2")
                .value("resource-tag-value-2")
                .build();

            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                .matchAnySuffix(".png", ".gif", ".jpg")
                .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                .name(storageLensGroupName)
                .filter(suffixFilter)
                .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
                CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

```
}  
  }  
}
```

Per esempi di configurazione JSON, consulta [Configurazione dei gruppi Storage Lens](#).

Collegare o rimuovere gruppi S3 Storage Lens a o da un pannello di controllo

Dopo aver effettuato l'upgrade al livello avanzato di Amazon S3 Storage Lens, puoi collegare [un gruppo Storage Lens](#) al pannello di controllo. Se hai diversi gruppi Storage Lens, puoi includere o escludere i gruppi desiderati.

I gruppi Storage Lens devono risiedere nella regione di origine designata nell'account del pannello di controllo. Dopo aver collegato un gruppo Storage Lens al pannello di controllo, riceverai i dati aggiuntivi relativi all'aggregazione dei gruppi Storage Lens nel documento di esportazione dei parametri entro 48 ore.

Note

Se desideri vedere le metriche aggregate per il gruppo Storage Lens, devi collegare quest'ultimo al tuo pannello di controllo Storage Lens. Per esempi di file di configurazione JSON del gruppo Storage Lens, consulta [Esempio di configurazione di S3 Storage Lens con gruppi Storage Lens in JSON](#).

Utilizzo della console S3

Per collegare un gruppo Storage Lens a un pannello di controllo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, in Storage Lens scegli Pannelli di controllo.
3. Scegli il pulsante di opzione per il pannello di controllo Storage Lens a cui desideri collegare un gruppo Storage Lens.
4. Scegli Modifica.
5. Sotto Metrics selection (Selezione dei parametri), scegli Advanced metrics and recommendations (Raccomandazioni e parametri avanzati).
6. Seleziona Aggregazione dei gruppi Storage Lens.

 Note

I parametri avanzati sono selezionati per impostazione predefinita. Tuttavia, è anche possibile deselezionare questa impostazione, poiché non è necessaria per aggregare i dati dei gruppi di Storage Lens.

7. Scorri verso il basso fino ad Aggregazione del gruppo Storage Lens e specifica il gruppo o i gruppi Storage Lens che desideri includere o escludere nell'aggregazione dei dati. È possibile utilizzare una qualsiasi delle seguenti opzioni di filtro:
 - Se desideri includere determinati gruppi di Storage Lens, scegli Includi gruppi Storage Lens. In Gruppi Storage Lens da includere, seleziona i tuoi gruppi Storage Lens.
 - Se desideri includere tutti i gruppi Storage Lens, seleziona Includi tutti i gruppi Storage Lens nella regione di origine di questo account.
 - Se desideri escludere determinati gruppi Storage Lens, scegli Escludi gruppi Storage Lens. In Gruppi Storage Lens da escludere, seleziona i gruppi Storage Lens che desideri escludere.
8. Scegli Save changes (Salva modifiche). Se hai configurato correttamente i gruppi Storage Lens, vedrai i dati di aggregazione aggiuntivi dei gruppi Storage Lens nel tuo pannello di controllo entro 48 ore.

Per rimuovere un gruppo Storage Lens da un pannello di controllo S3 Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, in Storage Lens scegli Pannelli di controllo.
3. Scegli il pulsante di opzione per il pannello di controllo Storage Lens dal quale desideri rimuovere un gruppo Storage Lens.
4. Scegli Visualizza configurazione del pannello di controllo.
5. Scegli Modifica.
6. Scorri verso il basso fino alla sezione Selezione di parametri.
7. In Aggregazione dei gruppi Storage Lens, scegli la X accanto al gruppo Storage Lens che desideri rimuovere. Al termine di questa operazione il gruppo Storage Lens viene rimosso.

Se nel pannello di controllo hai incluso tutti i gruppi Storage Lens, deseleziona la casella accanto a Includi tutti i gruppi Storage Lens nella regione di origine di questo account.

8. Scegli Save changes (Salva modifiche).

Note

Sono necessarie fino a 48 ore prima che il pannello di controllo rifletta gli aggiornamenti di configurazione.

Utilizzo di AWS SDK per Java

Example- Collegare tutti i gruppi Storage Lens a una dashboard

Il seguente esempio di SDK per Java collega tutti i gruppi Storage Lens dell'account **111122223333** alla dashboard: ***DashBoardConfigurationId***

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWithStorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel();

            AccountLevel accountLevel = new AccountLevel()
                .withBucketLevel(new BucketLevel())
                .withStorageLensGroupLevel(storageLensGroupLevel);
```



```

        StorageLensConfiguration configuration = new StorageLensConfiguration()
            .withId(configurationId)
            .withAccountLevel(accountLevel)
            .withIsEnabled(true);

        AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
            .withCredentials(new ProfileCredentialsProvider())
            .withRegion(US_WEST_2)
            .build();

        s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
            .withAccountId(sourceAccountId)
            .withConfigId(configurationId)
            .withStorageLensConfiguration(configuration)
        );
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it and returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
}
}

```

Example- Collegare due gruppi Storage Lens a una dashboard

L' AWS SDK per Java esempio seguente collega due gruppi Storage Lens (*StorageLensGroupName1*e*StorageLensGroupName2*) alla dashboard.
ExampleDashboardConfigurationId

```

package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;

```

```
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
StorageLensGroupLevelSelectionCriteria()
                .withInclude(
                    "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
+ ":storage-lens-group/" + storageLensGroupName1,
                    "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
+ ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                .withBucketLevel(new BucketLevel())
                .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                .withId(configurationId)
                .withAccountLevel(accountLevel)
                .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();

            s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
```

```

        .withAccountId(sourceAccountId)
        .withConfigId(configurationId)
        .withStorageLensConfiguration(configuration)
    );
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
}

```

Example- Collegare tutti i gruppi Storage Lens con le esclusioni

Il seguente esempio di SDK per Java collega tutti i gruppi Storage Lens alla *ExampleDashboardConfigurationId* dashboard, esclusi i due specificati (e):
StorageLensGroupName1 StorageLensGroupName2

```

package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroupsExcluded {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
    }
}

```

```
String storageLensGroupName2 = "StorageLensGroupName2";
String sourceAccountId = "111122223333";

try {
    StorageLensGroupLevelSelectionCriteria selectionCriteria = new
StorageLensGroupLevelSelectionCriteria()
        .withInclude(
            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
+ ":storage-lens-group/" + storageLensGroupName1,
            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
+ ":storage-lens-group/" + storageLensGroupName2);

    System.out.println(selectionCriteria);
    StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
        .withSelectionCriteria(selectionCriteria);

    AccountLevel accountLevel = new AccountLevel()
        .withBucketLevel(new BucketLevel())
        .withStorageLensGroupLevel(storageLensGroupLevel);

    StorageLensConfiguration configuration = new StorageLensConfiguration()
        .withId(configurationId)
        .withAccountLevel(accountLevel)
        .withIsEnabled(true);

    AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
        .withCredentials(new ProfileCredentialsProvider())
        .withRegion(US_WEST_2)
        .build();

    s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
        .withAccountId(sourceAccountId)
        .withConfigId(configurationId)
        .withStorageLensConfiguration(configuration)
    );
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
```

```
}  
}  
}
```

Visualizzazione dei dati dei gruppi Storage Lens

Puoi visualizzare i dati dei gruppi Storage Lens [collegando il gruppo al pannello di controllo di Amazon S3 Storage Lens](#). Dopo aver incluso il gruppo Storage Lens nell'aggregazione dei gruppi Storage Lens nella configurazione del pannello di controllo, possono essere necessarie fino a 48 ore prima che i dati del gruppo Storage Lens vengano visualizzati nel pannello di controllo.

Una volta aggiornata la configurazione del pannello di controllo, tutti i gruppi Storage Lens appena collegati vengono visualizzati nell'elenco delle risorse disponibili nella scheda Gruppi Storage Lens. È inoltre possibile analizzare ulteriormente l'utilizzo dell'archiviazione nella scheda Panoramica suddividendo in base ad altre dimensioni. Ad esempio, puoi scegliere uno degli elementi elencati nelle prime 3 categorie e scegliere Analizza per suddividere i dati in base a un'altra dimensione. Non è possibile applicare la stessa dimensione del filtro stesso.

Note

Non è possibile applicare un filtro del gruppo Storage Lens insieme a un filtro con prefisso o viceversa. Inoltre, non è possibile analizzare ulteriormente un gruppo Storage Lens utilizzando un filtro con prefisso.

Puoi utilizzare la scheda Gruppo Storage Lens nel pannello di controllo di Amazon S3 Storage Lens per personalizzare la visualizzazione dei dati per i gruppi di Storage Lens collegati al pannello di controllo. Puoi visualizzare i dati di tutti i gruppi Storage Lens collegati al pannello di controllo o solo di alcuni.

Quando visualizzi i dati del gruppo Storage Lens nel pannello di controllo di S3 Storage Lens, tieni presente quanto segue:

- S3 Storage Lens aggrega i parametri di utilizzo di un oggetto in tutti i gruppi Storage Lens corrispondenti. Pertanto, se un oggetto soddisfa le condizioni di filtro per due o più gruppi Storage Lens, i conteggi relativi all'utilizzo dell'archiviazione saranno visualizzati come ripetuti per lo stesso oggetto.
- Gli oggetti devono corrispondere ai filtri che includi nei gruppi Storage Lens. Se nessun oggetto corrisponde ai filtri che includi nel gruppo Storage Lens, non verrà generato alcun parametro. Per

determinare se ci sono oggetti non assegnati, controlla il numero totale di oggetti nel pannello di controllo a livello di account e di bucket.

Aggiornamento di un gruppo Storage Lens

I seguenti esempi illustrano come aggiornare un gruppo Amazon S3 Storage Lens. Puoi aggiornare un gruppo Storage Lens utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

Per aggiornare un gruppo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Gruppi Storage Lens.
3. In Gruppi Storage Lens, scegli il gruppo Storage Lens che desideri aggiornare.
4. In Ambito, scegli Modifica.
5. Nella pagina Ambito, scegli il filtro da applicare al gruppo Storage Lens. Per applicare più filtri, seleziona i filtri, quindi scegli l'operatore logico AND oppure OR.
 - Per il filtro Prefissi, seleziona Prefissi e inserisci una stringa di prefisso. Per aggiungere più prefissi, scegli Aggiungi prefisso. Per rimuovere un prefisso, scegli Rimuovi accanto al prefisso che desideri eliminare.
 - Per il filtro Tag di oggetti, inserisci la coppia chiave-valore per l'oggetto. Quindi scegli Aggiungi tag. Per rimuovere un tag, scegli Rimuovi accanto al tag che desideri eliminare.
 - Per il filtro Suffissi, seleziona Suffissi. e inserisci una stringa di suffisso. Per aggiungere più suffissi, scegli Aggiungi suffisso. Per rimuovere un suffisso, scegli Rimuovi accanto al suffisso che desideri eliminare.
 - Per il filtro Età, specifica l'intervallo di età dell'oggetto in giorni. Scegli Specifica l'età minima dell'oggetto e inserisci l'età minima dell'oggetto. In Specifica l'età massima dell'oggetto inserisci l'età massima dell'oggetto.
 - Per il filtro Dimensione, specifica l'intervallo di dimensioni dell'oggetto e l'unità di misura. Scegli Specifica la dimensione minima dell'oggetto e inserisci la dimensione minima dell'oggetto. In Specifica la dimensione massima dell'oggetto inserisci la dimensione dell'oggetto.

6. Scegli **Save changes** (Salva modifiche). Viene visualizzata la pagina dei dettagli del gruppo Storage Lens.
7. (Facoltativo) Se desideri aggiungere un nuovo tag di AWS risorsa, scorri fino alla sezione dei tag AWS delle risorse, quindi scegli **Aggiungi tag**. Viene visualizzata la pagina **Aggiungi tag**.

Aggiungi la nuova coppia chiave-valore, quindi scegli **Salva modifiche**. Viene visualizzata la pagina dei dettagli del gruppo Storage Lens.

8. (Facoltativo) Se desideri rimuovere un tag di AWS risorsa esistente, scorri fino alla sezione dei tag AWS delle risorse e seleziona il tag di risorsa. Quindi, scegli **Elimina**. Viene visualizzata la finestra di dialogo **Elimina i tag AWS**.

Scegli nuovamente **Elimina** per eliminare definitivamente il tag delle risorse AWS.

Note

Dopo aver eliminato definitivamente un tag di AWS risorsa, non può essere ripristinato.

Utilizzo di AWS CLI

Il comando di AWS CLI esempio seguente restituisce i dettagli di configurazione per un gruppo Storage Lens denominato *marketing-department*. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control get-storage-lens-group --account-id 111122223333 \  
--region us-east-1 --name marketing-department
```

L'AWS CLI esempio seguente aggiorna un gruppo Storage Lens. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control update-storage-lens-group --account-id 111122223333 \  
--region us-east-1 --storage-lens-group=file:///./marketing-department.json
```

Per esempi di configurazione JSON, consulta [Configurazione dei gruppi Storage Lens](#).

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente restituisce i dettagli di configurazione per il gruppo *Marketing-Department* Storage Lens nell'account *111122223333*. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
                GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .build();

            GetStorageLensGroupResponse response =
                s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```



```
}
```

Nell'esempio seguente viene aggiornato il gruppo Storage Lens *Marketing-Department* nell'account *111122223333*. In questo esempio l'ambito del pannello di controllo viene aggiornato per includere oggetti che corrispondano a uno dei seguenti suffissi: *.png*, *.gif*, *.jpg* o *.jpeg*. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.UpdateStorageLensGroupRequest;

public class UpdateStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create updated filter.
            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                .matchAnySuffix(".png", ".gif", ".jpg", ".jpeg")
                .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                .name(storageLensGroupName)
                .filter(suffixFilter)
                .build();

            UpdateStorageLensGroupRequest updateStorageLensGroupRequest =
                UpdateStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId)
                    .build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
```

```
        .credentialsProvider(ProfileCredentialsProvider.create())
        .build();
    s3ControlClient.updateStorageLensGroup(updateStorageLensGroupRequest);
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
```

Per esempi di configurazione JSON, consulta [Configurazione dei gruppi Storage Lens](#).

Gestione AWS tag di risorse con gruppi Storage Lens

Ogni gruppo Amazon S3 Storage Lens viene conteggiato come AWS risorsa con il proprio Amazon Resource Name (ARN). Pertanto, quando configuri il gruppo Storage Lens, puoi aggiungere facoltativamente tag delle risorse AWS al gruppo. È possibile aggiungere fino a 50 tag per ogni gruppo Storage Lens. Per creare un gruppo Storage Lens con tag, devi disporre delle autorizzazioni `s3:CreateStorageLensGroup` e `s3:TagResource`.

Puoi utilizzare i tag AWS delle risorse per classificare le risorse in base al reparto, alla linea di business o al progetto. Ciò è utile quando si dispone di numerose risorse dello stesso tipo. Applicando i tag, è possibile individuare rapidamente un gruppo Storage Lens in base ai tag che hai assegnato loro. È possibile utilizzare i tag anche per monitorare e allocare i costi.

Inoltre, quando si aggiunge un tag di AWS risorsa al gruppo Storage Lens, si attiva il controllo degli accessi [basato sugli attributi \(ABAC\)](#). L'ABAC è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, in questo caso ai tag. Puoi anche utilizzare condizioni che specificano i tag delle risorse nelle tue policy IAM per [controllare l'accesso alle risorse. AWS](#)

Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Inoltre, tieni presente le limitazioni seguenti:

- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole.
- Se aggiungi un tag con la stessa chiave di un tag esistente su quella risorsa, il nuovo valore sovrascrive il vecchio valore.

- Se elimini una risorsa, verranno eliminati anche tutti i tag a essa associati.
- Non includere dati privati o sensibili nei tag AWS delle risorse.
- I tag di sistema (con chiavi di tag che iniziano con aws :) non sono supportati.
- La lunghezza di ogni chiave di tag non può superare i 128 caratteri. La lunghezza di ogni valore di tag non può superare i 256 caratteri.

Gli esempi seguenti dimostrano come utilizzare i tag AWS delle risorse con i gruppi Storage Lens.

Argomenti

- [Aggiungere un AWS tag di risorsa a un gruppo Storage Lens](#)
- [Aggiornamento dei valori dei tag di un gruppo Storage Lens](#)
- [Eliminazione di un AWS tag di risorsa da un gruppo Storage Lens](#)
- [Elenco dei tag dei gruppi Storage Lens](#)

Aggiungere un AWS tag di risorsa a un gruppo Storage Lens

Gli esempi seguenti dimostrano come aggiungere tag di AWS risorse a un gruppo Amazon S3 Storage Lens. Puoi aggiungere tag di risorse utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e. AWS SDK per Java

Utilizzo della console S3

Per aggiungere un AWS tag di risorsa a un gruppo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Gruppi Storage Lens.
3. In Gruppi Storage Lens, scegli il gruppo Storage Lens che desideri aggiornare.
4. In Tag delle risorse AWS seleziona Aggiungi tag.
5. Nella pagina Aggiungi tag, aggiungi la nuova coppia chiave-valore.

Note

Aggiungendo un tag la cui chiave è la stessa di un tag esistente viene sovrascritto il valore del tag precedente.

6. (Facoltativo) Per aggiungere più di un nuovo tag, scegliete nuovamente **Aggiungi tag e aggiungi nuove voci**. Puoi aggiungere fino a 50 tag di AWS risorse al tuo gruppo Storage Lens.
7. (Facoltativo) Se desideri rimuovere un tag appena aggiunto, scegli **Rimuovi** accanto al tag che desideri eliminare.
8. Scegli **Save changes** (Salva modifiche).

Utilizzo di AWS CLI

Il AWS CLI comando di esempio seguente aggiunge due tag di risorse a un gruppo Storage Lens esistente denominato *marketing-department*. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control tag-resource --account-id 111122223333 \  
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-  
department \  
--region us-east-1 --tags Key=k1,Value=v1 Key=k2,Value=v2
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente aggiunge due tag di AWS risorse a un gruppo Storage Lens esistente. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;  
  
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.s3control.S3ControlClient;  
import software.amazon.awssdk.services.s3control.model.Tag;  
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;  
  
public class TagResource {  
    public static void main(String[] args) {  
        String resourceARN = "Resource_ARN";  
        String accountId = "111122223333";  
  
        try {  
            Tag resourceTag1 = Tag.builder()  
                .key("resource-tag-key-1")
```

```

        .value("resource-tag-value-1")
        .build();
    Tag resourceTag2 = Tag.builder()
        .key("resource-tag-key-2")
        .value("resource-tag-value-2")
        .build();
    TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
        .resourceArn(resourceARN)
        .tags(resourceTag1, resourceTag2)
        .accountId(accountId)
        .build();
    S3ControlClient s3ControlClient = S3ControlClient.builder()
        .region(Region.US_WEST_2)
        .credentialsProvider(ProfileCredentialsProvider.create())
        .build();
    s3ControlClient.tagResource(tagResourceRequest);
} catch (AmazonServiceException e) {
    // The call was transmitted successfully, but Amazon S3 couldn't process
    // it and returned an error response.
    e.printStackTrace();
} catch (SdkClientException e) {
    // Amazon S3 couldn't be contacted for a response, or the client
    // couldn't parse the response from Amazon S3.
    e.printStackTrace();
}
}
}

```

Aggiornamento dei valori dei tag di un gruppo Storage Lens

I seguenti esempi dimostrano come aggiornare i valori dei tag di gruppo Storage Lens utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java

Utilizzo della console S3

Per aggiornare un AWS tag di risorsa per un gruppo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Gruppi Storage Lens.
3. In Gruppi Storage Lens, scegli il gruppo Storage Lens che desideri aggiornare.
4. In Tag delle risorse AWS , seleziona il tag che desideri aggiornare.

5. Aggiungi il nuovo valore del tag, utilizzando la stessa chiave della coppia chiave-valore che desideri aggiornare. Seleziona l'icona del segno di spunta per aggiornare il valore del tag.

Note

Aggiungendo un tag la cui chiave è la stessa di un tag esistente viene sovrascritto il valore del tag precedente.

6. (Facoltativo) Se desideri aggiungere nuovi tag, scegli Aggiungi tag per aggiungere nuove voci. Viene visualizzata la pagina Aggiungi tag.

Puoi aggiungere fino a 50 tag di AWS risorse per il tuo gruppo Storage Lens. Una volta finito di aggiungere i tag, scegli Salva modifiche.

7. (Facoltativo) Se desideri rimuovere un tag appena aggiunto, scegli Rimuovi accanto al tag che desideri eliminare. Una volta finito di rimuovere i tag, scegli Salva modifiche.

Utilizzo di AWS CLI

Il AWS CLI comando di esempio seguente aggiorna due valori di tag per il gruppo Storage Lens denominato *marketing-department*. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control tag-resource --account-id 111122223333 \  
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-  
department \  
--region us-east-1 --tags Key=k1,Value=v3 Key=k2,Value=v4
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente aggiorna due valori di tag del gruppo Storage Lens. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;  
  
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.s3control.S3ControlClient;  
import software.amazon.awssdk.services.s3control.model.Tag;
```

```

import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class UpdateTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            Tag updatedResourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-updated-value-1")
                .build();
            Tag updatedResourceTag2 = Tag.builder()
                .key("resource-tag-key-2")
                .value("resource-tag-updated-value-2")
                .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                .resourceArn(resourceARN)
                .tags(updatedResourceTag1, updatedResourceTag2)
                .accountId(accountId)
                .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}

```

Eliminazione di un AWS tag di risorsa da un gruppo Storage Lens

I seguenti esempi dimostrano come eliminare un tag di AWS risorsa da un gruppo Storage Lens. Puoi eliminare i tag utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

Per eliminare un AWS tag di risorsa di un gruppo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Nel pannello di navigazione a sinistra, scegli Gruppi Storage Lens.
3. In Gruppi Storage Lens, scegli il gruppo Storage Lens che desideri aggiornare.
4. In Tag delle risorse AWS , seleziona la coppia chiave-valore che desideri eliminare.
5. Scegli Elimina. Viene visualizzata la finestra di dialogo Elimina i tag delle risorse AWS .

Note

Se si utilizzano tag per controllare l'accesso, effettuare questa operazione può influire sulle risorse correlate. Una volta eliminato definitivamente, non è possibile ripristinare un tag.

6. Scegli Elimina per eliminare la coppia chiave-valore in modo permanente.

Utilizzo di AWS CLI

Il AWS CLI comando seguente elimina due tag di AWS risorse da un gruppo Storage Lens esistente: per utilizzare questo comando di esempio, sostituiscili *user input placeholders* con le tue informazioni.

```
aws s3control untag-resource --account-id 111122223333 \  
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/Marketing-  
Department \  
--region us-east-1 --tag-keys k1 k2
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente elimina due tag di AWS risorse dal gruppo Storage Lens Amazon Resource Name (ARN) specificato nell'account. 111122223333 Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;
```



```

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;

public class UntagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            String tagKey1 = "resource-tag-key-1";
            String tagKey2 = "resource-tag-key-2";
            UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
                .resourceArn(resourceARN)
                .tagKeys(tagKey1, tagKey2)
                .accountId(accountId)
                .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .build();
            s3ControlClient.untagResource(untagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}

```

Elenco dei tag dei gruppi Storage Lens

Gli esempi seguenti dimostrano come elencare i tag delle AWS risorse associati a un gruppo Storage Lens. Puoi elencare i tag utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

Per esaminare l'elenco e i valori dei tag per un gruppo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Gruppi Storage Lens.
3. In Gruppi Storage Lens, scegli il gruppo Storage Lens di tuo interesse.
4. Scorri verso il basso fino alla sezione Tag delle risorse AWS . Tutti i tag AWS delle risorse definiti dall'utente che vengono aggiunti al gruppo Storage Lens sono elencati insieme ai relativi valori dei tag.

Utilizzo di AWS CLI

Il comando di AWS CLI esempio seguente elenca tutti i valori dei tag del gruppo Storage Lens per il gruppo Storage Lens denominato *marketing-department*. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control list-tags-for-resource --account-id 111122223333 \  
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-  
department \  
--region us-east-1
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente elenca i valori dei tag del gruppo Storage Lens per il gruppo Storage Lens Amazon Resource Name (ARN) specificato. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;  
  
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.s3control.S3ControlClient;  
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;  
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;
```

```

public class ListTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            ListTagsForResourceRequest listTagsForResourceRequest =
ListTagsForResourceRequest.builder()
                .resourceArn(resourceARN)
                .accountId(accountId)
                .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .build();
            ListTagsForResourceResponse response =
s3ControlClient.listTagsForResource(listTagsForResourceRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}

```

Elenco di tutti i gruppi Storage Lens

Negli esempi seguenti viene illustrato come elencare tutti i gruppi Amazon S3 Storage Lens in un Account AWS e una regione di origine. Questi esempi mostrano come elencare tutti i gruppi Storage Lens utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java

Utilizzo della console S3

Per elencare tutti i gruppi Storage Lens in un account e in una regione di origine

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nel riquadro di navigazione sinistro, scegli Gruppi Storage Lens.
3. In Gruppi Storage Lens, viene visualizzato l'elenco dei gruppi Storage Lens presenti nell'account.

Utilizzo di AWS CLI

L' AWS CLI esempio seguente elenca tutti i gruppi Storage Lens per il tuo account. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control list-storage-lens-groups --account-id 111122223333 \  
--region us-east-1
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente elenca i gruppi Storage Lens per account *111122223333*. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;  
  
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.SdkClientException;  
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;  
import software.amazon.awssdk.regions.Region;  
import software.amazon.awssdk.services.s3control.S3ControlClient;  
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsRequest;  
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsResponse;  
  
public class ListStorageLensGroups {  
    public static void main(String[] args) {  
        String accountId = "111122223333";  
  
        try {  
            ListStorageLensGroupsRequest listStorageLensGroupsRequest =  
ListStorageLensGroupsRequest.builder()  
                .accountId(accountId)  
                .build();  
            S3ControlClient s3ControlClient = S3ControlClient.builder()  
                .region(Region.US_WEST_2)  
                .credentialsProvider(ProfileCredentialsProvider.create())  
                .build();  
            ListStorageLensGroupsResponse response =  
s3ControlClient.listStorageLensGroups(listStorageLensGroupsRequest);
```

```
        System.out.println(response);
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it and returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}
```

Visualizzazione dei dettagli del gruppo Storage Lens

I seguenti esempi illustrano come visualizzare i dettagli di un gruppo Amazon S3 Storage Lens. Puoi visualizzare questi dettagli utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java.

Utilizzo della console S3

Per visualizzare i dettagli di configurazione del gruppo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Gruppi Storage Lens.
3. In Gruppi Storage Lens, scegli il pulsante di opzione accanto al gruppo Storage Lens di tuo interesse.
4. Seleziona Visualizza dettagli. Ora puoi rivedere i dettagli del tuo gruppo Storage Lens.

Utilizzo di AWS CLI

L' AWS CLI esempio seguente restituisce i dettagli di configurazione per un gruppo Storage Lens. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente restituisce i dettagli di configurazione per il gruppo Storage Lens indicato *Marketing-Department* nell'account *111122223333*. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
                GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .build();

            GetStorageLensGroupResponse response =
                s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

```
}
```

Eliminazione di un gruppo Storage Lens

Gli esempi seguenti dimostrano come eliminare un gruppo Amazon S3 Storage Lens utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI) e AWS SDK per Java

Utilizzo della console S3

Per eliminare un gruppo Storage Lens

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Gruppi Storage Lens.
3. In Gruppi Storage Lens, scegli il pulsante di opzione accanto al gruppo Storage Lens che desideri eliminare.
4. Scegli Elimina. Viene visualizzata la finestra di dialogo Elimina gruppo Storage Lens.
5. Scegli nuovamente Elimina per rimuovere definitivamente il gruppo Storage Lens.

Note

Una volta eliminato, non è più possibile ripristinare un gruppo Storage Lens.

Utilizzo di AWS CLI

L' AWS CLI esempio seguente elimina il gruppo Storage Lens denominato *marketing-department*. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws s3control delete-storage-lens-group --account-id 111122223333 \  
--region us-east-1 --name marketing-department
```

Utilizzo di AWS SDK per Java

L' AWS SDK per Java esempio seguente elimina il gruppo Storage Lens denominato *Marketing-Department* in account. *111122223333*. Per utilizzare questo esempio, sostituisci *user input placeholders* con le informazioni appropriate.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.DeleteStorageLensGroupRequest;

public class DeleteStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            DeleteStorageLensGroupRequest deleteStorageLensGroupRequest =
DeleteStorageLensGroupRequest.builder()
                .name(storageLensGroupName)
                .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(Region.US_WEST_2)
                .credentialsProvider(ProfileCredentialsProvider.create())
                .build();
            s3ControlClient.deleteStorageLensGroup(deleteStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Catalogazione e analisi dei dati con Inventario S3

Puoi usare Inventario Amazon S3 per gestire lo storage. Ad esempio, puoi utilizzarlo per effettuare l'audit e creare report sullo stato di replica e crittografia degli oggetti per attività, conformità ed esigenze normative. Inventario Amazon S3 può anche semplificare e accelerare flussi di lavoro aziendali e processi con Big Data, fornendo un'alternativa pianificata all'operazione API sincrona

List in Amazon S3. Inventario Amazon S3 non utilizza le operazioni API List per l'audit degli oggetti e non influisce sulla velocità di richiesta del bucket.

Inventario Amazon S3 fornisce file di output con valori separati da virgole (CSV), [Apache Optimized Row Columnar \(ORC\)](#) o [Apache Parquet](#) che elencano gli oggetti e i metadati corrispondenti con frequenza giornaliera o settimanale per un bucket S3 o oggetto con un prefisso condiviso, ovvero oggetti che hanno nomi che iniziano con una stringa comune. Se si imposta un inventario settimanale, un report viene generato ogni domenica (fuso orario UTC) dopo il report iniziale. Per informazioni sui prezzi di Amazon S3 Inventory, consulta [Prezzi di Amazon S3](#).

È possibile configurare diversi elenchi di inventario per un bucket. Quando si configura un elenco di inventario, è possibile specificare quanto segue:

- Quali metadati degli oggetti includere nell'inventario
- Se elencare tutte le versioni degli oggetti o solo le versioni correnti
- Dove archiviare l'output del file dell'elenco di inventario
- Se generare l'inventario su base giornaliera o settimanale
- Se crittografare il file dell'elenco di inventario

Puoi eseguire query su Inventario Amazon S3 con query SQL standard utilizzando [Amazon Athena](#), [Amazon Redshift Spectrum](#) e altri strumenti, come [Presto](#), [Apache Hive](#) e [Apache Spark](#). Per ulteriori informazioni sull'uso di Athena per effettuare query sui file di inventario, consulta [the section called "Esecuzione di query sull'inventario con Athena"](#).

 Note

Amazon S3 potrebbe impiegare fino a 48 ore per fornire il primo report di inventario.

 Note

Dopo aver eliminato una configurazione di inventario, Amazon S3 potrebbe comunque fornire un report di inventario aggiuntivo durante un breve periodo di transizione mentre il sistema elabora l'eliminazione.

Bucket di origine e di destinazione

Il bucket per il quale l'inventario elenca gli oggetti è chiamato bucket di origine. Il bucket nel quale viene archiviato il file dell'elenco di inventario è denominato bucket di destinazione.

Bucket di origine

L'inventario elenca gli oggetti che sono archiviati nel bucket di origine. È possibile ottenere un elenco di inventario per un intero bucket o filtrarlo in base al prefisso del nome della chiave dell'oggetto.

Il bucket di origine:

- Contiene gli oggetti elencati nell'inventario
- Contiene la configurazione per l'inventario

Bucket di destinazione

I file dell'elenco di Amazon S3 Inventory vengono scritti nel bucket di destinazione. Per raggruppare tutti i file di elenco dell'inventario in un percorso comune del bucket di destinazione, puoi specificare un prefisso di destinazione nella configurazione dell'inventario.

Il bucket di destinazione:

- Contiene gli elenchi dei file dell'inventario.
- Contiene i file manifesto che elencano tutti i file dell'inventario che sono archiviati nel bucket di destinazione. Per ulteriori informazioni, consulta [Manifest inventario](#).
- Deve avere una policy del bucket per concedere ad Amazon S3 le autorizzazioni necessarie per verificare la proprietà del bucket e per scrivere file nel bucket.
- Deve trovarsi nello stesso bucket Regione AWS di origine.
- Può coincidere con il bucket di origine.
- Può essere di proprietà di un account Account AWS diverso da quello che possiede il bucket di origine.

Elenco di Amazon S3 Inventory

Un file dell'elenco di inventario contiene un elenco degli oggetti presenti nel bucket di origine e i metadata per ogni oggetto. Un file dell'elenco di inventario viene archiviato nel bucket di destinazione con uno dei seguenti formati:

- Come un file CSV compresso con GZIP
- Come un file in formato ORC (optimized row columnar) Apache compresso con ZLIB
- Come un file Apache Parquet compresso con Snappy

Note

Non è garantito che gli oggetti nei report di Inventario Amazon S3 siano ordinati in qualsiasi ordine.

Un file di elenco di inventario contiene l'elenco degli oggetti presenti nel bucket di origine e i metadata per ogni oggetto elencato. I seguenti campi sono sempre inclusi:

- Bucket Name (Nome bucket): nome del bucket cui è destinato l'inventario.
- Nome chiave: il nome della chiave dell'oggetto (o chiave) che identifica in modo univoco l'oggetto nel bucket. Quando utilizzi il formato di file CSV, il nome della chiave è URL-encoded e deve essere decodificato prima di poterlo utilizzare.

È possibile scegliere di includere nel report i seguenti campi di metadata aggiuntivi:

- ETag: il tag di entità (ETag) è un hash dell'oggetto. L'ETag riflette solo i cambiamenti ai contenuti di un oggetto, non ai suoi metadata. Questo ETag può essere o meno un digest MD5 dei dati oggetto, a seconda di come l'oggetto è stato creato e crittografato. Per ulteriori informazioni, consulta [Object](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).
- Data dell'ultima modifica: la più recente tra la data di creazione dell'oggetto o la data dell'ultima modifica.
- Dimensione: la dimensione dell'oggetto in byte, esclusa la dimensione dei caricamenti incompleti in più parti, dei metadata degli oggetti e dei contrassegni di eliminazione.
- Classe di archiviazione: la classe di archiviazione utilizzata per archiviare l'oggetto. Imposta su STANDARD, REDUCED_REDUNDANCY, STANDARD_IA, ONEZONE_IA, INTELLIGENT_TIERING, GLACIER, o OUTPOSTS GLACIER_IRSNOW, o. EXPRESS_ONEZONE Per ulteriori informazioni, consulta [Comprensione e gestione delle classi di storage Amazon S3](#).
- Algoritmo di checksum: indica l'algoritmo usato per creare il checksum dell'oggetto. Per ulteriori informazioni, consulta [Utilizzo di algoritmi di checksum supportati](#).

- Stato della crittografia: lo stato della crittografia lato server, a seconda del tipo di chiave di crittografia utilizzata: crittografia lato server con chiavi gestite Amazon S3 (`None`), crittografia lato server con (SSE-S3) chiavi (`aws:kms`), crittografia lato server a doppio livello con AWS Key Management Service chiavi (SSE-KMS) o crittografia lato server con AWS KMS chiavi fornite dal cliente (DSSE-KMS). AWS KMS SSE-C Impostata su SSE-S3, SSE-KMS, DSSE-KMS, SSE-C o NOT-SSE. Uno stato di NOT-SSE indica che l'oggetto non è crittografato con crittografia lato server. Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia](#).
- Livello di Intelligent-Tiering accesso S3: livello di accesso (frequente o poco frequente) dell'oggetto se è archiviato nella classe di Intelligent-Tiering storage S3. Impostata su FREQUENT, INFREQUENT, ARCHIVE_INSTANT_ACCESS, ARCHIVE o DEEP_ARCHIVE. Per ulteriori informazioni, consulta [Classe di storage per ottimizzare automaticamente i dati con modelli di accesso variabili o sconosciuti](#).
- Data di fine conservazione del blocco oggetti S3: data fino alla quale l'oggetto bloccato non può essere eliminato. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).
- Modalità di conservazione del blocco oggetti S3: impostata su Governance o Compliance per gli oggetti bloccati. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).
- Stato legale blocco oggetti S3: impostato su On se è stato applicato un blocco di carattere legale a un oggetto, altrimenti su Off. Altrimenti il valore è impostato su Off. Per ulteriori informazioni, consulta [Blocco di oggetti con Object Lock](#).
- ID versione: l'ID versione dell'oggetto. Quando viene attivata la funzione Controllo delle versioni in un bucket, Amazon S3 assegna un numero di versione agli oggetti aggiunti al bucket. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#). (Questo campo non è incluso se l'elenco è configurato unicamente per la versione corrente degli oggetti).
- IsLatest— Impostato su True se l'oggetto è la versione corrente dell'oggetto. (Questo campo non è incluso se l'elenco è configurato unicamente per la versione corrente degli oggetti).
- Contrassegno di eliminazione: impostato su True se l'oggetto è un contrassegno di eliminazione. Per ulteriori informazioni, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#). (Questo campo viene aggiunto automaticamente al report se questo è stato configurato per comprendere tutte le versioni degli oggetti).
- Multipart upload flag (Contrassegno di caricamento in più parti): impostato su True se l'oggetto è stato caricato come caricamento in più parti. Per ulteriori informazioni, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).

- Proprietario dell'oggetto - L'ID utente canonico del proprietario dell'oggetto. Per ulteriori informazioni, consulta [Trova l'ID utente canonico per il tuo AWS account](#) nella Guida di riferimento per la gestione degli AWS account.
- Stato della replica: impostare su PENDING, COMPLETED, FAILED oppure REPLICA. Per ulteriori informazioni, consulta [Ottenimento delle informazioni sullo stato della replica](#).
- Stato delle chiavi bucket S3: impostare su ENABLED o DISABLED. Indica se l'oggetto utilizza una chiave S3 Bucket per. SSE-KMS Per ulteriori informazioni, consulta [Utilizzo di chiavi bucket Amazon S3](#).
- Elenco di controllo dell'accesso agli oggetti: un elenco di controllo degli accessi (ACL) per ogni oggetto che definisce a quale Account AWS o ai gruppi è concesso l'accesso a questo oggetto e il tipo di accesso concesso. Il campo ACL oggetto è definito in formato JSON. Un report Inventario S3 include gli ACL associati agli oggetti nel bucket di origine, anche quando gli ACL sono disabilitati per il bucket. Per ulteriori informazioni, consulta [Utilizzo del campo ACL oggetto](#) e [Panoramica delle liste di controllo accessi \(ACL\)](#).

Note

Il campo ACL oggetto è definito in formato JSON. Un report di inventario visualizza il valore per il campo ACL oggetto come stringa con codifica base64.

Ad esempio, si supponga di avere il seguente campo ACL oggetto in formato JSON:

```
{
  "version": "2022-11-10",
  "status": "AVAILABLE",
  "grants": [{
    "canonicalId": "example-canonical-user-ID",
    "type": "CanonicalUser",
    "permission": "READ"
  }]
}
```

Il campo ACL oggetto è codificato e visualizzato come la seguente stringa con codifica base64:

```
eyJ2ZXJzaW9uIjoiaWoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IktFWQUlMQUMRSIsImdyYW50cyI6IW3siY2Fub25pY2Fs
```

Per ottenere il valore decodificato in JSON per il campo ACL oggetto, puoi eseguire una query su questo campo in Amazon Athena. Per ulteriori esempi di query, consulta [Esecuzione di query sull'inventario Amazon S3 con Amazon Athena](#).

- Data di scadenza del ciclo di vita: impostata sulla data di scadenza del ciclo di vita dell'oggetto. Questo campo verrà compilato solo se l'oggetto deve scadere in base a una regola del ciclo di vita applicabile. In altri casi, il campo sarà vuoto. Gli oggetti con stato di FAILED replica non avranno una data di scadenza specificata, poiché S3 Lifecycle impedisce azioni di scadenza e transizione su questi oggetti fino al completamento della replica. Per ulteriori informazioni, consulta [Oggetti in scadenza](#).

 Note

Quando un oggetto raggiunge la fine del suo ciclo di vita in base alla relativa configurazione, Amazon S3 lo aggiunge alla coda degli oggetti da eliminare e lo rimuove in modo asincrono. Deve pertanto esistere un ritardo tra la data di scadenza dell'oggetto e la data in cui Amazon S3 rimuove tale oggetto. Il report di inventario include gli oggetti scaduti ma non ancora rimossi. Per ulteriori informazioni sulle operazioni di scadenza nel ciclo di vita S3, consulta [Oggetti in scadenza](#).

Di seguito è riportato un esempio di report di inventario con campi di metadati aggiuntivi, composto da quattro record.

amzn-s3-demo-bucket1	example-object-1	EXAMPLEDC81.XJCEN1F7LePaNIIvs001	TRUE
1500	2024-08-15T15:28:26.0004	EXAMPLE21e1518b92f3d92773570f600	STANDARD
FALSE	COMPLETED	SSE-KMS	2025-01-25T15:28:26.000Z
		COMPLIANCE	Off
		ENABLED	
eyJ2ZXJzaW9uIjoiaWoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IktFWQUlMQUMRSIsImdyYW50cyI6W3sicGVybWlzc2l2b2I6IktEXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7000			
amzn-s3-demo-bucket1	example-object-2	EXAMPLEDC81.XJCEN1F7LePaNIIvs002	
TRUE	200	2024-08-21T15:28:26.000Z	EXAMPLE21e1518b92f3d92773570f601
INTELLIGENT_TIERING	FALSE	COMPLETED	SSE-KMS
COMPLIANCE	Off	INFREQUENT	ENABLED
		SHA-256	
eyJ2ZXJzaW9uIjoiaWoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IktFWQUlMQUMRSIsImdyYW50cyI6W3sicGVybWlzc2l2b2I6IktEXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7001			
amzn-s3-demo-bucket1	example-object-3	EXAMPLEDC81.XJCEN1F7LePaNIIvs003	TRUE
12500	2023-01-15T15:28:30.000Z	EXAMPLE21e1518b92f3d92773570f602	STANDARD

Consigliamo di creare una policy del ciclo di vita che elimini i vecchi elenchi di inventario. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#).

L'autorizzazione `s3:PutInventoryConfiguration` consente all'utente di selezionare tutti i campi di metadati elencati in precedenza per ogni oggetto durante la configurazione di un elenco inventario e di specificare il bucket di destinazione in cui archiviare l'inventario. Un utente con accesso in lettura agli oggetti nel bucket di destinazione può accedere a tutti i campi di metadati degli oggetti disponibili nell'elenco inventario. Per limitare l'accesso a un report di inventario, consulta [Concedere autorizzazioni per S3 Inventory e S3 Analytics](#).

Consistenza dell'inventario

In ogni elenco di inventario potrebbero non comparire tutti gli oggetti. L'elenco inventario fornisce l'eventuale consistenza delle richieste PUT (sia di nuovi oggetti che di sovrascritture) e delle richieste DELETE. Ogni elenco di inventario per un bucket è una snapshot degli elementi del bucket. Questi elenchi sono alla fine coerenti (ovvero, un elenco potrebbe non includere oggetti aggiunti o eliminati di recente).

Per convalidare lo stato di un oggetto prima di agire sull'oggetto stesso, consigliamo di effettuare una richiesta REST API `HeadObject` per recuperare i metadati dell'oggetto o controllare le proprietà dell'oggetto nella console di Amazon S3. Puoi anche controllare i metadati degli oggetti con o gli SDKS. AWS CLI AWS Per ulteriori informazioni, consulta [HeadObject](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Per ulteriori informazioni sull'utilizzo di Amazon S3 Inventory, consulta gli argomenti riportati di seguito.

Argomenti

- Configurazione di Amazon S3 Inventory

- [Individuazione dell'elenco inventario](#)
- [Impostazione delle notifiche di eventi Amazon S3 per il completamento dell'inventario](#)
- [Esecuzione di query sull'inventario Amazon S3 con Amazon Athena](#)
- [Convertire stringhe di ID versione vuote nei report Inventario Amazon S3 in stringhe nulle](#)
- [Utilizzo del campo ACL oggetto](#)

Configurazione di Amazon S3 Inventory

Amazon S3 Inventory fornisce un elenco di tipo file flat contenente oggetti e metadati in base a una pianificazione definita. Puoi utilizzare S3 Inventory come alternativa pianificata all'operazione API sincrona `List` di Amazon S3. S3 Inventory fornisce file di output con valori separati da virgole (CSV), in [Apache formato ORC \(Optimized Row Columnar\)](#) o in formato [Apache Parquet \(Parquet\)](#) che elencano gli oggetti e i metadati corrispondenti.

Puoi configurare S3 Inventory per creare elenchi di inventario su base giornaliera o settimanale per un bucket S3 o per oggetti che condividono un prefisso (oggetti con nomi che iniziano con la stessa stringa). Per ulteriori informazioni, consulta [Catalogazione e analisi dei dati con Inventario S3](#).

In questa sezione viene descritto come configurare un inventario inserendo le informazioni sui bucket di origine e destinazione dell'inventario.

Argomenti

- [Panoramica di](#)
- [Creazione di una policy di bucket di destinazione](#)
- [Concessione ad Amazon S3 dell'autorizzazione per l'utilizzo della chiave gestita dal cliente per la crittografia](#)
- [Configurazione dell'inventario utilizzando la console S3](#)
- [Utilizzo di REST API per utilizzare Inventario S3](#)

Panoramica di

Amazon S3 Inventory semplifica la gestione dell'archiviazione tramite la creazione di elenchi di oggetti in un bucket S3 in base a una pianificazione definita. È possibile configurare diversi elenchi di inventario per un bucket. Gli elenchi di inventario sono pubblicati su file CSV, ORC o Parquet in un bucket di destinazione.

Il modo più semplice per configurare un inventario è utilizzare la console Amazon S3, ma puoi anche utilizzare l'API REST di Amazon S3, AWS Command Line Interface (AWS CLI) o gli SDK. AWS La console effettua la prima fase della seguente procedura: l'aggiunta di una policy di bucket al bucket di destinazione.

Per configurare un Amazon S3 Inventory per un bucket S3

1. Aggiungere una policy di bucket per il bucket di destinazione.

È necessario creare una policy del bucket sul bucket di destinazione che conceda le autorizzazioni ad Amazon S3 per scrivere oggetti nel bucket nella posizione definita. Per un esempio di policy, consulta [Concedere autorizzazioni per S3 Inventory e S3 Analytics](#).

2. Configurare un inventario per elencare gli oggetti in un bucket di origine e pubblicare l'elenco su un bucket di destinazione.

Quando si configura un elenco di inventario per un bucket di origine, viene specificato il bucket di destinazione dove si intende archiviare l'elenco, indicando se si vuole generare l'elenco giornalmente o settimanalmente. Si può anche configurare se elencare tutte le versioni dell'oggetto o solo quelle correnti e quali metadati dell'oggetto includere.

Alcuni campi dei metadati degli oggetti nelle configurazioni dei report dell'Inventario S3 sono opzionali, cioè sono disponibili per impostazione predefinita, ma possono essere limitati quando si concede a un utente l'autorizzazione `s3:PutInventoryConfiguration`. È possibile controllare se gli utenti possono includere questi campi di metadati opzionali nei loro report utilizzando la chiave di condizione `s3:InventoryAccessibleOptionalFields`.

Per ulteriori informazioni sui campi di metadati opzionali disponibili in Inventario S3, consulta la sezione [OptionalFields](#) in Riferimento API di Amazon Simple Storage Service. Per ulteriori informazioni sulla limitazione dell'accesso a determinati campi di metadati opzionali in una configurazione dell'inventario, consulta [Controllo della creazione della configurazione dei report di Inventario S3](#).

Puoi specificare che il file dell'elenco di inventario sia crittografato utilizzando la crittografia lato server con una chiave gestita da Amazon S3 (SSE-S3) o una chiave gestita dal cliente (AWS Key Management Service (AWS KMS)). SSE-KMS

 Note

La Chiave gestita da AWS (aws/s3) non è supportata per la SSE-KMS crittografia con S3 Inventory.

Per ulteriori informazioni su SSE-S3 e SSE-KMS, consulta [Protezione dei dati con la crittografia lato server](#). Se intendi utilizzare la SSE-KMS crittografia, consulta il passaggio 3.

- Per informazioni su come utilizzare la console per configurare un elenco inventario, consulta [Configurazione dell'inventario utilizzando la console S3](#).
 - Per utilizzare l'API Amazon S3 per configurare un elenco di inventario, utilizza l'operazione API [PutBucketInventoryConfiguration](#) REST o l'equivalente degli AWS SDK AWS CLI o.
3. Per crittografare il file dell'elenco di inventario con SSE-KMS, concedi ad Amazon S3 il permesso di utilizzare. AWS KMS key

Puoi configurare la crittografia per il file dell'elenco di inventario utilizzando la console Amazon S3, l'API REST di Amazon S3 o AWS gli AWS CLI SDK. Indipendentemente dalla soluzione scelta, devi concedere ad Amazon S3 l'autorizzazione per l'utilizzo della chiave gestita dal cliente per crittografare il file di inventario. Per [fornire ad Amazon S3 l'autorizzazione, modifica la policy della chiave gestita dal cliente](#) che desideri utilizzare per crittografare il file di inventario. Assicurati di aver fornito l'ARN della chiave KMS nella configurazione di Inventario S3 o nelle impostazioni di crittografia del bucket di destinazione. Se non è stato specificato l'ARN della chiave KMS e vengono utilizzate le impostazioni di crittografia predefinite, non potrai accedere al report di Inventario S3.

Il bucket di destinazione in cui è archiviato il file dell'elenco di inventario può essere di proprietà di un Account AWS diverso rispetto all'account che possiede il bucket di origine. Se utilizzi la SSE-KMS crittografia per le operazioni tra account di Amazon S3 Inventory, ti consigliamo di utilizzare una chiave ARN KMS completa quando configuri l'inventario S3. Per ulteriori informazioni, consulta [Utilizzo della SSE-KMS crittografia per le operazioni tra account](#) e [ServerSideEncryptionByDefault](#) nella Documentazione di riferimento delle API Amazon Simple Storage Service.

 Note

Se non riesci ad accedere al rapporto sull'inventario S3, utilizza l'[GetBucketEncryption](#) API e verifica se il bucket di destinazione ha la crittografia predefinita abilitata. SSE-

KMS Se non è stato specificato l'ARN della chiave KMS e vengono utilizzate le impostazioni di crittografia predefinite, non potrai accedere al report di Inventario S3. Per accedere nuovamente ai report di Inventario S3, fornisci l'ARN di una chiave KMS nella configurazione di Inventario S3 o nelle impostazioni di crittografia del bucket di destinazione.

bucket di directory

S3 Inventory è supportato per i bucket di directory. Quando configuri S3 Inventory per un bucket di directory, nota le seguenti differenze:

- Autorizzazioni: per i bucket di directory, è necessario utilizzare le `s3express:GetInventoryConfiguration` autorizzazioni `s3express:PutInventoryConfiguration` and in una policy IAM basata sull'identità anziché in una policy bucket. Queste autorizzazioni utilizzano lo spazio dei nomi anziché lo spazio dei `s3express:` nomi utilizzato per i bucket generici. `s3:` Per ulteriori informazioni, consulta [Autorizzazione delle operazioni API dell'endpoint regionale con IAM](#).
- Campi opzionali supportati: i seguenti campi opzionali sono supportati per i bucket di directory: `Size`, `LastModifiedDate`, `StorageClass`, `ETag`, `IsMultipartUploaded`, `EncryptionStatus`, `BucketKeyStatus`, `ChecksumAlgorithm`, `LifecycleExpirationDate`
- Chiave di condizione: per i bucket di directory, utilizza la chiave di `s3express:InventoryAccessibleOptionalFields` condizione per controllare l'accesso ai campi di metadati opzionali nei report di inventario.

Creazione di una policy di bucket di destinazione

Se crei la configurazione dell'inventario tramite la console Amazon S3, Amazon S3 crea automaticamente una policy di bucket sul bucket di destinazione che concede ad Amazon S3 l'autorizzazione di scrittura. Tuttavia, se crei la configurazione dell'inventario tramite gli AWS SDK o l'AWS CLI API REST di Amazon S3, devi aggiungere manualmente una policy del bucket nel bucket di destinazione. La policy del bucket di destinazione di Inventario S3 consente ad Amazon S3 di scrivere i dati per i report di inventario nel bucket.

Di seguito è riportato un esempio di policy dei bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InventoryExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
      ],
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
        },
        "StringEquals": {
          "aws:SourceAccount": "source-123456789012",
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Per ulteriori informazioni, consulta [Concedere autorizzazioni per S3 Inventory e S3 Analytics](#).

bucket di directory

Per i bucket di directory, è necessario aggiungere manualmente una policy per i bucket di destinazione. La policy dei bucket di destinazione utilizza un'entità di servizio e un formato ARN diversi rispetto ai bucket generici. Specifica `s3express.amazonaws.com` come entità del servizio e utilizza il formato ARN del bucket di directory per il bucket di origine. L'esempio seguente mostra una politica per i bucket di destinazione per i bucket di directory.

```
{
  "Version": "2012-10-17",
```

```

"Statement": [
  {
    "Sid": "InventoryExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "s3express.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": [
      "arn:aws:s3::DOC-EXAMPLE-DESTINATION-BUCKET/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceARN": "arn:aws:s3express:region:source-account-id:bucket/DOC-EXAMPLE-SOURCE-BUCKET--zone-id--x-s3"
      },
      "StringEquals": {
        "aws:SourceAccount": "source-account-id",
        "s3:x-amz-acl": "bucket-owner-full-control"
      }
    }
  }
]
}

```

Se si verifica un errore quando si tenta di creare la policy del bucket, vengono fornite le istruzioni su come correggerlo. Ad esempio, se scegli un bucket di destinazione in un altro Account AWS e non disponi delle autorizzazioni per leggere e scrivere sulla policy del bucket, viene visualizzato un messaggio di errore.

In questo caso, il proprietario del bucket di destinazione deve aggiungere la policy del bucket al bucket di destinazione. Se la policy non viene aggiunta al bucket di destinazione, non si otterrà alcun report di inventario, in quanto Amazon S3 non dispone dell'autorizzazione di scrittura per il bucket di destinazione. Se il bucket di origine è di proprietà di un account diverso da quello dell'utente attuale, l'ID account corretto del proprietario del bucket di origine verrà sostituito nella policy.

Note

Assicurati che non siano state aggiunte istruzioni di rifiuto alla policy del bucket di destinazione che impediscano la consegna dei report di inventario in questo bucket. Per

ulteriori informazioni, consulta [Perché non riesco a generare un report di Inventario Amazon S3?](#)

Concessione ad Amazon S3 dell'autorizzazione per l'utilizzo della chiave gestita dal cliente per la crittografia

Per concedere ad Amazon S3 il permesso di utilizzare la tua AWS Key Management Service (AWS KMS) chiave gestita dal cliente per la crittografia lato server, devi utilizzare una policy chiave. Per aggiornare la policy della chiave in modo da poter utilizzare la chiave gestita dal cliente, completa la procedura seguente.

Per concedere ad Amazon S3 le autorizzazioni per la crittografia utilizzando la chiave gestita dal cliente

1. Utilizzando la chiave gestita dal cliente Account AWS che possiede la chiave gestita dal cliente, accedi a Console di gestione AWS
2. Apri la AWS KMS console all'indirizzo <https://console.aws.amazon.com/kms>.
3. Per modificare il Regione AWS, usa il selettore di regione nell'angolo in alto a destra della pagina.
4. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
5. In Chiavi gestite dal cliente, scegli la chiave gestita dal cliente che desideri utilizzare per crittografare i file inventario.
6. Nella sezione Policy della chiave, scegli Passa alla visualizzazione della policy.
7. Per aggiornare la policy chiave, seleziona Modifica.
8. Nella pagina Modifica policy delle chiavi, aggiungi le seguenti righe alla policy della chiave esistente. Per *source-account-id* e *amzn-s3-demo-source-bucket*, fornisci i valori appropriati per il tuo caso d'uso.

```
{
  "Sid": "Allow Amazon S3 use of the customer managed key",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey"
```

```

    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "source-account-id"
      },
      "ArnLike": {
        "aws:SourceARN": "arn:aws:s3:::amzn-s3-demo-source-bucket"
      }
    }
  }
}

```

9. Scegli Save changes (Salva modifiche).

Per ulteriori informazioni sulla creazione di chiavi gestite dal cliente e sull'utilizzo delle policy delle chiavi, consulta i seguenti collegamenti nella Guida per Developer di AWS Key Management Service :

- [Gestione delle chiavi](#)
- [Politiche chiave in AWS KMS](#)

bucket di directory

Per i bucket di directory, la policy chiave del KMS utilizza un'entità di servizio e un formato ARN di origine diversi rispetto ai bucket generici. Specifica `s3express.amazonaws.com` come principale del servizio e usa il formato ARN del bucket di directory per l'ARN di origine. L'esempio seguente mostra la dichiarazione politica chiave per i bucket di directory.

```

{
  "Sid": "Allow S3 Express use of the KMS key",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3express.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {

```

```
        "aws:SourceAccount": "source-account-id"
      },
      "ArnLike": {
        "aws:SourceARN": "arn:aws:s3express:region:source-account-id:bucket/DOC-EXAMPLE-SOURCE-BUCKET--zone-id--x-s3"
      }
    }
  }
```

Note

Assicurati che non siano state aggiunte istruzioni di rifiuto alla policy del bucket di destinazione che impediscano la consegna dei report di inventario in questo bucket. Per ulteriori informazioni, consulta [Perché non riesco a generare un report di Inventario Amazon S3?](#)

Configurazione dell'inventario utilizzando la console S3

Segui queste istruzioni per configurare l'inventario utilizzando la console S3.

Note

La consegna del primo report di inventario Amazon S3 può richiedere fino a 48 ore.

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.

Note

La configurazione di S3 Inventory per i bucket di directory non è supportata nella console Amazon Simple Storage Service. Per configurare S3 Inventory per i bucket di directory, utilizza l'API REST di Amazon S3, AWS Command Line Interface () o gli SDK.AWS CLI AWS

3. Nell'elenco dei bucket seleziona il nome del bucket per cui desideri configurare Inventario Amazon S3.
4. Scegliere la scheda Management (Gestione),
5. In Configurazioni inventario seleziona Crea configurazione inventario.
6. Specifica un nome in Nome della configurazione dell'inventario.
7. Per Ambito dell'inventario, esegui le operazioni descritte di seguito.
 - Immetti un prefisso facoltativo. Non includere il nome del bucket nel prefisso.
 - Scegli quali versioni dell'oggetto includere, Solo versioni correnti o Includi tutte le versioni.
8. In Dettagli report scegli la posizione dell'account Account AWS in cui desideri salvare i report: Questo account o Un account diverso.
9. In Destinazione, scegli il bucket di destinazione in cui desideri salvare i report di inventario.

Il bucket di destinazione deve coincidere con il bucket per il quale stai configurando l'inventario. Regione AWS Il bucket di destinazione può trovarsi in un diverso Account AWS. Quando specifichi il bucket di destinazione, puoi anche includere un prefisso opzionale per raggruppare insieme i report di inventario.

Nel campo Bucket di destinazione viene visualizzata l'istruzione Autorizzazione del bucket di destinazione che viene aggiunta alla policy del bucket di destinazione per consentire ad Amazon S3 di inserire i dati in tale bucket. Per ulteriori informazioni, consulta [Creazione di una policy di bucket di destinazione](#).

10. In Frequenza, seleziona la frequenza con cui verrà generato il report: Giornaliero o Settimanale.
11. Per Formato di output, scegli uno dei seguenti formati per il report:
 - CSV: se prevedi di utilizzare questo report di inventario con Operazioni in batch S3 o se desideri analizzare questo report in un altro strumento, come Microsoft Excel, scegli CSV.
 - Apache ORC
 - Apache Parquet
12. In Stato seleziona Abilita o Disabilita.
13. Per configurare la crittografia lato server, in Crittografia dei report di inventario, segui la procedura riportata sotto:
 - a. In Server-side crittografia, scegli Non specificare una chiave di crittografia o Specifica una chiave di crittografia per crittografare i dati.

- Per conservare le impostazioni relative ai bucket per la crittografia predefinita degli oggetti lato server durante l'archiviazione in Amazon S3, scegli Non specificare una chiave di crittografia. Finché nella destinazione del bucket sono abilitate le chiavi bucket S3, l'operazione di copia applica la chiave bucket S3 al bucket di destinazione.

 Note

Se la policy del bucket per la destinazione specificata richiede la crittografia degli oggetti prima di archivarli in Amazon S3, è necessario scegliere Specifica una chiave di crittografia. In caso contrario, la copia degli oggetti nella destinazione avrà esito negativo.

- Per crittografare gli oggetti prima di archivarli in Amazon S3, scegli Specifica una chiave di crittografia.
- b. Se hai scelto Specifica una chiave di crittografia, in Tipo di crittografia, devi scegliere la chiave gestita da Amazon S3 (SSE-S3) o la AWS Key Management Service chiave (SSE-KMS).

SSE-S3 utilizza uno dei più potenti cifrari a blocchi: Advanced Encryption Standard (AES) a 256 bit per crittografare ogni oggetto. AES-256 SSE-KMS ti offre un maggiore controllo sulla tua chiave. Per ulteriori informazioni su SSE-S3, vedere [Utilizzo della crittografia lato server con chiavi gestite da Amazon S3 \(SSE-S3\)](#). Per ulteriori informazioni su SSE-KMS, vedere [Utilizzo della crittografia lato server con AWS KMS chiavi \(SSE-KMS\)](#).

 Note

Per crittografare il file dell'elenco di inventario con SSE-KMS, devi concedere ad Amazon S3 l'autorizzazione a utilizzare la chiave gestita dal cliente. Per le istruzioni, consulta la sezione [Concedere ad Amazon S3 l'autorizzazione delle chiavi KMS per la crittografia](#).

- c. Se hai scelto AWS Key Management Service key (SSE-KMS), in AWS KMS key, puoi specificare la tua AWS KMS chiave tramite una delle seguenti opzioni.

 Note

Se il bucket di destinazione che memorizza il file dell'elenco di inventario è di proprietà di un altro Account AWS, assicurati di utilizzare una chiave KMS ARN completa per specificare la tua chiave KMS.

- Per scegliere da un elenco di chiavi KMS disponibili, scegli Scegli tra le tue AWS KMS chiavi e scegli una chiave KMS di crittografia simmetrica dall'elenco delle chiavi disponibili. Assicurati che la chiave KMS sia nella stessa Regione del bucket.

 Note

Nell'elenco vengono visualizzate sia la chiave Chiave gestita da AWS (aws/s3) che quella gestita dal cliente. Tuttavia, la Chiave gestita da AWS (aws/s3) non è supportata per la SSE-KMS crittografia con S3 Inventory.

- Per inserire l'ARN della chiave KMS, scegli Inserisci la AWS KMS chiave ARN e inserisci la tua chiave KMS ARN nel campo visualizzato.
- Per creare una nuova chiave gestita dal cliente nella AWS KMS console, scegli Crea una chiave KMS.

14. Per Campi di metadati aggiuntivi, seleziona una o più delle seguenti opzioni per aggiungere il report di inventario:

- Dimensione: la dimensione dell'oggetto in byte, esclusa la dimensione dei caricamenti incompleti in più parti, dei metadati degli oggetti e dei contrassegni di eliminazione.
- Data dell'ultima modifica: la più recente tra la data di creazione dell'oggetto o la data dell'ultima modifica.
- Caricamento in più parti: specifica che l'oggetto è stato caricato in più parti. Per ulteriori informazioni, consulta [Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3](#).
- Stato di replica: lo stato di replica dell'oggetto. Per ulteriori informazioni, consulta [Ottenimento delle informazioni sullo stato della replica](#).
- Stato crittografia: il tipo di crittografia lato server utilizzata per crittografare l'oggetto. Per ulteriori informazioni, consulta [Protezione dei dati con la crittografia lato server](#).

- Stato della chiave del bucket: indica se una chiave a livello di bucket generata da AWS KMS si applica all'oggetto. Per ulteriori informazioni, consulta [Riduzione dei costi SSE-KMS con Amazon S3 Bucket Keys](#).
- Elenco di controllo dell'accesso agli oggetti: un elenco di controllo degli accessi (ACL) per ogni oggetto che definisce a quali Account AWS gruppi è concesso l'accesso a questo oggetto e il tipo di accesso concesso. Per ulteriori informazioni su questo campo, consulta [Utilizzo del campo ACL oggetto](#). Per ulteriori informazioni sulle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).
- Proprietario dell'oggetto: il proprietario dell'oggetto.
- Classe di archiviazione: la classe di archiviazione utilizzata per archiviare l'oggetto.
- Intelligent-Tiering: Livello di accesso: indica il livello di accesso (frequente o poco frequente) dell'oggetto se è stato archiviato nella classe di archiviazione S3 Intelligent-Tiering . Per ulteriori informazioni, consulta [Classe di storage per ottimizzare automaticamente i dati con modelli di accesso variabili o sconosciuti](#).
- ETag: il tag di entità (ETag) è un hash dell'oggetto. L'ETag riflette solo i cambiamenti ai contenuti di un oggetto, non ai suoi metadati. L'ETag potrebbe o meno essere un digest MD5 dei dati dell'oggetto, a seconda di come l'oggetto è stato creato e crittografato. Per ulteriori informazioni, consulta [Object](#) in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).
- Algoritmo di checksum: indica l'algoritmo usato per creare il checksum dell'oggetto. I valori supportati includono CRC64NVME, CRC32C, SHA1, SHA256, MD5, XXHASH64, XXHASH3, XXHASH128, e SHA512. Per ulteriori informazioni, consulta [Utilizzo di algoritmi di checksum supportati](#).
- Tutte le configurazioni di blocco degli oggetti: lo stato di blocco dell'oggetto, incluse le seguenti impostazioni:
 - Blocco degli oggetti: modalità di conservazione: il livello di protezione applicato all'oggetto, Governance o Conformità.
 - Blocco degli oggetti: mantenere fino alla data: data fino alla quale l'oggetto bloccato non può essere eliminato.
 - Blocco degli oggetti: status della conservazione di carattere legale: lo stato di conservazione ai fini legali dell'oggetto bloccato.

Per ulteriori informazioni sul blocco degli oggetti S3, consulta [Come funziona il blocco oggetti S3](#).

- **Data di scadenza del ciclo di vita:** la data di scadenza del ciclo di vita per gli oggetti nel rapporto sull'inventario. Questo campo verrà compilato solo se l'oggetto deve scadere in base a una regola del ciclo di vita applicabile. In altri casi, il campo sarà vuoto. Per ulteriori informazioni, consulta [Oggetti in scadenza](#).

Per ulteriori informazioni sul contenuto di un report di inventario, consulta [Elenco di Amazon S3 Inventory](#).

Per ulteriori informazioni sulla limitazione dell'accesso a determinati campi di metadati opzionali in una configurazione dell'inventario, consulta [Controllo della creazione della configurazione dei report di Inventario S3](#).

15. Scegli Crea.

Utilizzo di REST API per utilizzare Inventario S3

Di seguito sono riportate le operazioni REST che è possibile utilizzare per lavorare con Inventario Amazon S3.

- [DeleteBucketInventoryConfiguration](#)
- [GetBucketInventoryConfiguration](#)
- [ListBucketInventoryConfigurations](#)
- [PutBucketInventoryConfiguration](#)

Individuazione dell'elenco inventario

Quando viene pubblicato un elenco di inventario, i file manifest vengono pubblicati nel seguente percorso del bucket di destinazione.

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/manifest.json  
destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/  
manifest.checksum  
destination-prefix/amzn-s3-demo-source-bucket/config-ID/hive/dt=YYYY-MM-DD-HH-MM/  
symlink.txt
```

- *destination-prefix* è il prefisso del nome della chiave dell'oggetto specificato facoltativamente nella configurazione dell'inventario. Puoi utilizzare questo prefisso per raggruppare tutti i file dell'elenco di inventario in un percorso comune all'interno del bucket di destinazione.
- *amzn-s3-demo-source-bucket* è il bucket di origine per l'elenco inventario. Il nome del bucket di origine viene aggiunto per evitare conflitti quando più report di inventario provenienti da bucket di origine diversi vengono inviati allo stesso bucket di destinazione.
- *config-ID* viene aggiunto per evitare conflitti con più report di inventario provenienti dallo stesso bucket di origine inviati allo stesso bucket di destinazione. *config-ID* proviene dalla configurazione del report di inventario ed è il nome del report definito durante la configurazione.
- *YYYY-MM-DDTHH-MMZ* è il timestamp composto dall'ora di inizio e dalla data in cui la generazione del report di inventario comincia la scansione del bucket; ad esempio, 2016-11-06T21-32Z.
- *manifest.json* è il file manifest.
- *manifest.checksum* è l'hash MD5 del contenuto del file *manifest.json*.
- *symlink.txt* è il file manifesto compatibile con Apache Hive.

Gli elenchi di inventario vengono pubblicati giornalmente o settimanalmente nel seguente percorso del bucket di destinazione.

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name.csv.gz  
...  
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name-1.csv.gz
```

- *destination-prefix* è il prefisso del nome della chiave dell'oggetto specificato facoltativamente nella configurazione dell'inventario. Puoi utilizzare questo prefisso per raggruppare tutti i file dell'elenco di inventario in un percorso comune nel bucket di destinazione.
- *amzn-s3-demo-source-bucket* è il bucket di origine per l'elenco inventario. Il nome del bucket di origine viene aggiunto per evitare conflitti quando più report di inventario provenienti da bucket di origine diversi vengono inviati allo stesso bucket di destinazione.
- *example-file-name.csv.gz* è uno dei file CSV di inventario. I nomi di inventario ORC terminano con l'estensione del nome di file *.orc*, mentre i nomi di inventario Parquet terminano con l'estensione del nome di file *.parquet*.

Manifest inventario

Nei file `manifest.json` e `symlink.txt` viene descritto dove sono posizionati i file di inventario. Ogni volta che viene distribuito un nuovo elenco di inventario, quest'ultimo è accompagnato da un nuovo set di file `manifest`. Questi file potrebbero sovrascriversi l'un l'altro. Nei bucket con il controllo delle versioni abilitato, Amazon S3 crea nuove versioni dei file `manifest`.

Ogni `manifest` contenuto nel file `manifest.json` fornisce i metadata e altre informazioni di base riguardanti un inventario. Queste informazioni comprendono:

- Il nome del bucket di origine
- Il nome del bucket di destinazione
- La versione dell'inventario
- La creazione del timestamp in formato data epoca (Unix epoch) che è composto dall'ora di inizio e dalla data in cui il processo di generazione del report di inventario comincia la scansione del bucket
- Il formato e lo schema dei file di inventario
- Un elenco dei file di inventario che si trovano nel bucket di destinazione

Ogni volta che viene scritto un file `manifest.json`, questo è accompagnato da un file `manifest.checksum` che è l'hash MD5 del contenuto del file `manifest.json`.

Example Manifesto dell'inventario in un **manifest.json** file

Negli esempi seguenti viene illustrato un manifesto inventario in un file `manifest.json` per gli inventari in formato CSV, ORC e Parquet.

CSV

Di seguito è riportato un esempio di manifesto in un `manifest.json` file per un inventario CSV-formatted

```
{
  "sourceBucket": "amzn-s3-demo-source-bucket",
  "destinationBucket": "arn:aws:s3:::example-inventory-destination-bucket",
  "version": "2016-11-30",
  "creationTimestamp" : "1514944800000",
  "fileFormat": "CSV",
  "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
Size, LastModifiedDate, ETag, StorageClass, IsMultipartUploaded,
```

```

ReplicationStatus, EncryptionStatus, ObjectLockRetainUntilDate, ObjectLockMode,
ObjectLockLegalHoldStatus, IntelligentTieringAccessTier, BucketKeyStatus,
ChecksumAlgorithm, ObjectAccessControlList, ObjectOwner",
  "files": [
    {
      "key": "Inventory/amzn-s3-demo-source-bucket/2016-11-06T21-32Z/
files/939c6d46-85a9-4ba8-87bd-9db705a579ce.csv.gz",
      "size": 2147483647,
      "MD5checksum": "f11166069f1990abeb9c97ace9cdfabc"
    }
  ]
}

```

ORC

Di seguito è riportato un esempio di manifesto in un `manifest.json` file per un ORC-formatted inventario.

```

{
  "sourceBucket": "amzn-s3-demo-source-bucket",
  "destinationBucket": "arn:aws:s3:::example-destination-bucket",
  "version": "2016-11-30",
  "creationTimestamp" : "1514944800000",
  "fileFormat": "ORC",
  "fileSchema":
  "struct<bucket:string,key:string,version_id:string,is_latest:boolean,is_delete_marker:boolean>"
  "files": [
    {
      "key": "inventory/amzn-s3-demo-source-bucket/data/
d794c570-95bb-4271-9128-26023c8b4900.orc",
      "size": 56291,
      "MD5checksum": "5925f4e78e1695c2d020b9f6eexample"
    }
  ]
}

```

Parquet

Di seguito viene riportato un esempio di un manifesto in un file `manifest.json` per un inventario in formato Parquet.

```

{

```



```

"sourceBucket": "amzn-s3-demo-source-bucket",
"destinationBucket": "arn:aws:s3:::example-destination-bucket",
"version": "2016-11-30",
"creationTimestamp" : "1514944800000",
"fileFormat": "Parquet",
"fileSchema": "message s3.inventory { required binary bucket (UTF8);
required binary key (UTF8); optional binary version_id (UTF8); optional boolean
is_latest; optional boolean is_delete_marker; optional int64 size; optional
int64 last_modified_date (TIMESTAMP_MILLIS); optional binary e_tag (UTF8);
optional binary storage_class (UTF8); optional boolean is_multipart_uploaded;
optional binary replication_status (UTF8); optional binary encryption_status
(UTF8); optional int64 object_lock_retain_until_date (TIMESTAMP_MILLIS); optional
binary object_lock_mode (UTF8); optional binary object_lock_legal_hold_status
(UTF8); optional binary intelligent_tiering_access_tier (UTF8); optional binary
bucket_key_status (UTF8); optional binary checksum_algorithm (UTF8); optional
binary object_access_control_list (UTF8); optional binary object_owner (UTF8);}",
  "files": [
    {
      "key": "inventory/amzn-s3-demo-source-bucket/data/
d754c470-85bb-4255-9218-47023c8b4910.parquet",
      "size": 56291,
      "MD5checksum": "5825f2e18e1695c2d030b9f6eexample"
    }
  ]
}

```

Il file `symlink.txt` è un file manifesto compatibile con Apache Hive che consente a Hive di scoprire automaticamente i file di inventario e i relativi file di dati. Il manifest compatibile con Hive funziona con i servizi compatibili con Hive Athena e Amazon Redshift Spectrum. Funziona anche con applicazioni compatibili con Hive, incluse [Presto](#), [Apache Hive](#), [Apache Spark](#) e molte altre.

Important

Il file manifesto compatibile con `symlink.txt` Apache Hive attualmente non può essere utilizzato con AWS Glue.

La lettura del file `symlink.txt` con [Apache Hive](#) e [Apache Spark](#) non è supportata per i file di inventario in formato ORC e Parquet.

Impostazione delle notifiche di eventi Amazon S3 per il completamento dell'inventario

Puoi configurare una notifica di eventi Amazon S3 per ricevere una notifica quando viene creato il file checksum manifest, che indica che è stato aggiunto un elenco di inventario al bucket di destinazione. Il manifest è un elenco aggiornato di tutti gli elenchi di inventario nel percorso di destinazione.

Amazon S3 può pubblicare eventi in un argomento Amazon Simple Notification Service (Amazon SNS), una coda Amazon Simple Queue Service (Amazon SQS) o una funzione AWS Lambda . Per ulteriori informazioni, consulta [Notifiche di eventi Amazon S3](#).

La seguente configurazione di notifica definisce che tutti i file `manifest.checksum` recentemente aggiunti al bucket di destinazione sono elaborati da AWS Lambda `cloud-function-list-write`.

```
<NotificationConfiguration>
  <QueueConfiguration>
    <Id>1</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>destination-prefix/source-bucket</Value>
        </FilterRule>
        <FilterRule>
          <Name>suffix</Name>
          <Value>checksum</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <CloudFunction>arn:aws:lambda:us-west-2:222233334444:cloud-function-list-write</CloudFunction>
    <Event>s3:ObjectCreated:*</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

Per ulteriori informazioni, consulta [Using AWS Lambda with Amazon S3](#) nella AWS Lambda Developer Guide.

Esecuzione di query sull'inventario Amazon S3 con Amazon Athena

Puoi eseguire una query sui file di Inventario Amazon S3 con query SQL standard utilizzando Amazon Athena in tutte le regioni in cui Athena è disponibile. Per verificare Regione AWS la disponibilità, consulta la [Regione AWS tabella](#).

Athena può eseguire query sui file di Inventario Amazon S3 in formato [ORC \(optimized row columnar\) Apache](#), [Apache Parquet](#) o in formato CSV. Per una migliore velocità di interrogazione e costi inferiori, utilizza ORC-formatted file Parquet di inventario in formato OR. ORC e Parquet sono formati di file colonnari progettati per. [Apache Hadoop](#) Il formato colonnare permette al lettore di leggere, decomprimere ed elaborare solo le colonne necessarie per la query in corso. L'ORC e i Parquet formati per Amazon S3 Inventory sono disponibili in tutti. Regioni AWS

Come utilizzare Athena per eseguire query sui file di Inventario Amazon S3

1. Creare una tabella Athena. Per informazioni sulla creazione di una tabella, consultare [Creazione di tabelle in Amazon Athena](#) nella Guida per l'utente di Amazon Athena.
2. Crea la tua richiesta utilizzando uno dei seguenti modelli di query di esempio, a seconda che tu stia interrogando un ORC-formatted, a o un CSV-formatted rapporto Parquet-formatted di inventario.
 - Quando utilizzi Athena per interrogare un rapporto sull' ORC-formatted inventario, utilizza la seguente query di esempio come modello.

La seguente query di esempio include tutti i campi opzionali in un rapporto sull' ORC-formatted inventario.

Per utilizzare questa query di esempio, effettua le seguenti operazioni:

- Sostituisci *your_table_name* con il nome della tabella Athena creata.
- Rimuovi gli eventuali campi opzionali che non hai scelto per l'inventario in modo che la query corrisponda ai campi scelti.
- Sostituisci il nome del bucket e la posizione dell'inventario seguenti (l'ID configurazione) come appropriato in base alla configurazione.

```
s3://amzn-s3-demo-bucket/config-ID/hive/
```

- Sostituisci la data *2022-01-01-00-00* in `projection.dt.range` con il primo giorno dell'intervallo di tempo entro il quale esegui la partizione dei dati in Athena. Per ulteriori informazioni, consulta [Partizionamento dei dati in Athena](#).

```

CREATE EXTERNAL TABLE your_table_name (
    bucket string,
    key string,
    version_id string,
    is_latest boolean,
    is_delete_marker boolean,
    size bigint,
    last_modified_date timestamp,
    e_tag string,
    storage_class string,
    is_multipart_uploaded boolean,
    replication_status string,
    encryption_status string,
    object_lock_retain_until_date bigint,
    object_lock_mode string,
    object_lock_legal_hold_status string,
    intelligent_tiering_access_tier string,
    bucket_key_status string,
    checksum_algorithm string,
    object_access_control_list string,
    object_owner string,
    lifecycle_expiration_date timestamp
) PARTITIONED BY (
    dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive ql.io.orc.OrcSerde'
STORED AS INPUTFORMAT 'org.apache.hadoop.hive ql.io.SymlinkTextInputFormat'
OUTPUTFORMAT 'org.apache.hadoop.hive ql.io.IgnoreKeyTextOutputFormat'
LOCATION 's3://amzn-s3-demo-bucket/config-ID/hive/'
TBLPROPERTIES (
    "projection.enabled" = "true",
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
    "projection.dt.range" = "2022-01-01-00-00,NOW",
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
);

```

- Quando usi Athena per interrogare un rapporto Parquet di inventario formattato, utilizza la query di esempio per un rapporto. ORC-formatted Tuttavia, utilizza quanto segue al posto dell'ORC Parquet SerDe SerDe nella dichiarazione. ROW FORMAT SERDE

```
ROW FORMAT SERDE 'org.apache.hadoop.hive ql.io.parquet.serde.ParquetHiveSerDe'
```

- Quando utilizzi Athena per interrogare un rapporto sull' CSV-formatted inventario, utilizza la seguente query di esempio come modello.

La seguente query di esempio include tutti i campi opzionali in un rapporto sull' CSV-formatted inventario.

Per utilizzare questa query di esempio, effettua le seguenti operazioni:

- Sostituisci *your_table_name* con il nome della tabella Athena creata.
- Rimuovi gli eventuali campi opzionali che non hai scelto per l'inventario in modo che la query corrisponda ai campi scelti.
- Sostituisci il nome del bucket e la posizione dell'inventario seguenti (l'ID configurazione) come appropriato in base alla configurazione.

s3://amzn-s3-demo-bucket/config-ID/hive/

- Sostituisci la data *2022-01-01-00-00* in `projection.dt.range` con il primo giorno dell'intervallo di tempo entro il quale esegui la partizione dei dati in Athena. Per ulteriori informazioni, consulta [Partizionamento dei dati in Athena](#).

```
CREATE EXTERNAL TABLE your_table_name (  
    bucket string,  
    key string,  
    version_id string,  
    is_latest boolean,  
    is_delete_marker boolean,  
    size string,  
    last_modified_date string,  
    e_tag string,  
    storage_class string,  
    is_multipart_uploaded boolean,  
    replication_status string,  
    encryption_status string,  
    object_lock_retain_until_date string,  
    object_lock_mode string,  
    object_lock_legal_hold_status string,  
    intelligent_tiering_access_tier string,  
    bucket_key_status string,  
    checksum_algorithm string,
```

```

        object_access_control_list string,
        object_owner string,
        lifecycle_expiration_date string
    ) PARTITIONED BY (
        dt string
    )
    ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.OpenCSVSerde'
    STORED AS INPUTFORMAT 'org.apache.hadoop.hive ql.io.SymlinkTextInputFormat'
    OUTPUTFORMAT 'org.apache.hadoop.hive ql.io.IgnoreKeyTextOutputFormat'
    LOCATION 's3://amzn-s3-demo-bucket/config-ID/hive/'
    TBLPROPERTIES (
        "projection.enabled" = "true",
        "projection.dt.type" = "date",
        "projection.dt.format" = "yyyy-MM-dd-HH-mm",
        "projection.dt.range" = "2022-01-01-00-00,NOW",
        "projection.dt.interval" = "1",
        "projection.dt.interval.unit" = "HOURS"
    );

```

3. Ora puoi eseguire diverse query sull'inventario, come illustrato negli esempi seguenti. Sostituisci ogni *user input placeholder* con le tue informazioni.

```

# Get a list of the latest inventory report dates available.
SELECT DISTINCT dt FROM your_table_name ORDER BY 1 DESC limit 10;

# Get the encryption status for a provided report date.
SELECT encryption_status, count(*) FROM your_table_name WHERE dt = 'YYYY-MM-DD-HH-MM' GROUP BY encryption_status;

# Get the encryption status for inventory report dates in the provided range.
SELECT dt, encryption_status, count(*) FROM your_table_name
WHERE dt > 'YYYY-MM-DD-HH-MM' AND dt < 'YYYY-MM-DD-HH-MM' GROUP BY dt,
    encryption_status;

```

Quando configuri S3 Inventory per aggiungere il campo Elenco di controllo di accesso dell'oggetto (ACL) a un report di inventario, il report visualizza il valore per il campo ACL oggetto come una stringa con codifica base64. Per ottenere il valore decodificato in JSON per il campo ACL oggetto, puoi eseguire una query su questo campo utilizzando Athena. Fare riferimento agli esempi di query riportati di seguito. Per ulteriori informazioni sul campo ACL oggetto, consulta [Utilizzo del campo ACL oggetto](#).

```

# Get the S3 keys that have Object ACL grants with public access.

```

```

WITH grants AS (
    SELECT key,
           CAST(
               json_extract(from_utf8(from_base64(object_access_control_list)),
               '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
           ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'uri') = 'http://acs.amazonaws.com/groups/global/AllUsers'

```

```

# Get the S3 keys that have Object ACL grantees in addition to the object owner.
WITH grants AS
    (SELECT key,
     from_utf8(from_base64(object_access_control_list)) AS
     object_access_control_list,
     object_owner,
     CAST(json_extract(from_utf8(from_base64(object_access_control_list)),
     '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))) AS grants_array
    FROM your_table_name)
SELECT key,
       grant,
       objectowner
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE cardinality(grants_array) > 1 AND element_at(grant, 'canonicalId') !=
    object_owner;

```

```

# Get the S3 keys with READ permission that is granted in the Object ACL.
WITH grants AS (
    SELECT key,
           CAST(
               json_extract(from_utf8(from_base64(object_access_control_list)),
               '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
           ) AS grants_array
    FROM your_table_name
)
SELECT key,

```

```
    grants_array,  
    grant  
FROM grants, UNNEST(grants_array) AS t(grant)  
WHERE element_at(grant, 'permission') = 'READ';
```

```
# Get the S3 keys that have Object ACL grants to a specific canonical user ID.  
WITH grants AS (  
    SELECT key,  
        CAST(  
            json_extract(from_utf8(from_base64(object_access_control_list)),  
                '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))  
        ) AS grants_array  
    FROM your_table_name  
)  
SELECT key,  
    grants_array,  
    grant  
FROM grants, UNNEST(grants_array) AS t(grant)  
WHERE element_at(grant, 'canonicalId') = 'user-canonical-id';
```

```
# Get the number of grantees on the Object ACL.  
SELECT key,  
    object_access_control_list,  
    json_array_length(json_extract(object_access_control_list, '$.grants')) AS  
    grants_count  
FROM your_table_name;
```

Per ulteriori informazioni sull'utilizzo di Athena, consulta la [Guida per l'utente di Amazon Athena](#).

Convertire stringhe di ID versione vuote nei report Inventario Amazon S3 in stringhe nulle

Note

La procedura seguente si applica solo ai report di Amazon S3 Inventory che includono tutte le versioni e solo se i report "tutte le versioni" vengono utilizzati come manifest per S3 Batch

Operations su bucket che hanno il Controllo versioni S3 abilitato. Inoltre, non è necessario convertire stringhe per i report di inventario S3 che specificano solo la versione corrente.

Puoi utilizzare i report di S3 Inventory come manifest per S3 Batch Operations. Tuttavia, quando Controllo versioni S3 è abilitato su un bucket, i report di S3 Inventory che includono tutte le versioni contrassegnano gli oggetti con versione nulla con stringhe vuote nel campo ID versione. Quando un report di Inventory include tutti gli ID versione degli oggetti, Batch Operations riconosce le stringhe `null` come ID di versione ma non le stringhe vuote.

Quando un processo di S3 Batch Operations utilizza come manifest un report "tutte le versioni" di S3 Inventory, non riuscirà a portare a termine tutte le attività sugli oggetti con una stringa vuota nel campo ID versione. Per convertire stringhe vuote nel campo ID versione del report S3 Inventory in stringhe `null` per Batch Operations, attenersi alla procedura seguente.

Aggiorna un report di Amazon S3 Inventory da utilizzare con Batch Operations

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Vai al report di Inventario S3. Il report dell'inventario si trova nel bucket di destinazione specificato durante la configurazione del report dell'inventario. Per ulteriori informazioni sull'individuazione dei report di inventario, consulta [Individuazione dell'elenco inventario](#).
 - a. Scegliere il nome del bucket di destinazione.
 - b. Scegliere la cartella . La cartella prende il nome dal bucket della fonte d'origine.
 - c. Scegli la cartella che prende il nome dalla configurazione di inventario.
 - d. Seleziona la casella di spunta accanto alla cartella denominata hive. Scegli Copia URI S3 per copiare l'URI S3 per la cartella.
3. Apri la console Amazon Athena all'indirizzo. <https://console.aws.amazon.com/athena/>
4. Nell'editor di query, scegli Impostazioni, quindi seleziona Gestisci. Alla pagina Gestisci impostazioni per Posizione del risultato della query, scegli un bucket S3 in cui archiviare i risultati della query.
5. Nell'editor di query, creare una tabella Athena per conservare i dati nel report di inventario utilizzando il seguente comando. Sostituisci *table_name* con un nome a scelta e nella clausola LOCATION, inserisci l'URI S3 copiato in precedenza. Quindi scegli Esegui per eseguire la query.

```
CREATE EXTERNAL TABLE table_name(bucket string, key string,
  version_id string) PARTITIONED BY (dt string)ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.OpenCSVSerde'STORED AS INPUTFORMAT
  'org.apache.hadoop.hive.q1.io.SymLinkTextInputFormat' OUTPUTFORMAT
  'org.apache.hadoop.hive.q1.io.IgnoreKeyTextOutputFormat' LOCATION 'Copied S3 URI';
```

6. Per cancellare l'editor di query, scegli Cancella. Quindi, caricare il report di inventario nella tabella utilizzando il comando seguente. Sostituisci il codice *table_name* con quello che hai scelto nella fase precedente. Quindi scegli Esegui per eseguire la query.

```
MSCK REPAIR TABLE table_name;
```

7. Per cancellare l'editor di query, scegli Cancella. Esegui la seguente query SELECT per recuperare tutte le voci nel report di inventario originale e sostituire qualsiasi ID versione vuota con le stringhe null. Sostituisci il codice *table_name* con quello che hai scelto in precedenza e sostituisci *YYYY-MM-DD-HH-MM* nella clausola WHERE con la data del report di inventario su cui eseguire questo strumento. Quindi scegli Esegui per eseguire la query.

```
SELECT bucket as Bucket, key as Key, CASE WHEN version_id = '' THEN 'null' ELSE
  version_id END as VersionId FROM table_name WHERE dt = 'YYYY-MM-DD-HH-MM';
```

8. Torna alla console Amazon S3 (<https://console.aws.amazon.com/s3/>) e vai al bucket S3 che hai scelto in precedenza per Location of query result. All'interno, è presente una serie di cartelle che terminano con la data.

Ad esempio, dovresti vedere qualcosa come *s3://amzn-s3-demo-bucket.query-result-location* Unsaved/2021/10/07 Dovrebbe essere possibile visualizzare i file .csv contenenti i risultati della query SELECT che hai eseguito.

Scegli il file CSV con la data di modifica più recente. Scarica questo file sul tuo computer locale per il passaggio successivo.

9. Il file CSV generato contiene una riga di intestazione. Per utilizzare questo file CSV come input per un processo S3 Batch Operations, è necessario rimuovere la riga di intestazione, poiché Batch Operations non supporta le righe di intestazione nei manifest CSV.

Per rimuovere la riga di intestazione, è possibile eseguire uno dei seguenti comandi sul file. Sostituisci *file.csv* con il nome del tuo file CSV.

Per macchine macOS e Linux, eseguire il comando `tail` in una finestra Terminal.

```
tail -n +2 file.csv > tmp.csv && mv tmp.csv file.csv
```

Per le macchine Windows, esegui il seguente script in una PowerShell finestra di Windows. Sostituire *File-location* con il percorso al file e *file.csv* con il nome del file.

```
$ins = New-Object System.IO.StreamReader File-location\file.csv
$out = New-Object System.IO.StreamWriter File-location\temp.csv
try {
    $skip = 0
    while ( !$ins.EndOfStream ) {
        $line = $ins.ReadLine();
        if ( $skip -ne 0 ) {
            $out.WriteLine($line);
        } else {
            $skip = 1
        }
    }
} finally {
    $out.Close();
    $ins.Close();
}
Move-Item File-location\temp.csv File-location\file.csv -Force
```

10. Dopo aver rimosso la riga di intestazione dal file CSV, è possibile utilizzarla come manifest in un processo di S3 Batch Operations. Carica il file CSV in un bucket S3 o in una posizione a tua scelta, quindi crea un processo Batch Operations utilizzando il file CSV come manifest.

Per ulteriori informazioni sulla creazione di un processo di Batch Operations, consulta [Creazione di un processo di operazioni in batch S3](#).

Utilizzo del campo ACL oggetto

Un report Inventario Amazon S3 contiene un elenco degli oggetti presenti nel bucket di origine S3 e i metadata per ogni oggetto. Il campo Elenco di controllo di accesso dell'oggetto (ACL) è un campo di metadata disponibile in Inventario Amazon S3. In particolare, il campo ACL oggetto contiene la lista di controllo degli accessi (ACL) per ciascun oggetto. L'ACL per un oggetto definisce a quale Account AWS o ai gruppi è concesso l'accesso a questo oggetto e il tipo di accesso concesso. Per ulteriori informazioni, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#) e [Elenco di Amazon S3 Inventory](#).

Il campo ACL oggetto nei report di Inventario Amazon S3 è definito in formato JSON. I dati JSON includono i seguenti campi:

- **version**: la versione del formato del campo ACL oggetto nei report di inventario. È in formato data yyyy-mm-dd.
- **status**: i valori possibili sono AVAILABLE o UNAVAILABLE per indicare se un ACL oggetto ACL è disponibile per un oggetto. Quando lo stato dell'ACL oggetto è UNAVAILABLE, il valore del campo Proprietario dell'oggetto nel report di inventario è anche UNAVAILABLE.
- **grants**— Grantee-permission coppie che elencano lo stato di autorizzazione di ciascun beneficiario concesso dall'ACL dell'oggetto. I valori disponibili per un assegnatario sono CanonicalUser e Group. Per ulteriori informazioni sugli assegnatari, consulta [Assegnatari nelle liste di controllo degli accessi](#).

Per un assegnatario con il tipo Group, una coppia autorizzata dall'assegnatario include i seguenti attributi:

- **uri**: un gruppo Amazon S3 predefinito.
- **permission**: le autorizzazioni ACL che vengono concesse sull'oggetto. Per ulteriori informazioni, consulta [Autorizzazioni ACL su un oggetto](#).
- **type**: il tipoGroup, che denota che l'assegnatario è un gruppo.

Per un assegnatario con il tipo CanonicalUser, una coppia autorizzata dall'assegnatario include i seguenti attributi:

- **canonicalId**: una forma offuscata dell'ID Account AWS . L'ID utente canonico di un Account AWS è specifico per quell'account. È possibile recuperare l'ID utente canonico. Per ulteriori informazioni, consulta [Trovare l'ID utente canonico per il proprio Account AWS](#) nella Guida di riferimento per la gestione degli account AWS .
- **permission**: le autorizzazioni ACL che vengono concesse sull'oggetto. Per ulteriori informazioni, consulta [Autorizzazioni ACL su un oggetto](#).
- **type**— Il tipoCanonicalUser, che indica che il beneficiario è un Account AWS

L'esempio seguente mostra i possibili valori per il campo ACL oggetto in formato JSON:

```
{
  "version": "2022-11-10",
  "status": "AVAILABLE",
  "grants": [{
```

```

    "uri": "http://acs.amazonaws.com/groups/global/AllUsers",
    "permission": "READ",
    "type": "Group"
  }, {
    "canonicalId": "example-canonical-id",
    "permission": "FULL_CONTROL",
    "type": "CanonicalUser"
  }]
}

```

Note

Il campo ACL oggetto è definito in formato JSON. Un report di inventario visualizza il valore per il campo ACL oggetto come stringa con codifica base64.

Ad esempio, si supponga di avere il seguente campo ACL oggetto in formato JSON:

```

{
  "version": "2022-11-10",
  "status": "AVAILABLE",
  "grants": [{
    "canonicalId": "example-canonical-user-ID",
    "type": "CanonicalUser",
    "permission": "READ"
  }]
}

```

Il campo ACL oggetto è codificato e visualizzato come la seguente stringa con codifica base64:

```
eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIzInN0YXR1cyI6IkFWQU1MQUMRSIsImdyYW50cyI6W3siY2Fub25pY2FsSw
```

Per ottenere il valore decodificato in JSON per il campo ACL oggetto, puoi eseguire una query su questo campo in Amazon Athena. Per ulteriori esempi di query, consulta [Esecuzione di query sull'inventario Amazon S3 con Amazon Athena](#).

Best practice e modelli di progettazione: ottimizzazione delle prestazioni di Amazon S3

Le applicazioni possono facilmente raggiungere migliaia di transazioni al secondo come prestazioni delle richieste durante il caricamento e il recupero di risorse di storage da Amazon S3. Amazon S3 si ridimensiona automaticamente fino a tassi di richiesta elevati. Ad esempio, la tua applicazione può ottenere almeno 3.500 PUT/COPY/POST/DELETE o 5.500 GET/HEAD richieste al secondo per prefisso Amazon S3 partizionato. Non esistono limiti al numero di prefissi in un bucket. Puoi migliorare le prestazioni in lettura o scrittura utilizzando la parallelizzazione. Ad esempio, se si creano 10 prefissi in un bucket Amazon S3 per parallelizzare le letture, è possibile scalare le prestazioni di lettura a 55.000 richieste di lettura al secondo. Allo stesso modo, è possibile ridimensionare le operazioni di scrittura scrivendo su più prefissi. Nelle operazioni di lettura e scrittura il dimensionamento avviene gradualmente, non è istantaneo, e le prestazioni effettive variano in base alle caratteristiche specifiche del carico di lavoro, ai modelli di utilizzo e alla configurazione del sistema. Sebbene Amazon S3 stia eseguendo il dimensionamento alla nuova frequenza di richieste più elevata, si potrebbero verificare alcuni errori 503 (Slow Down). Questi errori scompariranno al termine del ridimensionamento. Per ulteriori informazioni sulla creazione e sull'utilizzo dei prefissi, consulta [Organizzazione degli oggetti utilizzando i prefissi](#).

Alcune applicazioni di data lake in Amazon S3 analizzano milioni o miliardi di oggetti per query eseguite su diversi petabyte di dati. Queste applicazioni di data lake raggiungono velocità di trasferimento a singola istanza che massimizzano l'uso dell'interfaccia di rete per l'istanza [Amazon EC2, che può arrivare fino a 100 su una singola](#) istanza. Gb/s Queste applicazioni poi aggregano throughput su più istanze per ottenere diversi terabit al secondo.

Altre applicazioni sono sensibili alla latenza, come le applicazioni di messaggistica sui social media. Tali applicazioni possono raggiungere latenze coerenti per oggetti di piccole dimensioni (e latenze al primo byte in uscita per oggetti più grandi) di circa 100–200 millisecondi.

Altri AWS servizi possono inoltre contribuire ad accelerare le prestazioni per diverse architetture applicative. Ad esempio, se desideri velocità di trasferimento più elevate su una singola connessione HTTP o latenze di millisecondi a una cifra, usa [Amazon o Amazon per la memorizzazione nella cache con Amazon CloudFront](#) S3. [ElastiCache](#)

Inoltre, se desideri trasferimenti dei dati veloci su lunghe distanze tra un client e un bucket S3, utilizza [Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#). Transfer

Acceleration utilizza le edge location distribuite a livello globale per accelerare il trasporto dei dati su distanze geografiche. CloudFront Se il tuo carico di lavoro Amazon S3 utilizza la crittografia lato server con AWS KMS, consulta [AWS KMS Limits](#) nella AWS Key Management Service Developer Guide per informazioni sulle tariffe di richiesta supportate per il tuo caso d'uso.

Gli argomenti seguenti presentano le linee guida e i modelli di progettazione per le best practice per ottimizzare le prestazioni per le applicazioni che utilizzano Amazon S3. Per le informazioni più aggiornate sull'ottimizzazione delle prestazioni per Amazon S3, consulta [Linee guida per le prestazioni di Amazon S3](#) e [Modelli di progettazione delle prestazioni per Amazon S3](#).

Note

Per ulteriori informazioni sull'utilizzo della classe di archiviazione Amazon S3 Express One Zone con bucket di directory, consulta [S3 Express One Zone](#) e [Operazioni con i bucket di directory](#).

Argomenti

- [Linee guida per le prestazioni di Amazon S3](#)
- [Modelli di progettazione delle prestazioni per Amazon S3](#)

Linee guida per le prestazioni di Amazon S3

Per sviluppare applicazioni che caricano e recuperano oggetti da Amazon S3, segui le nostre linee guida sulle best practice per ottimizzare le prestazioni. Offriamo anche [Modelli di progettazione delle prestazioni per Amazon S3](#) più dettagliati.

Per ottenere prestazioni ottimali per le applicazioni su Amazon S3, consigliamo di adottare le linee guida seguenti.

Argomenti

- [Misurare le prestazioni](#)
- [Scalare orizzontalmente le connessioni di archiviazione](#)
- [Utilizza i recuperi con intervallo di byte](#)

- [Nuovi tentativi di richieste per applicazioni sensibili alla latenza](#)
- [Combina Amazon S3 \(storage\) e Amazon EC2 \(elaborazione\) nello stesso Regione AWS](#)
- [Utilizza Amazon S3 Transfer Acceleration per ridurre al minimo la latenza causata dalla distanza](#)
- [Usa la versione più recente di AWS SDK](#)

Misurare le prestazioni

Quando ottimizzi le prestazioni, devi verificare i requisiti che riguardano il throughput della rete, la CPU e la DRAM. A seconda della combinazione di esigenze per queste risorse diverse, può essere utile valutare più tipi di istanza [Amazon EC2](#). Per ulteriori informazioni sui tipi di istanza, consulta [Tipi di istanza](#) nella Guida dell'utente di Amazon EC2.

Durante la misurazione delle prestazioni, è utile anche verificare i tempi, la latenza e la velocità del trasferimento dei dati DNS utilizzando strumenti di analisi HTTP.

Per comprendere i requisiti relativi alle prestazioni e ottimizzare le prestazioni dell'applicazione, puoi anche monitorare le risposte di errore 503 che ricevi. Il monitoraggio di determinate metriche delle prestazioni può comportare spese aggiuntive. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Monitoraggio del numero di risposte all'errore di stato 503 (Rallentamento)

Per monitorare il numero di risposte all'errore di stato 503 che ricevi, puoi utilizzare una delle seguenti opzioni:

- Usa le metriche delle CloudWatch richieste di Amazon per Amazon S3. Le metriche delle CloudWatch richieste includono una metrica per le risposte sullo stato 5xx. Per ulteriori informazioni sui parametri di richiesta di CloudWatch , consulta [Metriche di monitoraggio con Amazon CloudWatch](#).
- Utilizza il conteggio dell'errore 503 (Servizio non disponibile) disponibile nella sezione delle metriche avanzate di Amazon S3 Storage Lens. Per ulteriori informazioni, consulta [Utilizzo dei parametri di S3 Storage Lens per migliorare le prestazioni](#).
- Utilizza la registrazione degli accessi al server Amazon S3 Con la registrazione degli accessi al server, puoi filtrare ed esaminare tutte le richieste che ricevono risposte 503 (Errore interno). Puoi anche utilizzare Amazon Athena per analizzare i log. Per ulteriori informazioni sulla registrazione degli accessi al server, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#).

Monitorando il numero del codice di errore di stato HTTP 503, spesso puoi ottenere informazioni dettagliate preziose su quali prefissi, chiavi o bucket ricevono il maggior numero di richieste di limitazione (della larghezza di banda della rete).

Scalare orizzontalmente le connessioni di archiviazione

Distribuire le richieste su più connessioni è uno schema di progettazione comune per scalare orizzontalmente le prestazioni. Se devi creare applicazioni ad alte prestazioni, pensa ad Amazon S3 come un sistema distribuito di dimensioni molto grandi, non un singolo endpoint di rete come un server di storage tradizionale. Puoi ottenere prestazioni ottimali inviando più richieste simultanee ad Amazon S3. Distribuisci queste richieste su connessioni separate per massimizzare la larghezza di banda accessibile da Amazon S3. Amazon S3 non impone limiti al numero di connessioni effettuate al bucket.

Utilizza i recuperi con intervallo di byte

Utilizzando l'intestazione HTTP Range in una richiesta [GET Object](#), puoi recuperare un intervallo di byte da un oggetto, trasferendo solo la parte specificata. Puoi utilizzare connessioni simultanee ad Amazon S3 per recuperare diversi intervalli di byte all'interno dello stesso oggetto. Questa operazione ti permette di ottenere un throughput aggregato superiore rispetto a una singola richiesta whole-object. Recuperare range minori da oggetti più grandi permette inoltre alla tua applicazione di migliorare i tempi di ripetizione quando le richieste sono interrotte. Per ulteriori informazioni, consulta [Download di oggetti](#).

Se gli oggetti sono oggetti PUT che utilizzano un caricamento in più parti, è buona pratica trasformarli in oggetti GET nelle stesse dimensioni della parte (o almeno allineati ai limiti della parte) per ottenere le prestazioni migliori. Le richieste GET possono rivolgersi direttamente alle singole parti; ad esempio, GET ?partNumber=N.

Nuovi tentativi di richieste per applicazioni sensibili alla latenza

I timeout e i tentativi aggressivi aiutano a mantenere la latenza uniforme. Poiché Amazon S3 opera su vasta scala, se la prima richiesta è lenta, un nuovo tentativo di richiesta adotterà un percorso diverso e riuscirà rapidamente. Gli AWS SDK hanno valori di timeout e ripetizione configurabili che puoi adattare alle tolleranze della tua specifica applicazione.

Combina Amazon S3 (storage) e Amazon EC2 (elaborazione) nello stesso Regione AWS

Sebbene i nomi dei bucket S3 siano univoci a livello globale, ogni bucket viene archiviato in una regione che sceglierai durante la creazione del bucket stesso. Per saperne di più sulle linee guida per la denominazione dei bucket, consulta [Panoramica sui bucket](#) e [Regole di denominazione dei bucket](#). Per ottimizzare le prestazioni, ti consigliamo di accedere al bucket dalle istanze Amazon EC2 nelle stesse istanze, quando possibile. Regione AWS Questa operazione permette di ridurre la latenza e i costi di trasferimento dei dati.

Per ulteriori informazioni sui costi di trasferimento dei dati, consulta [Prezzi di Amazon S3](#).

Utilizza Amazon S3 Transfer Acceleration per ridurre al minimo la latenza causata dalla distanza

[Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#) gestisce trasferimenti di file veloci, facili e sicuri su vaste distanze geografiche tra il client e un bucket S3. Transfer Acceleration sfrutta le edge location distribuite a livello globale in Amazon. [CloudFront](#) Quando arrivano in una edge location, i dati vengono instradati ad Amazon S3 attraverso un percorso di rete ottimizzato. Transfer Acceleration è ideale per il trasferimento regolare di gigabyte e terabyte di dati sui diversi continenti. È inoltre utile per i clienti che effettuano il caricamento in un bucket centralizzato da tutto il mondo.

È possibile utilizzare lo [strumento di confronto della velocità di accelerazione dei trasferimenti di Amazon S3](#) per confrontare le velocità di caricamento accelerate e non accelerate nelle Regioni di Amazon S3. Questo strumento utilizza caricamenti in più parti per trasferire un file dal browser in uso a diverse regioni Amazon S3 con e senza l'utilizzo di Amazon S3 Transfer Acceleration.

Usa la versione più recente di AWS SDK

Gli AWS SDK forniscono il supporto integrato per molte delle linee guida consigliate per l'ottimizzazione delle prestazioni di Amazon S3. Gli SDK offrono un'API più semplice per utilizzare al meglio Amazon S3 internamente a un'applicazione e vengono aggiornati regolarmente in modo da seguire le best practice più recenti. Ad esempio, gli SDK includono la logica per riprovare automaticamente le richieste sugli errori HTTP 503 e investono in codice per rispondere e adattarsi a connessioni lente.

Gli SDK forniscono anche lo strumento [TransferManager](#), che automatizza connessioni con dimensionamento orizzontale in modo da raggiungere migliaia di richieste al secondo, usando

richieste di intervalli di byte laddove appropriato. È importante utilizzare la versione più recente degli AWS SDK per ottenere le ultime funzionalità di ottimizzazione delle prestazioni.

Puoi inoltre ottimizzare le prestazioni quando utilizzi le richieste dell'API REST HTTP. Quando utilizzi l'API REST, devi seguire le stesse best practice che fanno parte degli SDK. Consenti i timeout e i tentativi sulle richieste lente e le connessioni multiple per permettere il recupero dei dati degli oggetti in parallelo. Per informazioni sull'utilizzo della REST API, consulta la [Documentazione di riferimento delle API di Amazon Simple Storage Service](#).

Modelli di progettazione delle prestazioni per Amazon S3

Nel progettare applicazioni per caricare e recuperare oggetti da Amazon S3, utilizza i nostri schemi di progettazione delle best practice per ottenere prestazioni ottimali per l'applicazione. Offriamo anche [Linee guida per le prestazioni di Amazon S3](#), che puoi prendere in considerazione quando pianifichi l'architettura dell'applicazione.

Per ottimizzare le prestazioni, puoi utilizzare i seguenti schemi di progettazione.

Argomenti

- [Utilizzo della cache per i contenuti a cui si accede di frequente](#)
- [Timeout e retry per applicazioni sensibili alla latenza](#)
- [Scalabilità orizzontale e parallelizzazione delle richieste per un elevato throughput](#)
- [Utilizzo di Amazon S3 Transfer Acceleration per accelerare i trasferimenti di dati geograficamente eterogenei](#)
- [Ottimizzazione per carichi di lavoro a elevata frequenza di richieste](#)

Utilizzo della cache per i contenuti a cui si accede di frequente

Molte applicazioni che archiviano dati in Amazon S3 fungono da “set di lavoro” dei dati richiesti ripetutamente dagli utenti. Se un carico di lavoro invia richieste GET ripetute per un set comune di oggetti, puoi utilizzare una cache come [Amazon CloudFront](#) o [Amazon ElastiCache](#) per ottimizzare le prestazioni. L'adozione corretta di una cache può portare a una bassa latenza e a tassi di trasferimento dei dati più alti. Le applicazioni che utilizzano il caching inviano anche meno richieste dirette ad Amazon S3, riducendo i costi delle richieste.

Amazon CloudFront è una rete di distribuzione rapida dei contenuti (CDN) che memorizza nella cache in modo trasparente i dati di Amazon S3 in un ampio set di punti di presenza distribuiti

geograficamente (). PoPs Quando è possibile accedere agli oggetti da più regioni o tramite Internet, CloudFront consente di memorizzare i dati nella cache vicino agli utenti che accedono agli oggetti. In questo modo, è possibile distribuire contenuti Amazon S3 comuni con prestazioni elevate. Per informazioni su CloudFront, consulta la [Amazon CloudFront Developer Guide](#).

Amazon ElastiCache è una cache in memoria gestita. Con ElastiCache, puoi effettuare il provisioning di istanze Amazon EC2 che memorizzano nella cache gli oggetti in memoria. Il caching porta alla riduzione di grandezza della latenza GET e ad aumenti sostanziali nel throughput del download. Per utilizzarlo ElastiCache, è necessario modificare la logica dell'applicazione in modo da popolare la cache con oggetti caldi e controllare la presenza di oggetti caldi nella cache prima di richiederli ad Amazon S3. Per esempi di utilizzo per ElastiCache migliorare le prestazioni di Amazon S3 GET, consulta il post del blog [Turbocharge Amazon S3 with Amazon for Redis. ElastiCache](#)

Timeout e retry per applicazioni sensibili alla latenza

In alcune situazioni un'applicazione riceve una risposta da Amazon S3 che indica che è necessario un nuovo tentativo. Amazon S3 mappa i nomi dei bucket e degli oggetti ai dati degli oggetti a essi associati. Se un'applicazione genera alti tassi di richiesta (in genere tassi sostenuti di oltre 5.000 richieste al secondo per un piccolo numero di oggetti) potrebbe ricevere risposte di rallentamento HTTP 503. Se si verifica questo errore, ogni SDK AWS implementa la logica di tentativo automatica utilizzando il backoff esponenziale. Se non stai utilizzando un SDK AWS, quando ricevi un errore HTTP 503 è necessario implementare la logica di tentativo. Per informazioni sulle tecniche di back-off, consulta [Comportamento del tentativo](#) nella Guida di riferimento agli SDK e agli strumenti di AWS.

Amazon S3 si ridimensiona automaticamente in risposta a nuovi tassi di richiesta prolungati, ottimizzando dinamicamente le prestazioni. Mentre Amazon S3 ottimizza internamente per sostenere un nuovo tasso di richieste, riceverai temporaneamente risposte di richiesta HTTP 503 fino al completamento dell'ottimizzazione. Dopo che Amazon S3 ha ottimizzato internamente le prestazioni per il nuovo tasso di richiesta, tutte le richieste vengono in genere gestite senza nuovi tentativi.

Per le applicazioni sensibili alla latenza, Amazon S3 consiglia di monitorare e ritentare in modo aggressivo le operazioni più lente. Nel ritentare una richiesta, consigliamo di utilizzare una nuova connessione ad Amazon S3 e di eseguire una nuova ricerca DNS.

Quando effettui richieste di dimensioni grandi e variabili (ad esempio, oltre 128 MB), consigliamo di tracciare il throughput raggiunto e di ritentare il 5 per cento più lento delle richieste. Quando effettui richieste più piccole (ad esempio, meno di 512 KB) dove le latenze medie sono spesso

dell'ordine di decine di millisecondi, una buona linea guida è ritentare un'operazione GET o PUT dopo 2 secondi. Se sono necessari tentativi aggiuntivi, la best practice è di effettuare il backoff. Ad esempio, consigliamo di emettere un tentativo dopo 2 secondi e un secondo tentativo dopo 4 secondi aggiuntivi.

Se l'applicazione effettua richieste a dimensione fissa ad Amazon S3, il tempo di risposta per ogni richiesta sarà più costante. In questo caso, una strategia semplice è identificare l'1 per cento più lento delle richieste e ritentarle. Anche un singolo tentativo è efficace nella riduzione della latenza.

Se utilizzi AWS Key Management Service (AWS KMS) per la crittografia lato server, consulta [Quotas](#) nella AWS Key Management Service Developer Guide per informazioni sulle tariffe di richiesta supportate per il tuo caso d'uso.

Scalabilità orizzontale e parallelizzazione delle richieste per un elevato throughput

Amazon S3 è un sistema distribuito di dimensioni molto grandi. Per sfruttarne a pieno la capacità di dimensionamento, consigliamo di ridimensionare orizzontalmente le richieste parallele agli endpoint del servizio Amazon S3. Oltre a distribuire le richieste in Amazon S3, questo tipo di approccio al dimensionamento permette di distribuire il carico su più percorsi nella rete.

Per i trasferimenti a throughput elevato, Amazon S3 consiglia di utilizzare applicazioni che usano più connessioni a dati GET o PUT in parallelo. Ad esempio, questo è supportato da [Amazon S3 Transfer Manager](#) nell'SDK AWS Java e la maggior parte degli altri AWS SDK fornisce costrutti simili. Per alcune applicazioni, puoi raggiungere connessioni parallele lanciando simultaneamente richieste multiple in diversi thread dell'applicazione o in diverse istanze dell'applicazione. Il miglior approccio da adottare dipende dall'applicazione e dalla struttura degli oggetti a cui accedi.

Puoi utilizzare gli AWS SDK per inviare richieste GET e PUT direttamente anziché utilizzare la gestione dei trasferimenti nell'SDK. AWS Questo approccio ti permette di ottimizzare il carico di lavoro in modo più diretto senza rinunciare al supporto degli SDK per i tentativi e la gestione delle risposte HTTP 503 che potrebbero verificarsi. Come regola generale, quando scarichi oggetti di grandi dimensioni da Amazon S3, suggeriamo di effettuare richieste simultanee per massimizzare il throughput di rete e ottimizzare le prestazioni di download. È possibile ottenere ciò richiedendo intervalli di byte specifici dell'oggetto o scaricando contemporaneamente singole parti di un oggetto composto da più parti. Questo approccio di download parallelo consente di utilizzare appieno la capacità della scheda di interfaccia di rete (NIC). Per gli oggetti caricati utilizzando il caricamento in più parti, consigliamo di scaricarli utilizzando le stesse dimensioni delle parti o di allineare le richieste

ai limiti della parte originale per ottenere prestazioni ottimali. Questo metodo di download simultaneo offre un throughput aggregato più elevato rispetto alle richieste relative a singoli oggetti completi.

La misurazione delle prestazioni è importante quando ottimizzi il numero di richieste da emettere simultaneamente. Consigliamo di iniziare con un richiesta alla volta. Misura la larghezza di banda della rete raggiunta e l'uso delle altre risorse che la tua applicazione utilizza nell'elaborazione dei dati. Puoi quindi identificare la risorsa con un collo di bottiglia (ossia, la risorsa con l'utilizzo più elevato) e di conseguenza il numero di richieste che possono essere utili. Ad esempio, se elaborare una richiesta alla volta porta a un utilizzo della CPU del 25 per cento, questo dato suggerisce che possono essere emesse fino a quattro richieste simultanee. La misurazione è essenziale ed è utile per confermare l'utilizzo della risorsa quando il tasso di richiesta aumenta.

Se l'applicazione invia richieste direttamente ad Amazon S3 utilizzando l'API REST, ti consigliamo di utilizzare un pool di connessioni HTTP e di riutilizzare ogni connessione per una serie di richieste. Evitare la configurazione della connessione per richiesta elimina la necessità di eseguire handshake slow-start su TCP e Secure Sockets Layer (SSL) su ogni richiesta. Per informazioni sull'utilizzo dell'API REST, consulta la [Documentazione di riferimento delle API di Amazon Simple Storage Service](#).

Infine, è utile considerare con attenzione DNS e verificare accuratamente che le richieste vengano distribuite su un ampio pool di indirizzi IP di Amazon S3. Le query DNS per Amazon S3 passano per un elenco di grandi dimensioni di endpoint IP. Ma effettuare il caching dei resolver o del codice dell'applicazione che riutilizza un singolo indirizzo IP non trae vantaggio dalla diversità degli indirizzi e dal bilanciamento del carico che ne deriva. Utilità di rete come lo strumento a riga di comando `netstat` possono mostrare gli indirizzi IP utilizzati per la comunicazione con Amazon S3 e forniamo linee guida per le configurazioni DNS da utilizzare. Per ulteriori informazioni su queste linee guida, consulta la sezione [Esecuzione di richieste](#) nella documentazione di riferimento delle API di Amazon S3.

Utilizzo di Amazon S3 Transfer Acceleration per accelerare i trasferimenti di dati geograficamente eterogenei

[Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#) è efficace nel ridurre o eliminare la latenza causata dalla distanza geografica tra client lontani a livello globale e un'applicazione locale che utilizza Amazon S3. Transfer Acceleration utilizza le edge location distribuite a livello globale per il trasporto dei dati. CloudFront La rete AWS edge ha punti di presenza in più di 50 località. Oggi viene utilizzata per distribuire contenuti CloudFront e fornire risposte rapide alle richieste DNS effettuate [su Amazon Route 53](#).

La rete edge permette anche di accelerare i trasferimenti dei dati da e verso Amazon S3. È ideale per le applicazioni che trasferiscono i dati tra continenti, dispongono di connessioni a Internet veloci e utilizzano oggetti di grandi dimensioni o hanno molti contenuti da caricare. Quando arrivano in una edge location, i dati vengono instradati ad Amazon S3 su un percorso di rete ottimizzato. In generale, più lontano ti trovi da una regione Amazon S3, maggiore è il miglioramento della velocità che otterrai utilizzando Transfer Acceleration.

Puoi configurare Transfer Acceleration su bucket nuovi o esistenti. È possibile utilizzare un endpoint Amazon S3 Transfer Acceleration separato per utilizzare le edge location. AWS Il modo migliore per verificare se Transfer Acceleration migliora le prestazioni delle richieste client consiste nell'utilizzare lo [strumento Speed Comparison di Amazon S3 Transfer Acceleration](#). Le configurazioni e le condizioni della rete variano in base al momento e alla località. Vengono quindi addebitati solo i trasferimenti in cui Amazon S3 Transfer Acceleration può potenzialmente migliorare le prestazioni di caricamento. Per informazioni sull'utilizzo di Transfer Acceleration con diversi AWS SDK, consulta [Abilitazione e utilizzo di S3 Transfer Acceleration](#).

Ottimizzazione per carichi di lavoro a elevata frequenza di richieste

Le applicazioni che generano frequenze di richiesta elevate ad Amazon S3 richiedono modelli di progettazione specifici per ottenere prestazioni ottimali. Quando l'applicazione genera costantemente più di 3.500 PUT/COPY/POST/DELETE o 5.500 GET/HEAD richieste al secondo per prefisso, è necessario implementare strategie per distribuire le richieste e gestire il comportamento di scalabilità.

Amazon S3 scala automaticamente le risorse per soddisfare frequenze di richiesta più elevate, ma questo dimensionamento avviene gradualmente. Durante il processo di dimensionamento, potresti ricevere risposte HTTP 503 (Slow Down). Queste risposte sono temporanee e indicano che Amazon S3 sta ottimizzando i sistemi interni per il nuovo modello di richiesta. Una volta completato il dimensionamento, le richieste verranno eseguite senza limitazione (della larghezza di banda della rete).

Per ottimizzare le prestazioni per i carichi di lavoro con frequenza di richiesta elevata, considera le seguenti strategie:

- Distribuisci le richieste su più prefissi: utilizza un modello di prefisso randomizzato o sequenziale per distribuire le richieste su più partizioni. Ad esempio, invece di utilizzare nomi di oggetti sequenziali come `log-2024-01-01.txt`, utilizza prefissi randomizzati come `a1b2/log-2024-01-01.txt`. Questo aiuta Amazon S3 a distribuire il carico in modo più efficace.
- Implementa il backoff esponenziale per gli errori 503: quando ricevi risposte HTTP 503, implementa la logica dei tentativi con backoff esponenziale. Inizia con un breve ritardo e aumenta gradualmente

il tempo di attesa tra un tentativo e l'altro. Gli AWS SDK includono una logica di ripetizione integrata che gestisce questo problema automaticamente.

- Monitora i modelli di richiesta: utilizza le CloudWatch metriche di Amazon per monitorare i tassi di richiesta e i tassi di errore. Presta particolare attenzione alle metriche degli errori 5xx, che possono indicare quando l'applicazione sta raggiungendo o superando gli attuali limiti di dimensionamento.
- Aumenta gradualmente la frequenza di richiesta: quando si avviano nuove applicazioni o aumenta significativamente la frequenza di richiesta, è opportuno aumentare gradualmente il traffico nel tempo anziché raggiungere immediatamente le frequenze di picco. Ciò consente ad Amazon S3 di scalare in modo proattivo e riduce la probabilità di limitazione (della larghezza di banda della rete).
- Utilizza più connessioni: distribuisci le richieste su più connessioni HTTP per massimizzare il throughput e ridurre l'impatto di ogni singolo problema di connessione.

Per le applicazioni che richiedono prestazioni elevate e coerenti, prendi in considerazione l'utilizzo di Amazon S3 Express One Zone, progettato per applicazioni che richiedono latenze nell'ordine di millisecondi e può supportare centinaia di migliaia di richieste al secondo. Per ulteriori informazioni, consulta [S3 Express One Zone](#).

Hosting di un sito Web statico tramite Amazon S3

Puoi utilizzare Amazon S3 per ospitare un sito web statico. In un sito Web statico, le singole pagine Web includono contenuti statici. Potrebbero contenere anche script lato client.

Note

È consigliabile utilizzare [Hosting AWS Amplify](#) per ospitare contenuti di siti web statici archiviati su S3. Amplify Hosting è un servizio completamente gestito che semplifica l'implementazione dei tuoi siti Web su una rete di distribuzione di contenuti (CDN) disponibile a livello globale basata su Amazon CloudFront, consentendo un hosting sicuro di siti Web statici.

Con AWS Amplify Hosting, puoi selezionare la posizione dei tuoi oggetti all'interno del tuo bucket generico, distribuire i tuoi contenuti su un CDN gestito e generare un URL HTTPS pubblico affinché il tuo sito Web sia accessibile ovunque. Per ulteriori informazioni su Amplify Hosting, vedi [Distribuzione di un sito Web statico su AWS Amplify Hosting da un bucket S3 generico](#) e [Distribuzione di un sito Web statico da S3 utilizzando la console Amplify nella Guida per l'utente della console](#). AWS Amplify

Per ulteriori informazioni sull'hosting di un sito Web statico su Amazon S3, incluse istruzioni e spiegazioni dettagliate, consulta i seguenti argomenti.

Important

Se il bucket che stai utilizzando per ospitare il tuo sito Web statico è stato crittografato utilizzando la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS), devi creare una CloudFront distribuzione Amazon per servire il tuo sito Web perché non supporta utenti anonimi. SSE-KMS Quando crei la CloudFront distribuzione, devi utilizzare l'origin access control (OAC) anziché l'origin access identity (OAI) per proteggere l'origine. OAI non supporta SSE-KMS, quindi è necessario utilizzare invece OAC.

Per ulteriori informazioni su OAC, consulta [Limitare l'accesso a un'origine Amazon S3](#) nella Amazon Developer Guide. CloudFront Per un tutorial che mostra come ospitare un sito Web statico utilizzando Amazon CloudFront, consulta [the section called "Hosting di streaming video"](#)

Argomenti

- [Endpoint del sito Web](#)
- [Abilitazione dell'hosting di siti Web](#)
- [Configurazione di un documento indice](#)
- [Configurazione di un documento di errore personalizzato](#)
- [Impostazione delle autorizzazioni per l'accesso al sito Web](#)
- [\(Facoltativo\) Registrazione del traffico Web](#)
- [\(Facoltativo\) Configurazione del reindirizzamento di una pagina Web](#)
- [Utilizzo della funzionalità Cross-Origin Resource Sharing \(CORS\)](#)
- [Tutorial per siti web statici](#)

Endpoint del sito Web

Quando configuri il bucket come sito Web statico, il sito Web è disponibile nell'endpoint del sito Web specifico della Regione AWS del bucket. Gli endpoint dei siti Web sono diversi dagli endpoint dove si inviano le richieste REST API. Per ulteriori informazioni sulle differenze tra gli endpoint, consulta [Differenze chiave tra un endpoint del sito Web e un endpoint REST API](#).

A seconda della regione, gli endpoint del sito web Amazon S3 seguono uno di questi due formati.

- Regione s3-website dash - `http://bucket-name.s3-website-Region.amazonaws.com`
- s3-website dot (.) Regione - `http://bucket-name.s3-website.Region.amazonaws.com`

Questi URL restituiscono un documento di indice predefinito che si configura per il sito Web. Per un elenco completo degli endpoint dei siti Web Amazon S3, consulta la sezione [Endpoint di siti Web Amazon S3](#).

Note

Per aumentare la sicurezza dei siti Web statici di Amazon S3, i domini endpoint dei siti Web Amazon S3 (ad esempio, `s3-website-us-east-1.amazonaws.com` o `s3-website.ap-south-1.amazonaws.com`) sono registrati nel [Public Suffix List \(PSL\)](#). Per una maggiore sicurezza, consigliamo di utilizzare i cookie con un prefisso `__Host-` se hai bisogno di impostare cookie sensibili nel nome di dominio per i siti Web statici Amazon S3. Questa

pratica ti aiuterà a difendere il tuo dominio dai tentativi CSRF (cross-site request forgery). Per ulteriori informazioni, consulta la [Set-Cookie](#) pagina del Mozilla Developer Network.

Se desideri che il sito Web sia pubblico, è necessario rendere tutti i contenuti pubblicamente leggibili affinché i clienti possano accedervi nell'endpoint del sito Web. Per ulteriori informazioni, consulta [Impostazione delle autorizzazioni per l'accesso al sito Web](#).

Important

- Gli endpoint del sito Web di Amazon S3 non supportano HTTPS o access point. Per utilizzare HTTPS, puoi procedere in uno dei seguenti modi:
- (Consigliato) Utilizza [Hosting AWS Amplify](#) per ospitare contenuti di siti web statici archiviati su S3. Amplify Hosting è un servizio completamente gestito che semplifica l'implementazione dei tuoi siti Web su una rete di distribuzione di contenuti (CDN) disponibile a livello globale basata su Amazon CloudFront, consentendo un hosting sicuro di siti Web statici.

Con AWS Amplify Hosting, puoi selezionare la posizione dei tuoi oggetti all'interno del tuo bucket generico, distribuire i tuoi contenuti su un CDN gestito e generare un URL HTTPS pubblico affinché il tuo sito Web sia accessibile ovunque. Per ulteriori informazioni su Amplify Hosting, vedi [Distribuzione di un sito Web statico su AWS Amplify Hosting da un bucket S3 generico](#) e [Distribuzione di un sito Web statico da S3 utilizzando la console Amplify nella Guida per l'utente della console](#). AWS Amplify

- Usa Amazon per servire un sito Web statico CloudFront ospitato su Amazon S3. Per ulteriori informazioni, consulta [How do I use CloudFront to service request HTTPS per il mio bucket Amazon S3?](#) Per utilizzare HTTPS con un dominio personalizzato, consulta [Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#).
- I bucket con pagamento a carico del richiedente non consentono l'accesso tramite un endpoint di sito Web. Qualsiasi richiesta a tale bucket riceve una risposta 403 Accesso negato . Per ulteriori informazioni, consulta [Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati](#).

Argomenti

- [Esempi di endpoint del sito Web](#)
- [Aggiunta di un CNAME DNS](#)
- [Utilizzo di un dominio personalizzato con Route 53](#)
- [Differenze chiave tra un endpoint del sito Web e un endpoint REST API](#)

Esempi di endpoint del sito Web

Negli esempi seguenti viene illustrato come è possibile accedere a un bucket Amazon S3 configurato come sito web statico.

Example– Richiesta di un oggetto a livello root

Per richiedere un oggetto specifico archiviato a livello root nel bucket, utilizza la seguente struttura di URL:

```
http://bucket-name.s3-website.Region.amazonaws.com/object-name
```

Ad esempio, questo URL richiede l'oggetto `photo.jpg` archiviato a livello root nel bucket:

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/photo.jpg
```

Example– Richiesta di un oggetto in un prefisso

Per richiedere un oggetto archiviato in una cartella nel bucket, utilizza questa struttura di URL:

```
http://bucket-name.s3-website.Region.amazonaws.com/folder-name/object-name
```

Il seguente URL richiede l'oggetto `docs/doc1.html` nel bucket.

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/docs/doc1.html
```

Aggiunta di un CNAME DNS

Se si dispone di un dominio registrato, è possibile aggiungere una voce DNS CNAME che punti all'endpoint del sito web Amazon S3. Ad esempio, se hai registrato il dominio `www.example-bucket.com`, puoi creare un bucket `www.example-bucket.com` e aggiungere un record DNS CNAME che punti a `www.example-bucket.com.s3-website.Region.amazonaws.com`. Tutte

le richieste a `http://www.example-bucket.com` vengono instradate verso `www.example-bucket.com.s3-website.Region.amazonaws.com`.

Per ulteriori informazioni, consulta [Personalizzazione degli URL Amazon S3 con record CNAME](#).

Utilizzo di un dominio personalizzato con Route 53

Invece di accedere al sito web utilizzando un endpoint del sito web Amazon S3, è possibile utilizzare il proprio dominio registrato con Amazon Route 53 per servire i contenuti, ad esempio, `example.com`. Puoi utilizzare Amazon S3 con Route 53 per ospitare un sito web nel dominio principale. Ad esempio, se si dispone di un dominio root `example.com` e si ospita il sito web su Amazon S3, i visitatori del sito web possono accedere al sito dal loro browser, inserendo `http://www.example.com` o `http://example.com`.

Per un esempio di procedura guidata, consulta [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#).

Differenze chiave tra un endpoint del sito Web e un endpoint REST API

L'endpoint del sito web Amazon S3 è ottimizzato per l'accesso da un browser web. Nella tabella seguente vengono riepilogate le principali differenze tra un endpoint REST API e un endpoint del sito Web.

Differenze principali	Endpoint REST API	Endpoint del sito Web
Controllo degli accessi	Supporta contenuti pubblici e privati.	Supporta solo contenuti pubblicamente leggibili.
Gestione dei messaggi di errore	Restituisce una risposta XML-formata di errore	Restituisce un documento HTML.
Supporto del reindirizzamento	Non applicabile.	Supporta reindirizzamenti sia a livello di oggetto sia di bucket.
Richieste supportate	Supporta tutte le operazioni relative ai bucket e agli oggetti.	Supporta solo richieste GET e HEAD sugli oggetti.

Differenze principali	Endpoint REST API	Endpoint del sito Web
Risposte alle richieste GET e HEAD alla root di un bucket	Restituisce un elenco delle chiavi degli oggetti nel bucket.	Restituisce un documento di indice specificato nella configurazione del sito Web.
Supporto di Secure Sockets Layer (SSL)	Supporta connessioni SSL.	Non supporta connessioni SSL.

Per un elenco completo degli endpoint Amazon S3, consultare la sezione relativa a [endpoint e quote di Amazon S3](#) nella Riferimenti generali di AWS.

Abilitazione dell'hosting di siti Web

Quando configuri un bucket come sito Web statico, devi abilitare l'hosting statico del sito Web, configurare un documento di indice e impostare le autorizzazioni.

Puoi abilitare l'hosting di siti Web statici utilizzando la console Amazon S3, l'API REST, AWS gli SDK, o. AWS CLI CloudFormation

Per configurare il sito Web con un dominio personalizzato, consulta [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#).

Utilizzo della console S3

Per abilitare l'hosting di un sito Web statico

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket, seleziona il nome del bucket per cui desideri abilitare l'hosting di siti web statici.
4. Scegliere Properties (Proprietà).
5. In Hosting di siti Web statici, seleziona Modifica.

6. Seleziona Utilizza questo bucket per l'hosting di un sito Web.
7. In Hosting di siti Web statici, seleziona Abilita.
8. In Documento di indice immettere il nome file del documento di indice, in genere `index.html`.

Il nome del documento indice fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome del file del documento indice HTML che si prevede di caricare nel bucket S3. Quando si configura un bucket per l'hosting di siti Web, è necessario specificare un documento di indice. Amazon S3 restituisce questo documento di indice quando si eseguono richieste per il dominio root o per una delle sottocartelle. Per ulteriori informazioni, consulta [Configurazione di un documento indice](#).

9. Per fornire il tuo documento di errore personalizzato per gli errori di classe 4XX, specifica il nome file del documento in Documento di errore.

Il nome del documento di errore fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome del file del documento di errore HTML che si prevede di caricare nel bucket S3. Se non si specifica un documento di errore personalizzato e si verifica un errore, Amazon S3 restituisce un documento di errore HTML predefinito. Per ulteriori informazioni, consulta [Configurazione di un documento di errore personalizzato](#).

10. (Facoltativo) Per specificare regole di reindirizzamento avanzate, utilizza JSON per descrivere le regole in Regole reindirizzamento.

Ad esempio, è possibile instradare le richieste in base a prefissi o nomi della chiave dell'oggetto specifici nella richiesta. Per ulteriori informazioni, consulta [Configurazione delle regole di reindirizzamento per utilizzare i reindirizzamenti condizionali avanzati](#).

11. Seleziona Salva modifiche.

Amazon S3 abilita l'hosting statico del sito web per il tuo bucket. Nella parte inferiore della pagina, in Hosting di siti Web statici, viene visualizzato l'endpoint del sito web per il bucket.

12. In Hosting sito Web statico, prendi nota dell'endpoint.

Endpoint è l'endpoint del sito web Amazon S3 per il bucket. Dopo aver configurato il bucket come sito Web statico, è possibile utilizzare questo endpoint per testare il sito Web.

Utilizzo di REST API

Per maggiori informazioni sull'invio diretto di richieste REST per abilitare l'hosting statico di siti Web, consulta le seguenti sezioni nella Guida di riferimento all'API di Amazon Simple Storage Service:

- [PUT Bucket website](#)
- [GET Bucket website](#)
- [DELETE Bucket website](#)

Utilizzo di AWS SDK

Per ospitare un sito web statico su Amazon S3, si configura un bucket Amazon S3 per l'hosting di siti Web e, successivamente, si caricano i contenuti del sito Web nel bucket. È inoltre possibile utilizzare gli SDK AWS per creare, aggiornare ed eliminare la configurazione del sito Web a livello di codice. Gli SDK forniscono classi wrapper per REST API di Amazon S3. Se l'applicazione lo richiede, è possibile inviare richieste REST API direttamente dall'applicazione.

.NET

L'esempio seguente mostra come utilizzare per gestire la configurazione del sito Web AWS SDK per .NET per un bucket. Per aggiungere una configurazione del sito Web a un bucket, si fornisce un nome bucket e una configurazione del sito Web. La configurazione del sito Web deve includere un documento di indice e può contenere un documento di errore opzionale. Tali documenti devono essere archiviati nel bucket. Per ulteriori informazioni, consulta [PUT Bucket website](#). Per ulteriori informazioni sulla funzionalità website di Amazon S3 consulta [Hosting di un sito Web statico tramite Amazon S3](#).

L'esempio di codice C# seguente aggiunge una configurazione del sito Web al bucket specificato. La configurazione specifica sia il documento di indice, sia i nomi del documento di errore. Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella SDK for .NET AWS Developer Guide.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class WebsiteConfigTest
    {
        private const string bucketName = "**** bucket name ****";
        private const string indexDocumentSuffix = "**** index object key ****"; //
        For example, index.html.
    }
}
```



```

        private const string errorDocument = "*** error object key ***"; // For
example, error.html.
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddWebsiteConfigurationAsync(bucketName, indexDocumentSuffix,
errorDocument).Wait();
        }

        static async Task AddWebsiteConfigurationAsync(string bucketName,
                                                    string indexDocumentSuffix,
                                                    string errorDocument)
        {
            try
            {
                // 1. Put the website configuration.
                PutBucketWebsiteRequest putRequest = new PutBucketWebsiteRequest()
                {
                    BucketName = bucketName,
                    WebsiteConfiguration = new WebsiteConfiguration()
                    {
                        IndexDocumentSuffix = indexDocumentSuffix,
                        ErrorDocument = errorDocument
                    }
                };
                PutBucketWebsiteResponse response = await
client.PutBucketWebsiteAsync(putRequest);

                // 2. Get the website configuration.
                GetBucketWebsiteRequest getRequest = new GetBucketWebsiteRequest()
                {
                    BucketName = bucketName
                };
                GetBucketWebsiteResponse getResponse = await
client.GetBucketWebsiteAsync(getRequest);
                Console.WriteLine("Index document: {0}",
getResponse.WebsiteConfiguration.IndexDocumentSuffix);
                Console.WriteLine("Error document: {0}",
getResponse.WebsiteConfiguration.ErrorDocument);
            }
        }

```

```

        catch (AmazonS3Exception e)
        {
            Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
        }
        catch (Exception e)
        {
            Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
        }
    }
}
}
}

```

PHP

L'esempio di codice PHP seguente aggiunge una configurazione del sito Web al bucket specificato. Il metodo `create_website_config` fornisce esplicitamente il documento di indice e i nomi del documento di errore. L'esempio recupera inoltre la configurazione del sito Web e stampa la risposta. Per ulteriori informazioni sulla funzionalità `website` di Amazon S3 consulta [Hosting di un sito Web statico tramite Amazon S3](#).

Per ulteriori informazioni sull'API AWS SDK for Ruby, vai a [AWS SDK for Ruby - Version 2](#).

```

require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Add the website configuration.
$s3->putBucketWebsite([
    'Bucket' => $bucket,
    'WebsiteConfiguration' => [
        'IndexDocument' => ['Suffix' => 'index.html'],
        'ErrorDocument' => ['Key' => 'error.html']
    ]
]

```

```
]);  
  
// Retrieve the website configuration.  
$result = $s3->getBucketWebsite([  
    'Bucket' => $bucket  
]);  
echo $result->getPath('IndexDocument/Suffix');  
  
// Delete the website configuration.  
$s3->deleteBucketWebsite([  
    'Bucket' => $bucket  
]);
```

Utilizzo di AWS CLI

Per ulteriori informazioni sull'utilizzo di AWS CLI per configurare un bucket S3 come sito Web statico, [consulta il sito Web nel Command Reference](#). AWS CLI

Successivamente, è necessario configurare il documento indice e impostare le autorizzazioni. Per informazioni, consultare [Configurazione di un documento indice](#) e [Impostazione delle autorizzazioni per l'accesso al sito Web](#).

È inoltre possibile configurare facoltativamente un [documento di errore](#), la [registrazione del traffico Web](#) o un [reindirizzamento](#).

Configurazione di un documento indice

Quando si abilita l'hosting di siti Web, è necessario configurare e caricare un documento di indice. Un documento di indice è una pagina Web che Amazon S3 restituisce quando viene fatta una richiesta alla root di un sito web o a qualsiasi sottocartella. Ad esempio, se un utente inserisce `http://www.example.com` nel browser, l'utente non richiede alcuna pagina specifica. In questo caso, Amazon S3 fornisce il documento indice, talvolta chiamato pagina predefinita.

Quando si abilita l'hosting statico di siti Web per il bucket, si immette il nome del documento di indice (ad esempi, `index.html`). Dopo aver abilitato l'hosting statico di siti Web per il bucket, si carica un file HTML con il nome del documento di indice nel bucket.

La barra finale nell'URL a livello di root è facoltativa. Ad esempio, quando si configura il sito Web con `index.html` come documento di indice, entrambi gli URL seguenti restituiscono `index.html`.

```
http://example-bucket.s3-website.Region.amazonaws.com/  
http://example-bucket.s3-website.Region.amazonaws.com
```

Per ulteriori informazioni sugli endpoint del sito Amazon S3, consulta [Endpoint del sito Web](#).

Documento di indice e cartelle

In Amazon S3, un bucket è un container flat di oggetti. Non fornisce alcuna organizzazione gerarchica in quanto è il file system del computer a farlo. Tuttavia, è possibile creare una gerarchia logica utilizzando i nomi delle chiavi degli oggetti che implicano una struttura a cartelle.

Si supponga ad esempio un bucket con tre oggetti che hanno i nomi delle chiavi seguenti. Sebbene questi siano archiviati senza un'organizzazione gerarchica fisica, è possibile dedurre la seguente struttura logica a cartelle a partire dai nomi delle chiavi:

- `sample1.jpg`: l'oggetto è nella root del bucket.
- `photos/2006/Jan/sample2.jpg`: l'oggetto è nella sottocartella `photos/2006/Jan`.
- `photos/2006/Feb/sample3.jpg`: l'oggetto è nella sottocartella `photos/2006/Feb`.

Nella console Amazon S3 è anche possibile creare una cartella in un bucket. Ad esempio, è possibile creare una cartella denominata `photos`. È possibile caricare gli oggetti nel bucket o nella cartella `photos` all'interno del bucket. Se si aggiunge l'oggetto `sample.jpg` al bucket, il nome della chiave è `sample.jpg`. Se si carica l'oggetto nella cartella `photos`, il nome della chiave dell'oggetto è `photos/sample.jpg`.

Se si crea una struttura a cartelle nel bucket, occorre avere un documento di indice in ciascun livello. In ogni cartella, il documento di indice deve avere lo stesso nome, ad esempio, `index.html`. Quando un utente specifica un URL che si presenta come la ricerca di una cartella, la presenza o l'assenza di una barra finale determina il comportamento del sito Web. Ad esempio, il seguente URL, con barra finale, restituisce il documento di indice `photos/index.html`.

```
http://bucket-name.s3-website.Region.amazonaws.com/photos/
```

Tuttavia, se si esclude la barra finale dall'URL precedente, Amazon S3 cerca innanzitutto un oggetto `photos` nel bucket. Se non trova l'oggetto `photos`, cerca un documento indice, `photos/index.html`. Se questo documento viene trovato, Amazon S3 restituisce un messaggio 302 Found e punta alla chiave `photos/`. Per le successive richieste `photos/`, Amazon S3 restituisce `photos/index.html`. Se il documento di indice non viene trovato, Amazon S3 restituisce un errore.

Configurazione di un documento indice

Per configurare un documento indice utilizzando la console S3, attieniti alla procedura seguente. Puoi anche configurare un documento di indice utilizzando l'API REST, gli AWS SDK, o. AWS CLI CloudFormation

Note

In un bucket abilitato al controllo delle versioni, puoi caricare più copie del file `index.html`, ma verrà risolta solo la versione più recente. Per ulteriori informazioni sulla funzione Controllo delle versioni S3, consulta [Conservazione di più versioni degli oggetti con Controllo delle versioni S3](#).

Quando si abilita l'hosting statico di siti Web per il bucket, si immette il nome del documento di indice (ad esempi, **index.html**). Dopo aver abilitato l'hosting di siti Web statici per il bucket, si carica un file HTML con il nome del documento di indice nel bucket.

Per configurare il documento di indice

1. Creare un file `index.html`

Se non si dispone di un file `index.html`, è possibile utilizzare il seguente codice HTML per crearne uno:

```
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
  <title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
</html>
```

2. Salva il file indice in locale.

Il nome del file del documento indice deve corrispondere esattamente al nome del documento indice immesso nella finestra di dialogo Hosting sito Web statico. Il nome del documento indice distingue tra maiuscole e minuscole. Ad esempio, se si immette `index.html` per il nome del

documento Indice nella finestra di dialogo Hosting sito Web statico, anche il nome del file del documento indice deve essere `index.html` e non `Index.html`.

3. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
4. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
5. Nell'elenco dei bucket, seleziona il nome del bucket che desideri utilizzare per l'hosting di un sito web statico.
6. Abilitare l'hosting di siti Web statici per il bucket e inserire il nome esatto del documento di indice (ad esempi, `index.html`). Per ulteriori informazioni, consulta [Abilitazione dell'hosting di siti Web](#).

Dopo aver abilitato l'hosting di siti Web statici, procedere alla fase 6.

7. Per caricare il documento di indice nel bucket, eseguire una delle operazioni seguenti:
 - Trascinare e rilasciare il file di indice nell'elenco bucket della console.
 - Scegliere Upload (Carica) e seguire le istruzioni per scegliere e caricare il file di indice.

Per istruzioni dettagliate, consulta [Caricamento degli oggetti](#).

8. (Opzionale) Caricare altri contenuti del sito Web nel bucket.

Successivamente, è necessario impostare le autorizzazioni per l'accesso al sito Web. Per informazioni, consulta [Impostazione delle autorizzazioni per l'accesso al sito Web](#).

È inoltre possibile configurare facoltativamente un [documento di errore](#), la [registrazione del traffico Web](#) o un [reindirizzamento](#).

Configurazione di un documento di errore personalizzato

Dopo aver configurato il bucket come sito web statico, quando si verifica un errore, Amazon S3 restituisce un documento di errore HTML. È possibile configurare il bucket con un documento di errore personalizzato in modo che Amazon S3 restituisca tale documento quando si verifica un errore.

 Note

In caso di errore, alcuni browser visualizzano il loro messaggio di errore, ignorando il documento di errore che restituisce Amazon S3. Ad esempio, quando si verifica un errore HTTP 404 Non trovato, Google Chrome potrebbe ignorare il documento di errore che Amazon S3 restituisce e visualizzare il suo errore.

Argomenti

- [Codici di risposta HTTP di Amazon S3](#)
- [Configurazione di un documento di errore personalizzato](#)

Codici di risposta HTTP di Amazon S3

La seguente tabella elenca il sottoinsieme dei codici di risposta HTTP che Amazon S3 restituisce in caso di errore.

Codice di errore HTTP	Descrizione
301 Moved Permanently (301 Spostato definitivamente)	Quando un utente invia una richiesta direttamente agli endpoint del sito web Amazon S3 (<code>http://s3-website. <i>Region</i>.amazonaws.com/</code>), Amazon S3 restituisce una risposta 301 Moved Permanently (301 Spostato definitivamente) e reindirizza tali richieste a <code>https://aws.amazon.com/s3/</code> .
302 Found (302 Trovato)	Quando Amazon S3 riceve una richiesta per una chiave <code>x</code> , <code>http://<i>bucket-name</i>.s3-website. <i>Region</i>.amazonaws.com/</code> <code>x</code> , senza barra finale, cerca innanzitutto l'oggetto con nome della chiave <code>x</code> . Se l'oggetto non viene trovato, Amazon S3 stabilisce che la richiesta è per la sottocartella <code>x</code> , la reindirizza aggiungendo una barra finale e restituisce 302 Found (302 Trovato).
304 Not Modified (304 Non modificato)	Amazon S3 utilizza le intestazioni delle <code>If-Modified-Since</code> richieste <code>If-Match</code> and/or <code>If-None-Match</code> per determinare se l'oggetto richiesto

Codice di errore HTTP	Descrizione
	è uguale alla copia memorizzata nella cache del client. If-Unmodified-Since Se l'oggetto coincide, l'endpoint del sito Web restituisce una risposta 304 Not Modified (304 Non modificato).
400 Malformed Request (400 Richiesta non corretta)	L'endpoint del sito Web restituisce una risposta 400 Malformed Request (400 Richiesta non corretta) quando un utente cerca di accedere a un bucket attraverso l'endpoint regionale sbagliato.
403 Forbidden (403 Non consentito)	L'endpoint del sito Web restituisce una risposta 403 Forbidden (403 Non consentito) quando la richiesta di un utente viene trasferita a un oggetto che non è pubblicamente leggibile. Il proprietario dell'oggetto deve rendere l'oggetto pubblicamente leggibile mediante una policy del bucket o un'ACL.

Codice di errore HTTP	Descrizione
404 Not Found (404 Non trovato)	<p>L'endpoint del sito Web restituisce una risposta 404 Not Found (404 Non trovato) per i motivi seguenti:</p> <ul style="list-style-type: none">• Amazon S3 stabilisce che l'URL del sito web fa riferimento alla chiave di un oggetto che non esiste.• Amazon S3 deduce che la richiesta riguarda un documento di indice che non esiste.• Il bucket specificato nell'URL non esiste.• Il bucket specificato nell'URL esiste, ma non è configurato come sito Web. <p>È possibile creare un documento personalizzato che viene restituito per 404 Not Found (404 Non trovato). Assicurarsi che il documento sia caricato nel bucket configurato come sito Web e che la configurazione di hosting del sito Web preveda l'utilizzo del documento.</p> <p>Per informazioni su come Amazon S3 interpreta l'URL come richiesta di un oggetto o di un documento di indice, consulta Configurazione di un documento indice.</p>
500 Service Error (500 Errore servizio)	<p>L'endpoint del sito Web restituisce una risposta 500 Service Error (500 Errore servizio) in caso di errore del server interno.</p>
503 Service Unavailable (503 Servizio non disponibile)	<p>L'endpoint del sito web restituisce una risposta 503 Service Unavailable (503 Servizio non disponibile) quando Amazon S3 stabilisce che occorre ridurre il tasso di richiesta.</p>

Per ciascuno di questi errori, Amazon S3 restituisce un messaggio HTML predefinito. Di seguito è riportato un esempio di messaggio HTML che viene restituito per una risposta 403 Forbidden (403 Non consentito).

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 873CA367A51F7EC7
- HostId: DdQezl9vkuw5luD5HKsFaTDm9KH4PZzCPRkW3igimILbTu1DiYlvXjgyd7pVxq32

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

Configurazione di un documento di errore personalizzato

Quando configuri il bucket come sito Web statico, puoi fornire un documento di errore personalizzato contenente un messaggio di errore intuitivo e una guida aggiuntiva. Amazon S3 restituisce il documento di errore personalizzato solo per la classe dei codici di errore HTTP 4XX.

Per configurare un documento di errore personalizzato utilizzando la console S3, attenersi alla procedura riportata di seguito. Puoi anche configurare un documento di errore utilizzando l'API REST, gli AWS SDK, o. AWS CLI CloudFormation Per ulteriori informazioni, consulta gli argomenti seguenti:

- [PutBucketWebsite](#) nel riferimento alle API di Amazon Simple Storage Service
- [AWS: :S3: :Bucket WebsiteConfiguration](#) nella Guida per l'utente CloudFormation
- [put-bucket-website](#) nel Riferimento ai comandi di AWS CLI

Quando abiliti l'hosting di siti Web statici per il tuo bucket, specifichi il nome del documento di errore (ad esempio, **404.html**). Dopo avere abilitato l'hosting di siti Web statici per il bucket, carichi un file HTML con il nome del documento di errore nel bucket.

Per configurare un documento di errore

1. Crea un documento di errore, ad esempio **404.html**.

2. Salva il file del documento di errore in locale.

Il nome del documento di errore fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome immesso quando hai attivato l'hosting statico di siti Web. Ad esempio, se specifichi `404.html` per il nome del documento di errore nella finestra di dialogo Hosting sito Web statico, anche il nome file del documento di errore dovrà essere `404.html`.

3. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
4. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
5. Nell'elenco dei bucket, seleziona il nome del bucket che desideri utilizzare per l'hosting di un sito web statico.
6. Abilita l'hosting di siti Web statici per il bucket e inserisci il nome esatto del documento di errore (ad esempio, `404.html`). Per ulteriori informazioni, consulta [Abilitazione dell'hosting di siti Web](#) e [Configurazione di un documento di errore personalizzato](#).

Dopo aver abilitato l'hosting di siti Web statici, procedere alla fase 6.

7. Per caricare il documento di errore nel bucket, completa una delle operazioni riportate di seguito:
 - Trascina e rilascia il file del documento di errore nell'elenco dei bucket della console.
 - Scegliere Upload (Carica) e seguire le istruzioni per scegliere e caricare il file di indice.

Per istruzioni dettagliate, consulta [Caricamento degli oggetti](#).

Impostazione delle autorizzazioni per l'accesso al sito Web

Quando si configura un bucket come sito Web statico, se si desidera che il sito Web sia pubblico, è possibile concedere l'accesso per la lettura pubblica. Per consentire la lettura pubblica del bucket, occorre disabilitare le impostazioni di blocco dell'accesso pubblico al bucket e scrivere una policy del bucket che conceda l'accesso per la lettura pubblica. Se il bucket contiene oggetti che non appartengono al proprietario del bucket, potrebbe essere necessario aggiungere anche una lista di controllo degli accessi (ACL) dell'oggetto che concede a tutti l'accesso in lettura.

Se non desideri disabilitare le impostazioni di blocco dell'accesso pubblico per il tuo bucket ma desideri comunque che il tuo sito web sia pubblico, puoi creare una CloudFront distribuzione Amazon per servire il tuo sito web statico. Per ulteriori informazioni, consulta [Velocizza il tuo sito Web con](#)

[Amazon CloudFront](#) o [Usa una CloudFront distribuzione Amazon per servire un sito Web statico](#) nella [Amazon Route 53 Developer Guide](#).

Note

Nell'endpoint del sito web, se un utente richiede un oggetto che non esiste, Amazon S3 restituisce un codice di risposta HTTP 404 (Not Found). Se l'oggetto esiste ma la relativa autorizzazione di lettura non è stata concessa, l'endpoint del sito Web restituisce un codice di risposta HTTP 403 (Access Denied). L'utente può utilizzare il codice di risposta per capire se esiste un oggetto specifico. Per evitare questo tipo di comportamento, il supporto di siti Web per il bucket non deve essere abilitato.

Argomenti

- [Fase 1: modifica delle impostazioni dell'accesso pubblico ai blocchi Amazon S3](#)
- [Fase 2: aggiunta di una policy del bucket](#)
- [Liste di controllo accessi dell'oggetto](#)

Fase 1: modifica delle impostazioni dell'accesso pubblico ai blocchi Amazon S3

Per configurare un bucket esistente come sito web statico con accesso pubblico, devi modificare le impostazioni di blocco dell'accesso pubblico per il bucket. Potrebbe anche essere necessario modificare le impostazioni di blocco dell'accesso pubblico a livello di account. Amazon S3 applica la combinazione più restrittiva di impostazioni blocco di accesso pubblico a livello di account e a livello di bucket.

Ad esempio, se consenti l'accesso pubblico per un bucket ma lo blocchi a livello dell'account, Amazon S3 continuerà a bloccare l'accesso pubblico al bucket. In questo scenario, sarà necessario modificare le impostazioni di blocco dell'accesso pubblico a livello di bucket e di account. Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

Per impostazione predefinita, Amazon S3 blocca l'accesso pubblico all'account e ai bucket. Per utilizzare un bucket per ospitare un sito Web statico, puoi seguire questa procedura per modificare le impostazioni di blocco dell'accesso pubblico:

⚠ Warning

Prima di completare questi passaggi, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#) per assicurarsi di aver compreso e accettato i rischi connessi alla concessione dell'accesso pubblico. Quando si disattivano le impostazioni di blocco dell'accesso pubblico per rendere pubblico il bucket, chiunque su Internet può accedere al bucket. Consigliamo di bloccare tutti gli accessi pubblici ai bucket.

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Seleziona il nome del bucket configurato come sito Web statico.
3. Seleziona Autorizzazioni.
4. In Blocca accesso pubblico (impostazioni bucket), seleziona Modifica.
5. Deseleziona Blocca tutto l'accesso pubblico, quindi seleziona Salva modifiche.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 

**Account settings for Block Public Access are currently turned on**

[Account settings for Block Public Access](#) that are enabled apply even if they are disabled for this bucket.

- ☐ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
 - ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
 - ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
 - ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
 - ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Amazon S3 disattiva le impostazioni di blocco dell'accesso pubblico per il bucket. Per creare un sito web pubblico statico, potrebbe essere necessario [modificare anche le impostazioni di blocco dell'accesso pubblico](#) per l'account prima di aggiungere una policy del bucket. Se le impostazioni dell'account per il blocco dell'accesso pubblico sono attualmente attivate, verrà visualizzata una nota in Blocca accesso pubblico (impostazioni bucket).

Fase 2: aggiunta di una policy del bucket

Per rendere gli oggetti nel bucket pubblicamente leggibili, devi scrivere una policy del bucket che conceda a tutti l'autorizzazione `s3:GetObject`.

Dopo aver modificato le impostazioni di blocco dell'accesso pubblico S3, è possibile aggiungere una policy del bucket per concedere l'accesso pubblico in lettura al bucket. Quando concedi l'accesso pubblico in lettura, chiunque su Internet può accedere al bucket.

Important

La policy seguente è solo un esempio e consente l'accesso completo ai contenuti del bucket. Prima di continuare con questa fase, esamina l'argomento relativo a [come proteggere i file nel bucket Amazon S3](#) per assicurarti di comprendere le best practice per la protezione dei file nel bucket S3 e i rischi connessi alla concessione dell'accesso pubblico .

1. In Bucket, scegli il nome del bucket.
2. Seleziona Autorizzazioni.
3. In Policy del bucket, seleziona Modifica.
4. Per concedere l'accesso in lettura pubblico al sito Web, copiare la policy del bucket seguente e incollarla in Editor della policy del bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ]
    }
  ]
}
```

```
    ],  
    "Resource": [  
        "arn:aws:s3:::Bucket-Name/*"  
    ]  
  }  
]
```

5. Aggiorna Resource al tuo nome bucket.

Nell'esempio precedente, bucket policy, *Bucket-Name* è un segnaposto per il nome del bucket. Per utilizzare questa policy di bucket con il proprio bucket, è necessario aggiornare il nome in modo che corrisponda al bucket.

6. Seleziona Salva modifiche.

Viene visualizzato un messaggio che indica che la policy del bucket è stata aggiunta correttamente.

Se viene visualizzato l'errore `Policy has invalid resource`, conferma che il nome del bucket nella policy di bucket corrisponde al nome del bucket. Per informazioni sull'aggiunta di una policy del bucket, consulta [In che modo aggiungere una policy del bucket S3?](#)

Se viene visualizzato un messaggio di errore e non è possibile salvare la policy di bucket, controlla le impostazioni di blocco dell'accesso pubblico all'account e al bucket per confermare che consenti l'accesso pubblico al bucket.

Liste di controllo accessi dell'oggetto

Puoi utilizzare una policy del bucket per concedere l'autorizzazione in lettura pubblica per gli oggetti. Tuttavia, la policy del bucket si applica solo agli oggetti appartenenti al proprietario del bucket. Se il bucket contiene oggetti che non appartengono al proprietario del bucket, quest'ultimo deve utilizzare la lista di controllo degli accessi (ACL) per concedere l'autorizzazione READ pubblica per tali oggetti.

S3 Proprietà dell'oggetto è un'impostazione a livello di bucket Amazon S3 che è possibile utilizzare per controllare la proprietà degli oggetti caricati nel bucket e per disabilitare o abilitare le liste di controllo degli accessi (ACL). Per impostazione predefinita, Proprietà dell'oggetto è impostata su Proprietario del bucket applicato e tutte le liste di controllo degli accessi (ACL) sono disabilitate. Quando le ACL sono disabilitate, il proprietario del bucket dispone di tutti gli oggetti nel bucket e gestisce l'accesso ad essi in maniera esclusiva utilizzando policy di gestione dell'accesso.

La maggior parte degli attuali casi d'uso in Amazon S3 non richiede più l'uso delle ACL. È consigliabile mantenere le ACL disabilitate, tranne nelle circostanze in cui è necessario controllare individualmente l'accesso per ciascun oggetto. Con le ACL disabilitate, puoi utilizzare le policy per controllare l'accesso a tutti gli oggetti nel bucket, a prescindere da chi ha caricato gli oggetti nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

Important

Se il bucket per uso generico utilizza l'impostazione Proprietario del bucket applicato per Proprietà dell'oggetto S3, è necessario utilizzare le policy per fornire l'accesso al bucket per uso generico e agli oggetti in esso contenuti. Con l'impostazione Proprietario del bucket applicato abilitata, le richieste per impostare liste di controllo degli accessi (ACL) e aggiornare le ACL non vanno a buon fine e restituiscono il codice di errore `AccessControlListNotSupported`. Le richieste di lettura delle ACL sono ancora supportate.

Per rendere un oggetto pubblicamente leggibile mediante un ACL, occorre concedere l'autorizzazione READ al gruppo `AllUsers`, come illustrato nel seguente elemento "grant". Aggiungere questo elemento "grant" all'ACL dell'oggetto. Per informazioni sulla gestione delle ACL, consulta [Panoramica delle liste di controllo accessi \(ACL\)](#).

```
<Grant>
  <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="Group">
    <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
  </Grantee>
  <Permission>READ</Permission>
</Grant>
```

(Facoltativo) Registrazione del traffico Web

Facoltativamente puoi abilitare la registrazione dell'accesso al server Amazon S3 per un bucket configurato come sito web statico. La registrazione degli accessi al server fornisce record dettagliati per le richieste che sono effettuate al bucket. Per ulteriori informazioni, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#). Se prevedi di utilizzare Amazon per CloudFront

[velocizzare il tuo sito web](#), puoi anche utilizzare la registrazione. CloudFront Per ulteriori informazioni, consulta [Configurazione e utilizzo dei log di accesso](#) nella Amazon CloudFront Developer Guide.

Per abilitare la registrazione dell'accesso al server per il bucket del sito Web statico

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella stessa Regione in cui è stato creato il bucket configurato come sito web statico, crea un bucket per uso generico per la registrazione di log, ad esempio `logs.example.com`.
3. Creare una cartella per i file di registrazione degli accessi al server (ad esempio, `logs`).
4. (Facoltativo) Se desideri utilizzarlo CloudFront per migliorare le prestazioni del tuo sito web, crea una cartella per i file di CloudFront registro (ad esempio, `cdn`).

Per ulteriori informazioni, consulta [Velocizza il tuo sito Web con Amazon CloudFront](#).

5. Nell'elenco Bucket, seleziona il nome del bucket.
6. Scegliere Properties (Proprietà).
7. In Registrazione accesso server, seleziona Modifica.
8. Scegli Enable (Abilita).
9. In Bucket di destinazione, seleziona la destinazione del bucket e della cartella per i log di accesso al server:
 - Individua la cartella e il percorso del bucket:
 1. Seleziona Sfoglia S3.
 2. Scegli il nome del bucket, quindi seleziona la cartella dei log.
 3. Seleziona Scegli percorso.
 - Specifica il percorso del bucket S3, ad esempio, **`s3://logs.example.com/logs/`**.
10. Seleziona Salva modifiche.

Nel bucket di log, ora puoi accedere ai tuoi log. Amazon S3 scrive i log di accesso del sito web nel bucket log ogni due ore.

(Facoltativo) Configurazione del reindirizzamento di una pagina Web

Se il bucket Amazon S3 è configurato per l'hosting di siti Web statici, è possibile configurare i reindirizzamenti per il bucket o gli oggetti in esso contenuti. Per configurare il reindirizzamento sono disponibili le opzioni riportate di seguito.

Argomenti

- [Reindirizzamento delle richieste per l'endpoint del sito Web del bucket a un altro bucket o dominio](#)
- [Configurazione delle regole di reindirizzamento per utilizzare i reindirizzamenti condizionali avanzati](#)
- [Reindirizzamento delle richieste per un oggetto](#)

Reindirizzamento delle richieste per l'endpoint del sito Web del bucket a un altro bucket o dominio

È possibile reindirizzare tutte le richieste a un endpoint di sito Web per un bucket a un altro bucket o a un dominio. Se vengono reindirizzate tutte le richieste, qualsiasi richiesta effettuata all'endpoint del sito Web viene reindirizzata al bucket o al dominio specificato.

Ad esempio, se il dominio root è `example.com` e desideri servire richieste sia per `http://example.com` che per `http://www.example.com`, puoi creare due bucket denominati `example.com` e `www.example.com`. Successivamente, mantenere il contenuto nel bucket `example.com` e configurare l'altro bucket `www.example.com` per reindirizzare tutte le richieste al bucket `example.com`. Per ulteriori informazioni, consulta [Configurazione di un sito Web statico utilizzando un nome di dominio personalizzato](#).

Per reindirizzare le richieste per un endpoint di un sito Web bucket

1. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. In Bucket seleziona il nome del bucket da cui desideri reindirizzare le richieste (ad esempio, `www.example.com`).
3. Scegliere Properties (Proprietà).
4. In Hosting di siti Web statici, seleziona Modifica.
5. Seleziona Reindirizza richieste per un oggetto.

6. Nella casella Nome host specifica l'endpoint del sito Web per il bucket o il dominio personalizzato.

Ad esempio, se il reindirizzamento è effettuato verso un indirizzo di dominio root, digita **example.com**.

7. Per Protocollo, seleziona il protocollo per le richieste reindirizzate (nessuno, http o https).

Se non si specifica un protocollo, l'opzione predefinita è nessuno.

8. Seleziona Salva modifiche.

Configurazione delle regole di reindirizzamento per utilizzare i reindirizzamenti condizionali avanzati

Con le regole di reindirizzamento avanzato, è possibile instradare le richieste in modo condizionale in base ai nomi delle chiavi degli oggetti specifici, ai prefissi nella richiesta o ai codici di risposta. Si supponga ad esempio di eliminare o rinominare un oggetto nel bucket. È possibile aggiungere una regola di routing che reindirizza la richiesta a un altro oggetto. Se si desidera rendere una cartella non disponibile, è possibile aggiungere una regola di routing per reindirizzare la richiesta a un'altra pagina Web. Inoltre, è possibile aggiungere una regola di routing per gestire le condizioni di errore instradando le richieste che restituiscono l'errore a un altro dominio dove viene elaborato l'errore.

Quando abiliti l'hosting di siti Web statici per il tuo bucket, puoi specificare facoltativamente regole di reindirizzamento avanzate. Amazon S3 ha un limite di 50 regole di routing per configurazione di sito web. Se sono necessarie più di 50 regole di routing, è possibile utilizzare l'instradamento degli oggetti. Per ulteriori informazioni, consulta [Utilizzo della console S3](#).

Per ulteriori informazioni sulla configurazione delle regole di routing utilizzando l'API REST, consulta [PutBucketWebsite](#) Amazon Simple Storage Service API Reference.

Important

Per creare regole di reindirizzamento nella nuova console Amazon S3, è necessario utilizzare JSON. Per gli esempi JSON, consulta [Esempi regole di reindirizzamento](#).

Per configurare le regole di reindirizzamento per un sito Web statico

Per aggiungere le regole di reindirizzamento per un bucket che ha già abilitato l'hosting di siti Web statici, attieniti alla seguente procedura.

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket scegli il nome di un bucket configurato come sito web statico.
4. Scegliere Properties (Proprietà).
5. In Hosting di siti Web statici, seleziona Modifica.
6. Nella casella Redirection rules (Regole di reindirizzamento), immettere le regole di reindirizzamento in JSON.

Nella console S3 descrivi le regole utilizzando JSON. Per gli esempi JSON, consulta [Esempi regole di reindirizzamento](#). Amazon S3 ha un limite di 50 regole di routing per configurazione di sito web.

7. Seleziona Salva modifiche.

Elementi regola instradamento

Di seguito è riportata la sintassi generale per definire le regole di routing in una configurazione di un sito Web in XML. Per configurare le regole di reindirizzamento nella nuova console S3, è necessario utilizzare JSON. Per gli esempi JSON, consulta [Esempi regole di reindirizzamento](#).

JSON

```
[
  {
    "Condition": {
      "HttpErrorCodeReturnedEquals": "string",
      "KeyPrefixEquals": "string"
    },
    "Redirect": {
      "HostName": "string",
      "HttpRedirectCode": "string",
      "Protocol": "http"|"https",
      "ReplaceKeyPrefixWith": "string",
      "ReplaceKeyWith": "string"
    }
  }
]
```

```
}
]
```

Note: Redirect must each have at least one child element. You can have either ReplaceKeyPrefix with or ReplaceKeyWith but not both.

XML

```
<RoutingRules> =
  <RoutingRules>
    <RoutingRule>...</RoutingRule>
    [<RoutingRule>...</RoutingRule>
     ...]
  </RoutingRules>

<RoutingRule> =
  <RoutingRule>
    [ <Condition>...</Condition> ]
    <Redirect>...</Redirect>
  </RoutingRule>

<Condition> =
  <Condition>
    [ <KeyPrefixEquals>...</KeyPrefixEquals> ]
    [ <HttpErrorCodeReturnedEquals>...</HttpErrorCodeReturnedEquals> ]
  </Condition>
  Note: <Condition> must have at least one child element.

<Redirect> =
  <Redirect>
    [ <HostName>...</HostName> ]
    [ <Protocol>...</Protocol> ]
    [ <ReplaceKeyPrefixWith>...</ReplaceKeyPrefixWith> ]
    [ <ReplaceKeyWith>...</ReplaceKeyWith> ]
    [ <HttpRedirectCode>...</HttpRedirectCode> ]
  </Redirect>
```

Note: <Redirect> must have at least one child element. You can have either ReplaceKeyPrefix with or ReplaceKeyWith but not both.

Nella seguente tabella sono descritti gli elementi della regola di routing.

Nome	Descrizione
<code>RoutingRules</code>	Container per una raccolta di elementi <code>RoutingRule</code> .
<code>RoutingRule</code>	<p>Una regola che stabilisce una condizione e il reindirizzamento che viene applicato quando la condizione è soddisfatta.</p> <p>Condizione:</p> <ul style="list-style-type: none">• Un container <code>RoutingRules</code> deve contenere almeno una regola di routing.
<code>Condition</code>	Container per descrivere una condizione che deve essere soddisfatta per l'applicazione del reindirizzamento specificato. Se la regola di routing non include una condizione, la regola viene applicata a tutte le richieste.
<code>KeyPrefixEquals</code>	<p>Il prefisso del nome della chiave dell'oggetto da cui vengono reindirizzate le richieste.</p> <p><code>KeyPrefixEquals</code> è obbligatorio se <code>HttpErrorCodeReturnedEquals</code> non è specificato. Se <code>KeyPrefixEquals</code> e <code>HttpErrorCodeReturnedEquals</code> sono specificati, devono essere entrambi veri perché la condizione sia soddisfatta.</p>
<code>HttpErrorCodeReturnedEquals</code>	<p>Il codice di errore HTTP che deve corrispondere perché il reindirizzamento venga applicato. Se si verifica un errore e se il codice di errore corrisponde a questo valore, il reindirizzamento specificato viene applicato.</p> <p><code>HttpErrorCodeReturnedEquals</code> è obbligatorio se <code>KeyPrefixEquals</code> non è specificato. Se <code>KeyPrefixEquals</code> e <code>HttpErrorCodeReturnedEquals</code> sono specificati, devono essere entrambi veri perché la condizione sia soddisfatta.</p>

Nome	Descrizione
<code>Redirect</code>	<p>Elemento del container che fornisce istruzioni per il reindirizzamento della richiesta. È possibile reindirizzare le richieste a un altro host o a un'altra pagina oppure specificare un altro protocollo da utilizzare. Un <code>RoutingRule</code> deve avere un elemento <code>Redirect</code>. Un elemento <code>Redirect</code> deve contenere almeno uno dei seguenti elementi di pari livello: <code>Protocol</code>, <code>HostName</code>, <code>ReplaceKeyPrefixWith</code>, <code>ReplaceKeyWith</code> o <code>HttpRedirectCode</code>.</p>
<code>Protocol</code>	<p>Il protocollo, <code>http</code> o <code>https</code>, da utilizzare nell'intestazione <code>Location</code> che viene restituita nella risposta.</p> <p>Se viene fornito uno degli elementi di pari livello, <code>Protocol</code> non è necessario.</p>
<code>HostName</code>	<p>Il nome dell'host da utilizzare nell'intestazione <code>Location</code> che viene restituita nella risposta.</p> <p>Se viene fornito uno degli elementi di pari livello, <code>HostName</code> non è necessario.</p>
<code>ReplaceKeyPrefixWith</code>	<p>Il prefisso del nome della chiave dell'oggetto che sostituisce il valore di <code>KeyPrefixEquals</code> nella richiesta di reindirizzamento.</p> <p>Se viene fornito uno degli elementi di pari livello, <code>ReplaceKeyPrefixWith</code> non è necessario. Può essere fornito solo se <code>ReplaceKeyWith</code> non è fornito.</p>

Nome	Descrizione
<code>ReplaceKeyWith</code>	<p>La chiave dell'oggetto da utilizzare nell'intestazione <code>Location</code> che viene restituita nella risposta.</p> <p>Se viene fornito uno degli elementi di pari livello, <code>ReplaceKeyWith</code> non è necessario. Può essere fornito solo se <code>ReplaceKeyPrefixWith</code> non è fornito.</p>
<code>HttpRedirectCode</code>	<p>Il codice di reindirizzamento HTTP da utilizzare nell'intestazione <code>Location</code> che viene restituita nella risposta.</p> <p>Se viene fornito uno degli elementi di pari livello, <code>HttpRedirectCode</code> non è necessario.</p>

Esempi regole di reindirizzamento

Gli esempi seguenti illustrano le comuni attività di reindirizzamento:

Important

Per creare regole di reindirizzamento nella nuova console Amazon S3, è necessario utilizzare JSON.

Example 1: reindirizzamento dopo la ridenominazione del prefisso di una chiave

Si supponga che il bucket contenga i seguenti oggetti:

- `index.html`
- `docs/article1.html`
- `docs/article2.html`

Si decide di rinominare la cartella da `docs/` a `documents/`. Dopo aver apportato questa modifica, occorre reindirizzare le richieste del prefisso `docs/` verso `documents/`. Ad esempio, la richiesta di `docs/article1.html` sarà reindirizzata a `documents/article1.html`.

In questo caso, si aggiunge la seguente regola di routing alla configurazione del sito Web.

JSON

```
[
  {
    "Condition": {
      "KeyPrefixEquals": "docs/"
    },
    "Redirect": {
      "ReplaceKeyPrefixWith": "documents/"
    }
  }
]
```

XML

```
<RoutingRules>
  <RoutingRule>
    <Condition>
      <KeyPrefixEquals>docs/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyPrefixWith>documents/</ReplaceKeyPrefixWith>
    </Redirect>
  </RoutingRule>
</RoutingRules>
```

Example 2: reindirizzamento delle richieste di una cartella eliminata verso una pagina

Si supponga l'eliminazione della cartella `images/` (ovvero, l'eliminazione di tutti gli oggetti con prefisso della chiave `images/`). È possibile aggiungere una regola di routing che reindirizza le richieste di qualsiasi oggetto con prefisso della chiave `images/` verso una pagina denominata `folderdeleted.html`.

JSON

```
[
  {
    "Condition": {
      "KeyPrefixEquals": "images/"
    }
  }
]
```

```
    },
    "Redirect": {
      "ReplaceKeyWith": "folderdeleted.html"
    }
  }
]
```

XML

```
<RoutingRules>
  <RoutingRule>
    <Condition>
      <KeyPrefixEquals>images/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyWith>folderdeleted.html</ReplaceKeyWith>
    </Redirect>
  </RoutingRule>
</RoutingRules>
```

Example 3: reindirizzamento a un altro dominio con un percorso specifico

Si supponga di voler reindirizzare le richieste con un percorso specifico a un altro dominio. Ad esempio, si desidera reindirizzare le richieste con `/redirect/me` a `https://example.com/new/path`.

Quando si utilizzano insieme `HostName` e `ReplaceKeyWith`, Amazon S3 crea l'URL di reindirizzamento concatenando il nome host e la chiave di sostituzione con una barra tra loro. Pertanto, non si deve includere una barra iniziale nel valore `ReplaceKeyWith`. Amazon S3 aggiunge automaticamente la barra tra il nome host e la chiave di sostituzione.

JSON

```
[
  {
    "Condition": {
      "KeyPrefixEquals": "redirect/me"
    },
    "Redirect": {
      "HostName": "example.com",
      "ReplaceKeyWith": "new/path"
    }
  }
]
```

```
]
  }
}
```

XML

```
<RoutingRules>
  <RoutingRule>
    <Condition>
      <KeyPrefixEquals>redirect/me</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <HostName>example.com</HostName>
      <ReplaceKeyWith>new/path</ReplaceKeyWith>
    </Redirect>
  </RoutingRule>
</RoutingRules>
```

Questa configurazione reindirizza una richiesta con `https://yourbucket.s3-website-region.amazonaws.com/redirect/me` a `https://example.com/new/path`. Si noti che `ReplaceKeyWith` è impostato su `new/path` senza barra iniziale.

Example 4: Reindirizzamento per un errore HTTP

Si supponga che quando non viene trovato un oggetto richiesto, si desidera reindirizzare le richieste a un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Aggiungere una regola di reindirizzamento in modo tale che, quando viene restituito un codice di stato HTTP 404 (Non trovato), il visitatore del sito venga reindirizzato a un'istanza Amazon EC2 che gestisca la richiesta.

Il seguente esempio riporta nel reindirizzamento anche il prefisso della chiave dell'oggetto `report-404/`. Ad esempio, se la richiesta di una pagina `ExamplePage.html` restituisce un errore HTTP 404, la richiesta viene reindirizzata a una pagina `report-404/ExamplePage.html` sull'istanza Amazon EC2 specificata. Se non sono presenti regole di routing e si verifica l'errore HTTP 404, viene restituito il documento di errore specificato nella configurazione.

JSON

```
[
  {
    "Condition": {
      "HttpErrorCodeReturnedEquals": "404"
```

```
    },  
    "Redirect": {  
      "HostName": "ec2-11-22-333-44.compute-1.amazonaws.com",  
      "ReplaceKeyPrefixWith": "report-404/"  
    }  
  }  
]
```

XML

```
<RoutingRules>  
  <RoutingRule>  
    <Condition>  
      <HttpErrorCodeReturnedEquals>404</HttpErrorCodeReturnedEquals >  
    </Condition>  
    <Redirect>  
      <HostName>ec2-11-22-333-44.compute-1.amazonaws.com</HostName>  
      <ReplaceKeyPrefixWith>report-404/</ReplaceKeyPrefixWith>  
    </Redirect>  
  </RoutingRule>  
</RoutingRules>
```

Reindirizzamento delle richieste per un oggetto

Puoi reindirizzare le richieste di un oggetto a un altro oggetto o URL impostando la posizione di reindirizzamento del sito Web nei metadati dell'oggetto. Si imposta il reindirizzamento aggiungendo la proprietà `x-amz-website-redirect-location` ai metadati dell'oggetto. Nella console Amazon S3, la Posizione di reindirizzamento del sito Web si imposta nei metadati dell'oggetto. Se utilizzi l'[API Amazon S3](#), hai impostato `x-amz-website-redirect-location`. Il sito Web interpreta quindi l'oggetto come reindirizzamento 301.

Per reindirizzare una richiesta a un altro oggetto, si imposta la posizione di reindirizzamento sulla chiave dell'oggetto di destinazione. Per reindirizzare una richiesta a un URL esterno, si imposta la posizione di reindirizzamento sull'URL desiderato. Per ulteriori informazioni sui metadati degli oggetti, consulta [System-defined metadati degli oggetti](#).

Quando si imposta il reindirizzamento di una pagina, è possibile mantenere o eliminare il contenuto dell'oggetto di origine. Ad esempio, se nel bucket è presente un oggetto `page1.html`, è possibile reindirizzare qualsiasi richiesta per questa pagina a un altro oggetto `page2.html`. Sono disponibili due opzioni:

- Mantenere il contenuto dell'oggetto `page1.html` e reindirizzare le richieste per la pagina.
- Eliminare il contenuto di `page1.html` e caricare un oggetto a zero byte denominato `page1.html` per sostituire l'oggetto esistente e reindirizzare le richieste per la pagina.

Utilizzo della console S3

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nell'elenco Bucket, seleziona il nome di un bucket configurato come sito Web statico (ad esempio, `example.com`).
3. In Oggetti, seleziona l'oggetto.
4. Seleziona Operazioni, quindi Modifica metadati.
5. Seleziona Metadati.
6. Seleziona Aggiungi metadati.
7. In Tipo, seleziona Definito dal sistema.
8. In Chiave, scegli `x-amz-website-redirect-location`.
9. In Valore, immettere il nome della chiave dell'oggetto a cui si desidera reindirizzare, ad esempio `/page2.html`.

Per un altro oggetto nello stesso bucket, il prefisso `/` nel valore è obbligatorio. È possibile inoltre impostare il valore su un URL esterno, ad esempi, `http://www.example.com`.

10. Seleziona Modifica metadati.

Utilizzo di REST API

Le seguenti operazioni API Amazon S3 supportano l'intestazione `x-amz-website-redirect-location` nella richiesta. Amazon S3 archivia il valore dell'intestazione nei metadati dell'oggetto come `x-amz-website-redirect-location`.

- [PUT Object](#)
- [Avvio del caricamento in più parti](#)
- [POST Object](#)
- [PUT Object - Copy](#)

Un bucket configurato per l'hosting di siti Web presenta sia l'endpoint del sito Web che l'endpoint REST. La richiesta di una pagina configurata come reindirizzamento 301 può generare i seguenti risultati, a seconda dell'endpoint della richiesta:

- Region-specific endpoint del sito Web: Amazon S3 reindirizza la richiesta di pagina in base al valore della proprietà. `x-amz-website-redirect-location`
- Endpoint REST: Amazon S3 non reindirizza la richiesta della pagina. Restituisce l'oggetto richiesto.

Per ulteriori informazioni sugli endpoint, consulta [Differenze chiave tra un endpoint del sito Web e un endpoint REST API](#).

Quando si imposta il reindirizzamento di una pagina, è possibile mantenere o eliminare il contenuto dell'oggetto. Supponi, ad esempio, di avere un oggetto `page1.html` nel bucket.

- Per mantenere il contenuto di `page1.html` e reindirizzare solo le richieste della pagina, è possibile inviare una richiesta [PUT Object - Copy](#) per creare un nuovo oggetto `page1.html` che utilizzi l'oggetto `page1.html` esistente come origine. Nella richiesta, si imposta l'intestazione `x-amz-website-redirect-location`. Al completamento della richiesta, si ottiene la pagina originale con contenuto invariato, ma Amazon S3 reindirizza qualsiasi richiesta della pagina alla posizione di reindirizzamento specificata.
- Per eliminare il contenuto dell'oggetto `page1.html` e reindirizzare le richieste della pagina, è possibile inviare una richiesta PUT Object per caricare un oggetto da zero byte con la stessa chiave dell'oggetto: `page1.html`. Nella richiesta PUT, si imposta `x-amz-website-redirect-location` per `page1.html` sul nuovo oggetto. Al completamento della richiesta, `page1.html` non ha contenuto e le richieste vengono reindirizzate alla posizione specificata da `x-amz-website-redirect-location`.

Quando si recupera l'oggetto tramite l'operazione [GET Object](#), insieme ad altri metadati dell'oggetto, Amazon S3 restituisce nella risposta l'intestazione `x-amz-website-redirect-location`.

Utilizzo della funzionalità Cross-Origin Resource Sharing (CORS)

Cross-origin la condivisione delle risorse (CORS) definisce un modo per le applicazioni Web client caricate in un dominio di interagire con le risorse di un dominio diverso. Con il supporto della funzionalità CORS, è possibile creare applicazioni Web lato client complete con Amazon S3 e concedere l'accesso multiorigine alle risorse di Amazon S3 in modo selettivo.

In questa sezione viene fornita una panoramica della funzionalità CORS. Gli argomenti secondari descrivono come abilitare CORS utilizzando la console Amazon S3 o programmaticamente utilizzando l'API REST di Amazon S3 e gli SDK. AWS

Cross-origin condivisione delle risorse: scenari Use-case

Di seguito sono riportati alcuni scenari di esempio per l'uso della funzionalità CORS.

Scenario 1

Si supponga di ospitare un sito Web in un bucket Amazon S3 denominato `website`, come descritto in [Hosting di un sito Web statico tramite Amazon S3](#). Gli utenti caricano l'endpoint del sito Web:

```
http://website.s3-website.us-east-1.amazonaws.com
```

Ora vuoi utilizzare JavaScript le pagine Web archiviate in questo bucket per poter effettuare richieste GET e PUT autenticate sullo stesso bucket utilizzando l'endpoint API Amazon S3 per il bucket, `website.s3.us-east-1.amazonaws.com`. Normalmente un browser JavaScript impedirebbe di consentire tali richieste, ma con CORS puoi configurare il bucket per abilitare esplicitamente le richieste tra origini diverse da `website.s3-website.us-east-1.amazonaws.com`.

Scenario 2

Si supponga di voler ospitare un font Web dal bucket S3. Anche in questo caso, i browser richiedono un controllo della funzionalità CORS (anche denominato "controllo preliminare") per il caricamento dei font Web. È necessario configurare il bucket che ospita il font Web in modo da consentire a qualsiasi origine di eseguire queste richieste.

In che modo Amazon S3 valuta la configurazione CORS in un bucket?

Quando Amazon S3 riceve una richiesta preliminare da un browser, valuta la configurazione CORS per il bucket e utilizza la prima regola `CORSRule` corrispondente alla richiesta del browser in entrata per abilitare una richiesta multiorigine. Per garantire la corrispondenza tra la regola e la richiesta, è necessario che siano soddisfatte le condizioni elencate di seguito.

- L'intestazione `Origin` di una richiesta CORS al bucket deve corrispondere alle origini dell'elemento `AllowedOrigins` nella configurazione CORS.
- I metodi HTTP specificati in `Access-Control-Request-Method` in una richiesta CORS al bucket devono corrispondere al metodo o ai metodi elencati nell'elemento `AllowedMethods` della configurazione CORS.

- Le intestazioni elencate nell'intestazione Access-Control-Request-Headers di una richiesta di verifica devono corrispondere alle intestazioni dell'elemento AllowedHeaders nella configurazione CORS.

Note

Le ACL e le policy continuano a essere valide quando si abilita la funzionalità CORS nel bucket.

In che modo Punto di accesso per le espressioni Lambda dell'oggetto supporta CORS

Quando Lambda per oggetti Amazon S3 riceve una richiesta da un browser o la richiesta include un'intestazione Origin, Lambda per oggetti Amazon S3 aggiunge sempre un campo di intestazione "AllowedOrigins": "*".

Per ulteriori informazioni sull'uso di CORS, consulta gli argomenti riportati di seguito.

Argomenti

- [Elementi di una configurazione CORS](#)
- [Configurazione della funzionalità Cross-Origin Resource Sharing \(CORS\)](#)
- [Test di CORS](#)
- [Risoluzione dei problemi di CORS](#)

Elementi di una configurazione CORS

Per configurare il bucket in modo da consentire le richieste multiorigine, si crea una configurazione CORS. La configurazione CORS è un documento con elementi che identificano le origini che potranno accedere al bucket, le operazioni (metodi HTTP) supportate per ogni origine e altre informazioni specifiche dell'operazione. È possibile aggiungere fino a 100 regole alla configurazione. È possibile aggiungere la configurazione CORS come risorsa secondaria cors al bucket.

Se configura CORS nella console S3, è necessario utilizzare JSON per creare una configurazione CORS. La nuova console S3 supporta solo configurazioni JSON CORS.

Per ulteriori informazioni sulla configurazione CORS e sugli elementi in essa contenuti, consulta gli argomenti riportati di seguito. Per istruzioni su come aggiungere una configurazione CORS, consulta [Configurazione della funzionalità Cross-Origin Resource Sharing \(CORS\)](#).

 Important

Nella console S3, la configurazione CORS deve essere JSON.

Argomenti

- [Elemento AllowedMethods](#)
- [Elemento AllowedOrigins](#)
- [Elemento AllowedHeaders](#)
- [Elemento ExposeHeaders](#)
- [Elemento MaxAgeSeconds](#)
- [Esempi di configurazioni CORS](#)

Elemento **AllowedMethods**

Nella configurazione CORS è possibile specificare i valori indicati di seguito per l'elemento AllowedMethods.

- GET
- PUT
- POST
- DELETE
- HEAD

Elemento **AllowedOrigins**

Nell'elemento AllowedOrigins, è possibile specificare le origini da cui si desiderano consentire le richieste multidominio, ad esempio `http://www.example.com`. La stringa di origine può contenere solamente un carattere jolly *, ad esempio `http://*.example.com`. Se si desidera, è possibile specificare * come origine per consentire a tutte le origini di inviare richieste multiorigine. È anche possibile specificare `https` per abilitare solo le origini sicure.

Elemento **AllowedHeaders**

L'elemento `AllowedHeaders` specifica le intestazioni consentite in una richiesta preliminare tramite l'intestazione `Access-Control-Request-Headers`. Ogni nome di intestazione in `Access-Control-Request-Headers` deve corrispondere a una voce nell'elemento. Tra le intestazioni richieste, Amazon S3 invierà nella risposta solo quelle consentite. Per un esempio di elenco di intestazioni che possono essere utilizzate nelle richieste ad Amazon S3, consulta l'argomento relativo alle [intestazioni di richiesta comuni](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Ogni `AllowedHeaders` stringa nella configurazione può contenere al massimo un carattere `*` jolly. Ad esempio, `<AllowedHeader>x-amz-*` abilita tutte le Amazon-specific intestazioni.

Elemento **ExposeHeaders**

Ogni `ExposeHeader` elemento identifica un'intestazione nella risposta a cui desideri che i clienti possano accedere dalle loro applicazioni (ad esempio, da un `JavaScript XMLHttpRequest` oggetto). Per un elenco delle intestazioni di risposta più comuni di Amazon S3, consulta l'argomento relativo alle [intestazioni di richiesta comuni](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service.

Elemento **MaxAgeSeconds**

L'elemento `MaxAgeSeconds` specifica l'intervallo di tempo in secondi durante il quale il browser può memorizzare nella cache la risposta a una richiesta preliminare identificata in base a risorsa, metodo HTTP e origine.

Esempi di configurazioni CORS

Anziché accedere a un sito Web utilizzando un endpoint del sito Web Amazon S3, è possibile utilizzare il proprio dominio, come `example1.com`, per consegnare il contenuto. Per informazioni sull'uso del proprio dominio, consulta [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#).

La configurazione CORS di esempio riportata di seguito include tre regole, specificate come elementi `CORSRule`:

- La prima regola consente le richieste multiorigine `PUT`, `POST` e `DELETE` provenienti dall'origine `http://www.example1.com`. La regola consente inoltre tutte le intestazioni in una richiesta

OPTIONS preliminare tramite l'intestazione `Access-Control-Request-Headers`. In risposta alle richieste OPTIONS preliminari, Amazon S3 restituisce le intestazioni richieste.

- La seconda regola consente le stesse richieste multiorigine della prima regola, ma si applica a un'altra origine, `http://www.example2.com`.
- La terza regola consente le richieste multiorigine GET provenienti da tutte le origini. Il carattere jolly * si riferisce a tutte le origini.

JSON

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "PUT",
      "POST",
      "DELETE"
    ],
    "AllowedOrigins": [
      "http://www.example1.com"
    ],
    "ExposeHeaders": []
  },
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "PUT",
      "POST",
      "DELETE"
    ],
    "AllowedOrigins": [
      "http://www.example2.com"
    ],
    "ExposeHeaders": []
  },
  {
    "AllowedHeaders": [],
    "AllowedMethods": [
```

```
        "GET"  
    ],  
    "AllowedOrigins": [  
        "*"   
    ],  
    "ExposeHeaders": []  
  }  
]
```

XML

```
<CORSConfiguration>  
  <CORSRule>  
    <AllowedOrigin>http://www.example1.com</AllowedOrigin>  
  
    <AllowedMethod>PUT</AllowedMethod>  
    <AllowedMethod>POST</AllowedMethod>  
    <AllowedMethod>DELETE</AllowedMethod>  
  
    <AllowedHeader>*</AllowedHeader>  
  </CORSRule>  
  <CORSRule>  
    <AllowedOrigin>http://www.example2.com</AllowedOrigin>  
  
    <AllowedMethod>PUT</AllowedMethod>  
    <AllowedMethod>POST</AllowedMethod>  
    <AllowedMethod>DELETE</AllowedMethod>  
  
    <AllowedHeader>*</AllowedHeader>  
  </CORSRule>  
  <CORSRule>  
    <AllowedOrigin>*</AllowedOrigin>  
    <AllowedMethod>GET</AllowedMethod>  
  </CORSRule>  
</CORSConfiguration>
```

La configurazione CORS supporta anche i parametri di configurazione opzionali, come illustrato nella seguente configurazione CORS. In questo esempio la configurazione CORS consente le richieste multiorigine PUT, POST e DELETE provenienti dall'origine `http://www.example.com`.

JSON

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "PUT",
      "POST",
      "DELETE"
    ],
    "AllowedOrigins": [
      "http://www.example.com"
    ],
    "ExposeHeaders": [
      "x-amz-server-side-encryption",
      "x-amz-request-id",
      "x-amz-id-2"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

XML

```
<CORSConfiguration>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
    <MaxAgeSeconds>3000</MaxAgeSeconds>
    <ExposeHeader>x-amz-server-side-encryption</
ExposeHeader>
    <ExposeHeader>x-amz-request-id</
ExposeHeader>
    <ExposeHeader>x-amz-id-2</ExposeHeader>
  </CORSRule>
</CORSConfiguration>
```

L'elemento `CORSRule` nella configurazione precedente include gli elementi opzionali riportati di seguito.

- `MaxAgeSeconds` – Specifica l'intervallo di tempo in secondi (in questo esempio, 3000) durante il quale il browser memorizza nella cache una risposta Amazon S3 a una richiesta `OPTIONS` preliminare per la risorsa specificata. La memorizzazione nella cache della risposta consente al browser di non inviare richieste preliminari ad Amazon S3 se la richiesta originale viene ripetuta.
- `ExposeHeaders`—Identifica le intestazioni delle risposte (in questo esempio, `x-amz-server-side-encryption`, `x-amz-request-id`, `ex-amz-id-2`) a cui i clienti possono accedere dalle proprie applicazioni (ad esempio, da un oggetto). `JavaScript XMLHttpRequest`

Configurazione della funzionalità Cross-Origin Resource Sharing (CORS)

Cross-origin la condivisione delle risorse (CORS) definisce un modo per le applicazioni Web client caricate in un dominio di interagire con le risorse di un dominio diverso. Con il supporto della funzionalità CORS, è possibile creare applicazioni Web lato client complete con Amazon S3 e concedere l'accesso multiorigine alle risorse di Amazon S3 in modo selettivo.

Questa sezione mostra come abilitare CORS utilizzando la console Amazon S3, l'API REST di Amazon S3 e gli SDK. AWS Per configurare il bucket in modo da consentire richieste tra più origini, è necessario aggiungere una configurazione CORS al bucket. La configurazione CORS è un documento in cui sono definite regole che identificano le origini che potranno accedere al bucket, le operazioni (metodi HTTP) supportate per ogni origine e altre informazioni specifiche dell'operazione. Nella console S3, la configurazione CORS deve essere un documento JSON.

Per esempi di configurazioni CORS in JSON e XML, consulta [Elementi di una configurazione CORS](#).

Utilizzo della console S3

In questa sezione viene descritto come utilizzare la console di Amazon S3 per aggiungere una configurazione CORS (Cross-Origin Resource Sharing, condivisione delle risorse multiorigine) a un bucket S3.

Quando si abilita la funzionalità CORS nel bucket, le liste di controllo degli accessi (ACL) e altre policy di autorizzazione di accesso continuano ad essere valide.

 Important

Nella console S3, la configurazione CORS deve essere JSON. Per esempi di configurazioni CORS in JSON e XML, consulta [Elementi di una configurazione CORS](#).

Per aggiungere una configurazione CORS a un bucket S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket, seleziona il nome del bucket per il quale desideri creare una policy di bucket.
4. Seleziona Autorizzazioni.
5. Nella sezione Condivisione Cross-origin delle risorse (CORS), scegli Modifica.
6. Nella casella di testo CORS configuration editor (Editor configurazione CORS), digitare o copiare e incollare una nuova configurazione CORS oppure modificare una configurazione esistente.

La configurazione CORS è un file JSON. Il testo digitato nell'editor deve essere in formato JSON valido. Per ulteriori informazioni, consulta [Elementi di una configurazione CORS](#).

7. Seleziona Salva modifiche.

 Note

Amazon S3 visualizza l'Amazon Resource Name (ARN) per il bucket accanto al titolo CORS configuration editor (Editor configurazione CORS). Per ulteriori informazioni sugli ARN, consulta [Amazon Resource Names \(ARN\) e AWS Service Namespaces](#) nel. Riferimenti generali di Amazon Web Services

Utilizzo di AWS SDK

Puoi utilizzare l' AWS SDK per gestire la condivisione di risorse tra origini (CORS) per un bucket. Per ulteriori informazioni sulla funzionalità CORS, consulta [Utilizzo della funzionalità Cross-Origin Resource Sharing \(CORS\)](#).

Gli esempi seguenti:

- Crea una configurazione CORS e imposta la configurazione su un bucket
- Recupera la configurazione e la modifica aggiungendo una regola
- Aggiunge la configurazione modificata al bucket
- Elimina la configurazione

Java

Example

Example

Per istruzioni su come creare e testare un campione funzionante, consulta [Getting Started](#) nella Developer Guide. AWS SDK per Java

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketCrossOriginConfiguration;
import com.amazonaws.services.s3.model.CORSRule;

import java.io.IOException;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;

public class CORS {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        // Create two CORS rules.
        List<CORSRule.AllowedMethods> rule1AM = new
        ArrayList<CORSRule.AllowedMethods>();
        rule1AM.add(CORSRule.AllowedMethods.PUT);
        rule1AM.add(CORSRule.AllowedMethods.POST);
        rule1AM.add(CORSRule.AllowedMethods.DELETE);
```



```
CORSRule rule1 = new
CORSRule().withId("CORSRule1").withAllowedMethods(rule1AM)
    .withAllowedOrigins(Arrays.asList("http://*.example.com"));

List<CORSRule.AllowedMethods> rule2AM = new
ArrayList<CORSRule.AllowedMethods>();
rule2AM.add(CORSRule.AllowedMethods.GET);
CORSRule rule2 = new
CORSRule().withId("CORSRule2").withAllowedMethods(rule2AM)
    .withAllowedOrigins(Arrays.asList("*")).withMaxAgeSeconds(3000)
    .withExposedHeaders(Arrays.asList("x-amz-server-side-encryption"));

List<CORSRule> rules = new ArrayList<CORSRule>();
rules.add(rule1);
rules.add(rule2);

// Add the rules to a new CORS configuration.
BucketCrossOriginConfiguration configuration = new
BucketCrossOriginConfiguration();
configuration.setRules(rules);

try {
    AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
        .withCredentials(new ProfileCredentialsProvider())
        .withRegion(clientRegion)
        .build();

    // Add the configuration to the bucket.
    s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

    // Retrieve and display the configuration.
    configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
    printCORSConfiguration(configuration);

    // Add another new rule.
    List<CORSRule.AllowedMethods> rule3AM = new
    ArrayList<CORSRule.AllowedMethods>();
    rule3AM.add(CORSRule.AllowedMethods.HEAD);
    CORSRule rule3 = new
    CORSRule().withId("CORSRule3").withAllowedMethods(rule3AM)
        .withAllowedOrigins(Arrays.asList("http://www.example.com"));

    rules = configuration.getRules();
    rules.add(rule3);
```

```

        configuration.setRules(rules);
        s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

        // Verify that the new rule was added by checking the number of rules in
the
        // configuration.
        configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
        System.out.println("Expected # of rules = 3, found " +
configuration.getRules().size());

        // Delete the configuration.
        s3Client.deleteBucketCrossOriginConfiguration(bucketName);
        System.out.println("Removed CORS configuration.");

        // Retrieve and display the configuration to verify that it was
        // successfully deleted.
        configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
        printCORSConfiguration(configuration);
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 couldn't be contacted for a response, or the client
        // couldn't parse the response from Amazon S3.
        e.printStackTrace();
    }
}

private static void printCORSConfiguration(BucketCrossOriginConfiguration
configuration) {
    if (configuration == null) {
        System.out.println("Configuration is null.");
    } else {
        System.out.println("Configuration has " +
configuration.getRules().size() + " rules\n");

        for (CORSRule rule : configuration.getRules()) {
            System.out.println("Rule ID: " + rule.getId());
            System.out.println("MaxAgeSeconds: " + rule.getMaxAgeSeconds());
            System.out.println("AllowedMethod: " + rule.getAllowedMethods());
            System.out.println("AllowedOrigins: " + rule.getAllowedOrigins());
            System.out.println("AllowedHeaders: " + rule.getAllowedHeaders());
            System.out.println("ExposeHeader: " + rule.getExposedHeaders());
        }
    }
}

```

```
        System.out.println();  
    }  
}  
}
```

.NET

Example

Per informazioni sulla configurazione e l'esecuzione degli esempi di codice, consulta [Getting Started with the AWS SDK for .NET](#) nella AWS SDK for .NET Developer Guide.

```
using Amazon;  
using Amazon.S3;  
using Amazon.S3.Model;  
using System;  
using System.Collections.Generic;  
using System.Threading.Tasks;  
  
namespace Amazon.DocSamples.S3  
{  
    class CORSTest  
    {  
        private const string bucketName = "**** bucket name ****";  
        // Specify your bucket region (an example region is shown).  
        private static readonly RegionEndpoint bucketRegion =  
            RegionEndpoint.USWest2;  
        private static IAmazonS3 s3Client;  
  
        public static void Main()  
        {  
            s3Client = new AmazonS3Client(bucketRegion);  
            CORSConfigTestAsync().Wait();  
        }  
        private static async Task CORSConfigTestAsync()  
        {  
            try  
            {  
                // Create a new configuration request and add two rules  
                CORSConfiguration configuration = new CORSConfiguration  
                {  
                    Rules = new System.Collections.Generic.List<CORSRule>
```

```

        {
            new CORSRule
            {
                Id = "CORSRule1",
                AllowedMethods = new List<string> {"PUT", "POST",
"DELETE"},
                AllowedOrigins = new List<string> {"http://
*.example.com"}
            },
            new CORSRule
            {
                Id = "CORSRule2",
                AllowedMethods = new List<string> {"GET"},
                AllowedOrigins = new List<string> {"*"},
                MaxAgeSeconds = 3000,
                ExposeHeaders = new List<string> {"x-amz-server-side-
encryption"}
            }
        }
    };

    // Add the configuration to the bucket.
    await PutCORSConfigurationAsync(configuration);

    // Retrieve an existing configuration.
    configuration = await RetrieveCORSConfigurationAsync();

    // Add a new rule.
    configuration.Rules.Add(new CORSRule
    {
        Id = "CORSRule3",
        AllowedMethods = new List<string> { "HEAD" },
        AllowedOrigins = new List<string> { "http://www.example.com" }
    });

    // Add the configuration to the bucket.
    await PutCORSConfigurationAsync(configuration);

    // Verify that there are now three rules.
    configuration = await RetrieveCORSConfigurationAsync();
    Console.WriteLine();
    Console.WriteLine("Expected # of rulest=3; found:{0}",
configuration.Rules.Count);
    Console.WriteLine();

```

```
        Console.WriteLine("Pause before configuration delete. To continue,
click Enter...");
        Console.ReadKey();

        // Delete the configuration.
        await DeleteCORSConfigurationAsync();

        // Retrieve a nonexistent configuration.
        configuration = await RetrieveCORSConfigurationAsync();
    }
    catch (AmazonS3Exception e)
    {
        Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
    catch (Exception e)
    {
        Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
    }
}

static async Task PutCORSConfigurationAsync(CORSConfiguration configuration)
{
    PutCORSConfigurationRequest request = new PutCORSConfigurationRequest
    {
        BucketName = bucketName,
        Configuration = configuration
    };

    var response = await s3Client.PutCORSConfigurationAsync(request);
}

static async Task<CORSConfiguration> RetrieveCORSConfigurationAsync()
{
    GetCORSConfigurationRequest request = new GetCORSConfigurationRequest
    {
        BucketName = bucketName
    };

    var response = await s3Client.GetCORSConfigurationAsync(request);
    var configuration = response.Configuration;
    PrintCORSRules(configuration);
}
```

```
        return configuration;
    }

    static async Task DeleteCORSConfigurationAsync()
    {
        DeleteCORSConfigurationRequest request = new
DeleteCORSConfigurationRequest
        {
            BucketName = bucketName
        };
        await s3Client.DeleteCORSConfigurationAsync(request);
    }

    static void PrintCORSRules(CORSConfiguration configuration)
    {
        Console.WriteLine();

        if (configuration == null)
        {
            Console.WriteLine("\nConfiguration is null");
            return;
        }

        Console.WriteLine("Configuration has {0} rules:",
configuration.Rules.Count);
        foreach (CORSRule rule in configuration.Rules)
        {
            Console.WriteLine("Rule ID: {0}", rule.Id);
            Console.WriteLine("MaxAgeSeconds: {0}", rule.MaxAgeSeconds);
            Console.WriteLine("AllowedMethod: {0}", string.Join(", ",
rule.AllowedMethods.ToArray()));
            Console.WriteLine("AllowedOrigins: {0}", string.Join(", ",
rule.AllowedOrigins.ToArray()));
            Console.WriteLine("AllowedHeaders: {0}", string.Join(", ",
rule.AllowedHeaders.ToArray()));
            Console.WriteLine("ExposeHeader: {0}", string.Join(", ",
rule.ExposeHeaders.ToArray()));
        }
    }
}
```

Utilizzo della REST API

Per impostare una configurazione CORS nel bucket, è possibile utilizzare la Console di gestione AWS. Se l'applicazione lo richiede, si può inoltre inviare le richieste REST direttamente. Le sezioni seguenti della Documentazione di riferimento delle API di Amazon Simple Storage Service descrivono le operazioni di REST API correlate alla configurazione CORS.

- [PutBucketCors](#)
- [GetBucketCors](#)
- [DeleteBucketCors](#)
- [OPTIONS object](#)

Test di CORS

Per testare la configurazione CORS, è possibile inviare una richiesta di verifica CORS con il metodo OPTIONS in modo che il server possa rispondere se l'invio della richiesta è accettabile. Quando Amazon S3 riceve una richiesta di verifica, S3 valuta la configurazione CORS per il bucket e utilizza la prima regola `CORSRule` corrispondente alla richiesta in entrata per abilitare una richiesta multiorigine. Per garantire la corrispondenza tra la regola e la richiesta, è necessario che siano soddisfatte le condizioni elencate di seguito.

- L'intestazione `Origin` di una richiesta CORS al bucket deve corrispondere alle origini dell'elemento `AllowedOrigins` nella configurazione CORS.
- I metodi HTTP specificati in `Access-Control-Request-Method` in una richiesta CORS al bucket devono corrispondere al metodo o ai metodi elencati nell'elemento `AllowedMethods` della configurazione CORS.
- Le intestazioni elencate nell'intestazione `Access-Control-Request-Headers` di una richiesta di verifica devono corrispondere alle intestazioni dell'elemento `AllowedHeaders` nella configurazione CORS.

Di seguito è riportato un esempio di configurazione CORS. Per creare una configurazione CORS, consulta [Configurazione di CORS](#). Per altri esempi di configurazione CORS, consulta [Elementi di una configurazione CORS](#).

Per indicazioni sulla configurazione e la risoluzione dei problemi delle regole CORS, consulta [Come si configura CORS in Amazon S3 e si confermano le regole CORS utilizzando cURL?](#) nel Knowledge Center. AWS re:Post

JSON

```
[
  {
    "AllowedHeaders": [
      "Authorization"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE"
    ],
    "AllowedOrigins": [
      "http://www.example1.com"
    ],
    "ExposeHeaders": [
      "x-amz-meta-custom-header"
    ]
  }
]
```

Per testare la configurazione CORS, è possibile inviare un controllo OPTIONS di verifica utilizzando il seguente comando CURL. CURL è uno strumento da riga di comando che può essere usato per interagire con S3. Per ulteriori informazioni, consulta [CURL](#).

```
curl -v -X OPTIONS \
-H "Origin: http://www.example1.com" \
-H "Access-Control-Request-Method: PUT" \
-H "Access-Control-Request-Headers: Authorization" \
-H "Access-Control-Expose-Headers: x-amz-meta-custom-header" \
"http://bucket_name.s3.amazonaws.com/object_prefix_name"
```

Nell'esempio precedente, il comando `curl -v -x OPTIONS` viene utilizzato per inviare una richiesta di verifica a S3 per chiedere se S3 consente di inviare una richiesta PUT su un oggetto

dall'origine incrociata `http://www.example1.com`. Le intestazioni `Access-Control-Request-Headers` e `Access-Control-Expose-Headers` sono opzionali.

- In risposta all'intestazione `Access-Control-Request-Method` della richiesta `OPTIONS` di verifica, Amazon S3 restituisce l'elenco dei metodi consentiti se i metodi richiesti corrispondono.
- In risposta all'intestazione `Access-Control-Request-Headers` della richiesta `OPTIONS` di verifica, Amazon S3 restituisce l'elenco delle intestazioni consentite se le intestazioni richieste corrispondono.
- In risposta all'intestazione `Access-Control-Expose-Headers` della richiesta `OPTIONS` di verifica, Amazon S3 restituisce un elenco di intestazioni consentite se le intestazioni richieste corrispondono alle intestazioni consentite a cui possono accedere gli script in esecuzione nel browser.

Note

Quando si invia una richiesta di verifica, se una delle intestazioni della richiesta CORS non è consentita, non viene restituita nessuna delle intestazioni CORS della risposta.

In risposta a questa richiesta `OPTIONS` di verifica, riceverai una risposta `200 OK`. Per i codici di errore più comuni ricevuti durante il test di CORS e ulteriori informazioni per risolvere i problemi relativi a CORS, vedere. [Risoluzione dei problemi di CORS](#)

```
< HTTP/1.1 200 OK
< Date: Fri, 12 Jul 2024 00:23:51 GMT
< Access-Control-Allow-Origin: http://www.example1.com
< Access-Control-Allow-Methods: GET, PUT, POST, DELETE
< Access-Control-Allow-Headers: Authorization
< Access-Control-Expose-Headers: x-amz-meta-custom-header
< Access-Control-Allow-Credentials: true
< Vary: Origin, Access-Control-Request-Headers, Access-Control-Request-Method
< Server: AmazonS3
< Content-Length: 0
```

Risoluzione dei problemi di CORS

I seguenti argomenti sono utili per risolvere alcuni problemi CORS comuni relativi a S3.

Argomenti

- [Errore 403 Accesso negato: CORS non è abilitato per questo bucket](#)
- [Errore 403 Accesso negato: questa richiesta CORS non è consentita](#)
- [Intestazioni non trovate nella risposta CORS](#)
- [Considerazioni su CORS nelle integrazioni proxy S3](#)

Errore 403 Accesso negato: CORS non è abilitato per questo bucket

Il seguente errore 403 `Forbidden` si verifica quando viene inviata una richiesta multiorigine ad Amazon S3 ma CORS non è configurato sul bucket S3.

Errore: HTTP/1.1 403 Risposta CORS proibita: CORS non è abilitato per questo bucket.

La configurazione CORS è un documento o una policy con regole che identificano le origini che potranno accedere al bucket, le operazioni (metodi HTTP) supportate per ogni origine e altre informazioni specifiche dell'operazione. Scopri come [configurare CORS](#) su S3 utilizzando la console Amazon S3, gli AWS SDK e l'API REST. Per ulteriori informazioni su CORS ed esempi di configurazione CORS, consulta [Elementi di CORS](#).

Errore 403 Accesso negato: questa richiesta CORS non è consentita

Il seguente errore 403 `Forbidden` viene ricevuto quando una regola CORS nella configurazione CORS non corrisponde ai dati nella richiesta.

Errore: HTTP/1.1 403 Risposta CORS proibita: questa richiesta CORS non è consentita.

Di conseguenza, questo errore 403 `Forbidden` può verificarsi per diversi motivi:

- L'origine non è consentita.
- I metodi non sono consentiti.
- Le intestazioni richieste non sono consentite.

Per ogni richiesta ricevuta da Amazon S3, è necessario disporre di una regola CORS nella configurazione CORS che corrisponda ai dati nella richiesta.

L'origine non è consentita

L'intestazione `Origin` di una richiesta CORS al bucket deve corrispondere alle origini dell'elemento `AllowedOrigins` nella configurazione CORS. Un carattere jolly ("`*`") nell'elemento

AllowedOrigins corrisponderà a tutti i metodi HTTP. Per ulteriori informazioni su come aggiornare l'elemento AllowedOrigins, consulta [Configuring cross-origin resource sharing \(CORS\)](#).

Ad esempio, se nell'elemento AllowedOrigins è incluso solo il dominio `http://www.example1.com`, una richiesta CORS inviata dal dominio `http://www.example2.com` riceverà l'errore 403 Forbidden.

L'esempio seguente mostra parte di una configurazione CORS che include il dominio `http://www.example1.com` nell'elemento AllowedOrigins.

```
"AllowedOrigins":[
  "http://www.example1.com"
]
```

Affinché una richiesta CORS inviata dal dominio `http://www.example2.com` abbia esito positivo, il dominio `http://www.example2.com` deve essere incluso nell'elemento AllowedOrigins di configurazione CORS.

```
"AllowedOrigins":[
  "http://www.example1.com"
  "http://www.example2.com"
]
```

I metodi non sono consentiti

I metodi HTTP specificati in Access-Control-Request-Method in una richiesta CORS al bucket devono corrispondere al metodo o ai metodi elencati nell'elemento AllowedMethods della configurazione CORS. Un carattere jolly ("*") in AllowedMethods corrisponderà a tutti i metodi HTTP. Per ulteriori informazioni su come aggiornare l'elemento AllowedOrigins, consulta [Configuring cross-origin resource sharing \(CORS\)](#).

Nella configurazione CORS è possibile specificare i metodi seguenti nell'elemento AllowedMethods:

- GET
- PUT
- POST
- DELETE
- HEAD

L'esempio seguente mostra parte di una configurazione CORS che include il metodo GET nell'elemento AllowedMethods. Solo le richieste che includono il metodo GET avranno esito positivo.

```
"AllowedMethods": [
  "GET"
]
```

Se un metodo HTTP (ad esempio, PUT) è stato utilizzato in una richiesta CORS o incluso in una richiesta di verifica CORS al bucket ma il metodo non è presente nella configurazione CORS, la richiesta genererà un errore 403 Forbidden. Per consentire questa richiesta CORS o richiesta di verifica CORS, il metodo PUT deve essere aggiunto alla configurazione CORS.

```
"AllowedMethods": [
  "GET"
  "PUT"
]
```

Le intestazioni richieste non sono consentite

Le intestazioni elencate nell'intestazione Access-Control-Request-Headers di una richiesta di verifica devono corrispondere alle intestazioni dell'elemento AllowedHeaders nella configurazione CORS. Per un elenco di intestazioni comuni che possono essere utilizzate nelle richieste ad Amazon S3, consulta [Common Request Headers](#). Per ulteriori informazioni su come aggiornare l'elemento AllowedHeaders, consulta [Configuring cross-origin resource sharing \(CORS\)](#).

L'esempio seguente mostra parte di una configurazione CORS che include l'intestazione Authorization nell'elemento AllowedHeaders. Solo le richieste per l'intestazione Authorization avranno esito positivo.

```
"AllowedHeaders": [
  "Authorization"
]
```

Se un'intestazione (ad esempio, Content-MD5) è stata inclusa in una richiesta CORS ma l'intestazione non è presente nella configurazione CORS, la richiesta genererà un errore 403 Forbidden. Per consentire questa richiesta CORS, l'intestazione Content-MD5 deve essere aggiunta alla configurazione CORS. Se si desidera passare entrambe le intestazioni

Authorization e **Content-MD5** in una richiesta CORS al bucket, verificare che entrambe le intestazioni siano incluse nell'elemento **AllowedHeaders** della configurazione CORS.

```
"AllowedHeaders": [  
  "Authorization"  
  "Content-MD5"  
]
```

Intestazioni non trovate nella risposta CORS

L'elemento **ExposeHeaders** nella configurazione CORS identifica le intestazioni di risposta che si desidera rendere accessibili agli script e alle applicazioni in esecuzione nei browser, in risposta a una richiesta CORS.

Se gli oggetti archiviati nel bucket S3 hanno metadati definiti dall'utente (ad esempio **x-amz-meta-custom-header**) insieme ai dati di risposta, questa intestazione personalizzata potrebbe contenere metadati o informazioni aggiuntivi a cui desideri accedere dal codice lato client. JavaScript Tuttavia, per impostazione predefinita, i browser bloccano l'accesso alle intestazioni personalizzate per motivi di sicurezza. Per consentire al lato client di accedere alle intestazioni personalizzate, è JavaScript necessario includere l'intestazione nella configurazione CORS.

Nell'esempio seguente, l'intestazione **x-amz-meta-custom-header1** è inclusa nell'elemento **ExposeHeaders**. **x-amz-meta-custom-header2** non è incluso nell'elemento **ExposeHeaders** e manca nella configurazione CORS. Nella risposta, verranno restituiti solo i valori inclusi nell'elemento **ExposeHeaders**. Se la richiesta includesse l'intestazione **x-amz-meta-custom-header2** nell'intestazione **Access-Control-Expose-Headers**, la risposta restituirebbe comunque **200 OK**. Tuttavia, solo l'intestazione consentita, ad esempio **x-amz-meta-custom-header**, verrà restituita e mostrata nella risposta.

```
"ExposeHeaders": [  
  "x-amz-meta-custom-header1"  
]
```

Per garantire che tutte le intestazioni vengano visualizzate nella risposta, aggiungi tutte le intestazioni consentite all'elemento **ExposeHeaders** nella configurazione CORS come mostrato di seguito.

```
"ExposeHeaders": [  
  "x-amz-meta-custom-header1",  
  "x-amz-meta-custom-header2"  
]
```

]

Considerazioni su CORS nelle integrazioni proxy S3

Se riscontri errori e hai già verificato la configurazione CORS sul tuo bucket S3 e la richiesta cross-origin viene inviata a proxy come, prova quanto segue: AWS CloudFront

- Configurare le impostazioni per consentire il metodo `OPTIONS` per le richieste HTTP.
- Configurare il proxy per inoltrare le seguenti intestazioni: `Origin`, `Access-Control-Request-Headers` e `Access-Control-Request-Method`.
- Configurare le impostazioni del proxy in modo da includere l'intestazione di origine nella relativa chiave di cache. Questo è importante perché i proxy di caching che non includono l'intestazione di origine nella loro chiave di cache potrebbero restituire risposte memorizzate che non contengono le intestazioni CORS appropriate per le diverse origini.

Alcuni proxy forniscono funzionalità predefinite per le richieste CORS. Ad esempio, in CloudFront, puoi configurare una policy che includa le intestazioni

che abilitano le richieste CORS (Cross-Origin Resource Sharing) quando l'origine è un bucket Amazon S3.

Questa policy ha le seguenti impostazioni:

- Intestazioni incluse nelle richieste di origine:

`Origin`

`Access-Control-Request-Headers`

`Access-Control-Request-Method`

- Cookie inclusi nelle richieste di origine: Nessuno
- Stringhe di query incluse nelle richieste di origine: Nessuna

Per ulteriori informazioni, consulta [Controllare le richieste di origine con una policy](#) e [Use managed origin request policy](#) nella CloudFront Developer Guide.

Tutorial per siti web statici

I seguenti tutorial o procedure dettagliate presentano procedure complete su come creare e configurare un bucket Amazon S3 per uso generico per l'hosting di siti web statici e l'hosting di streaming video on demand. Lo scopo di questi tutorial è di fornire linee guida generali. I tutorial presentati sono solo esempi con nomi di bucket e utenti destinati a essere usati in un ambiente di laboratorio. Non devono essere utilizzati direttamente nell'ambiente di produzione, senza un'accurata opera di revisione e adattamento alle necessità esclusive del tuo ambiente lavorativo.

- [Hosting di video in streaming su richiesta con Amazon S3 CloudFront, Amazon e Amazon Route 53](#): puoi utilizzare Amazon S3 con Amazon CloudFront per ospitare video per la visualizzazione su richiesta in modo sicuro e scalabile. Dopo che il video è stato impacchettato nei formati giusti, puoi archiviarlo su un server o in un bucket S3 per uso generico e quindi consegnarlo quando gli spettatori lo richiedono. CloudFront In questo tutorial, scoprirai come configurare il tuo bucket generico per ospitare streaming video su richiesta utilizzando Amazon Route 53 per la distribuzione e Amazon Route 53 CloudFront per il Domain Name System (DNS) e la gestione personalizzata dei domini. CloudFront serve il video dalla sua cache, recuperandolo dal bucket generico solo se non è già memorizzato nella cache. Ciò accelera la distribuzione dei video agli spettatori a livello globale con bassa latenza e velocità effettiva e velocità di trasferimento elevate. Per ulteriori informazioni sulla gestione della CloudFront cache, consulta [Optimizing caching and availability nella Amazon Developer Guide](#). CloudFront
- [Configurazione di un sito web statico](#): è possibile configurare un bucket per uso generico in modo da funzionare come un sito web. Questo tutorial illustra i passaggi per ospitare un sito web su Amazon S3, tra cui la creazione di un bucket, l'abilitazione dell'hosting di siti web statici nella console S3, la creazione di un documento indice e la creazione di un documento di errore. Per ulteriori informazioni, consulta [Hosting di un sito web statico tramite Amazon S3](#).
- [Configurazione di un sito web statico utilizzando un dominio personalizzato registrato con Route 53](#): è possibile creare e configurare un bucket per uso generico per ospitare un sito web statico e creare reindirizzamenti su S3 per un sito web con un nome di dominio personalizzato registrato con Amazon Route 53. Route 53 viene utilizzato per registrare domini e definire dove instradare il traffico Internet per il dominio. Questo tutorial illustra come creare record di alias Route 53 che instradano il traffico per un dominio e un sottodominio a un bucket per uso generico contenente un file HTML. Per ulteriori informazioni, consulta [Utilizzo del proprio dominio per un sito web statico in un bucket Amazon S3](#) nella Guida per gli sviluppatori di Amazon Route 53. Dopo aver completato questo tutorial, puoi opzionalmente utilizzarlo CloudFront per migliorare le prestazioni del tuo sito web. Per ulteriori informazioni, consulta [Velocizzare il tuo sito web con Amazon. CloudFront](#)

- [Distribuzione di un sito Web statico su AWS Amplify Hosting da un bucket S3 per uso generico](#): ti consigliamo di utilizzare [AWS Amplify Hosting](#) per ospitare contenuti di siti Web statici archiviati su S3. Amplify Hosting è un servizio completamente gestito che semplifica l'implementazione dei tuoi siti Web su una rete di distribuzione di contenuti (CDN) disponibile a livello globale basata su Amazon CloudFront, consentendo l'hosting sicuro di siti Web statici senza una configurazione estesa. Con AWS Amplify Hosting, puoi selezionare la posizione dei tuoi oggetti all'interno del tuo bucket generico, distribuire i tuoi contenuti su un CDN gestito e generare un URL HTTPS pubblico affinché il tuo sito Web sia accessibile ovunque. Per ulteriori informazioni, consulta [Implementazione di un sito web statico da S3 utilizzando la console Amplify](#) nella Guida per l'utente di Hosting AWS Amplify.

Tutorial: Hosting di video in streaming su richiesta con Amazon S3 CloudFront, Amazon e Amazon Route 53

Puoi usare Amazon S3 con Amazon CloudFront per ospitare video da visualizzare su richiesta in modo sicuro e scalabile. Nello streaming di video on demand (VOD), i contenuti video vengono archiviati su un server e gli spettatori possono guardarli in qualsiasi momento.

CloudFront è un servizio CDN (Content Delivery Network) veloce, altamente sicuro e programmabile. CloudFront è in grado di distribuire i tuoi contenuti in modo sicuro tramite HTTPS da tutte le CloudFront edge location del mondo. Per ulteriori informazioni CloudFront, consulta [Cos'è Amazon CloudFront?](#) nella Amazon CloudFront Developer Guide.

CloudFront il caching riduce il numero di richieste a cui il server di origine deve rispondere direttamente. Quando uno spettatore (utente finale) richiede un video che viene visualizzato CloudFront, la richiesta viene indirizzata a una posizione periferica vicina più vicina a dove si trova lo spettatore. CloudFront serve il video dalla sua cache, recuperandolo dal bucket S3 solo se non è già memorizzato nella cache. Ciò accelera la distribuzione dei video agli spettatori a livello globale con bassa latenza e velocità effettiva e velocità di trasferimento elevate. Per ulteriori informazioni sulla gestione della cache, consulta [Optimizing CloudFront caching and availability nella Amazon Developer Guide](#). CloudFront



Obiettivo

In questo tutorial, configuri un bucket S3 per ospitare streaming video su richiesta utilizzando Amazon Route 53 per la distribuzione e Amazon Route 53 CloudFront per il Domain Name System (DNS) e la gestione personalizzata dei domini.

Argomenti

- [Prerequisiti: registrazione e configurazione di un dominio personalizzato con Route 53](#)
- [Fase 1: Creazione di un bucket S3](#)
- [Fase 2: Caricamento di un video nel bucket S3](#)
- [Fase 3: Creare un'identità di accesso di CloudFront origine](#)
- [Fase 4: Creare una CloudFront distribuzione](#)
- [Fase 5: Accedi al video tramite la distribuzione CloudFront](#)
- [Passaggio 6: configura la CloudFront distribuzione per utilizzare il tuo nome di dominio personalizzato](#)
- [Passaggio 7: accedi al video S3 tramite la CloudFront distribuzione con il nome di dominio personalizzato](#)
- [\(Facoltativo\) Fase 8: Visualizza i dati sulle richieste ricevute dalla tua CloudFront distribuzione](#)

- [Fase 9: Pulizia](#)
- [Fasi successive](#)

Prerequisiti: registrazione e configurazione di un dominio personalizzato con Route 53

Prima di iniziare questo tutorial, devi registrare e configurare un dominio personalizzato (ad esempio, **example.com**) con Route 53 in modo da poter configurare la CloudFront distribuzione per utilizzare un nome di dominio personalizzato in un secondo momento.

Senza un nome di dominio personalizzato, il tuo video S3 è accessibile CloudFront al pubblico e ospitato tramite un URL simile al seguente:

```
https://CloudFront distribution domain name/Path to an S3 video
```

Ad esempio, **https://d111111abcdef8.cloudfront.net/sample.mp4**.

Dopo aver configurato la CloudFront distribuzione per utilizzare un nome di dominio personalizzato configurato con Route 53, il video S3 è accessibile CloudFront al pubblico e ospitato tramite un URL simile al seguente:

```
https://CloudFront distribution alternate domain name/Path to an S3 video
```

Ad esempio, **https://www.example.com/sample.mp4**. Un nome di dominio personalizzato è più semplice e intuitivo da usare per gli spettatori.

Per registrare un nome di dominio, consulta [Registrazione dei nomi di dominio utilizzando Route 53](#) nella Guida per gli sviluppatori di Amazon Route 53.

Quando registri un nome di dominio con Route 53, Route 53 crea automaticamente la zona ospitata, che utilizzerai più avanti in questo tutorial. Questa zona ospitata è dove memorizzi le informazioni su come indirizzare il traffico per il tuo dominio, ad esempio, verso un'istanza o una CloudFront distribuzione di Amazon EC2.

Sono previste tariffe associate alla registrazione del dominio, alla tua zona ospitata e alle query DNS ricevute dal tuo dominio. Per ulteriori informazioni, consulta la [pagina dei Prezzi Amazon Route 53](#).

Note

Quando registri un dominio, il costo è immediato ed è irreversibile. Puoi scegliere di non rinnovare automaticamente il dominio, ma il pagamento è anticipato e resti proprietario per un

anno. Per maggiori informazioni, consulta [Registrazione di un nuovo dominio](#) nella Guida per gli sviluppatori di Amazon Route 53.

Fase 1: Creazione di un bucket S3

Devi creare un bucket per archiviare il video originale che intendi riprodurre in streaming.

Per creare un bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella barra di navigazione, scegli il nome dell'oggetto attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare un bucket.

Note

Scegli una regione nelle tue vicinanze per ridurre al minimo la latenza e i costi o essere conforme ai requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione. Per un elenco di Amazon S3 Regioni AWS, consulta gli [Servizio AWS endpoint](#) in. Riferimenti generali di Amazon Web Services

3. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
4. Scegliere Create bucket (Crea bucket). Viene visualizzata la pagina Create bucket (Crea bucket).
5. Per Nome bucket, immetti un nome per il bucket, ad esempio **tutorial-bucket**.

Per ulteriori informazioni sulle regole di denominazione del bucket in Amazon S3, consulta [Regole di denominazione dei bucket per uso generico](#).

6. Per la regione, scegli la Regione AWS posizione in cui desideri che il bucket risieda.

Se possibile, dovresti scegliere la località della regione che probabilmente sarà più vicina alla maggior parte dei tuoi spettatori. Per ulteriori informazioni sulla Regione del bucket, consulta [Panoramica dei bucket per uso generico](#).

7. In Block Public Access settings for this bucket (Blocca le impostazioni di accesso pubblico per questo bucket), mantieni le impostazioni predefinite (è abilitato Block all public access (Blocca tutto l'accesso pubblico)).

Anche con l'opzione **Blocca** tutti gli accessi pubblici abilitata, gli spettatori possono comunque accedere al video caricato tramite CloudFront. Questa funzionalità è uno dei principali vantaggi dell'utilizzo CloudFront per ospitare un video archiviato in S3.

È consigliabile di lasciare tutte le impostazioni abilitate, a meno che non abbia bisogno di disattivarne una o più per il caso d'uso. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#).

8. Mantieni le impostazioni rimanenti impostate sui valori di default.

(Facoltativo) Se desideri configurare ulteriori impostazioni del bucket per il tuo caso d'uso specifico, consulta [Creazione di un bucket per uso generico](#).

9. Seleziona **Crea bucket**.

Fase 2: Caricamento di un video nel bucket S3

La procedura riportata di seguito illustra come caricare un file video in un bucket S3 utilizzando la console. Quando carichi un video in S3, puoi anche possibile utilizzare [Amazon S3 Transfer Acceleration](#) per configurare trasferimenti di file veloci e sicuri. Transfer Acceleration può velocizzare il caricamento dei video nel bucket S3 per il trasferimento a lunga distanza di video di grandi dimensioni. Per ulteriori informazioni, consulta [Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#).

Per caricare un file nel bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli **Bucket per uso generico**.
3. Nell'elenco **Bucket per uso generico**, seleziona il nome del bucket che hai creato nella [Fase 1](#) (ad es. **tutorial-bucket**) in cui caricare il file.
4. Nella scheda **Oggetti del bucket** seleziona **Carica**.
5. Nella pagina **Upload (Caricamento)**, sotto **Files and Folders (File e cartelle)** scegli **Add Files (Aggiungi file)**.
6. Seleziona un file da caricare, quindi scegli **Apri**.

Ad esempio, puoi caricare un file video denominato `sample.mp4`.

7. Scegli **Carica**.

Fase 3: Creare un'identità di accesso di CloudFront origine

Per limitare l'accesso diretto al video dal tuo bucket S3, crea un CloudFront utente speciale chiamato origin access identity (OAI). In questo tutorial, assocerai l'OAI alla distribuzione. Utilizzando un OAI, ti assicuri che gli spettatori non possano bypassare CloudFront e ottenere il video direttamente dal bucket S3. Solo l' CloudFront OAI può accedere al file nel bucket S3. Per ulteriori informazioni, consulta [Limitare l'accesso a un'origine Amazon S3](#) nella Amazon Developer Guide. CloudFront

Important

Se il bucket che stai utilizzando per ospitare il tuo sito Web statico è stato crittografato utilizzando la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS), devi utilizzare il controllo dell'accesso all'origine (OAC) anziché l'identità di accesso all'origine (OAI) per proteggere l'origine. OAI non supporta SSE-KMS, quindi è necessario utilizzare invece OAC. Per ulteriori informazioni su OAC, consulta [Limitare l'accesso a un'origine Amazon S3](#) nella Amazon Developer Guide. CloudFront

Per creare un OAI CloudFront

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Nel pannello di navigazione sulla sinistra, nella sezione Sicurezza, scegli Accesso origine.
3. Nella scheda Identità, scegli Crea identità di accesso origine.
4. Immediatamente inserisci un nome (ad esempio, **S3-OAI**) come nuova identità di accesso origine.
5. Scegli Crea.

Fase 4: Creare una CloudFront distribuzione

Per CloudFront utilizzarlo per servire e distribuire il video nel tuo bucket S3, devi creare una CloudFront distribuzione.

Fasi secondarie

- [Crea una distribuzione CloudFront](#)
- [Revisione della policy del bucket](#)

Crea una distribuzione CloudFront

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Nel riquadro di navigazione a sinistra, scegliere Distribuzioni.
3. Scegli Create Distribution (Crea distribuzione).
4. Nella sezione Origine, per Dominio origine scegli il nome di dominio dell'origine S3, che inizia con il nome del bucket S3 creato nella [Fase 1](#) (ad esempio, **tutorial-bucket**).
5. Per Accesso origine, seleziona Identità di accesso legacy.
6. In Identità di accesso origine, scegli l'identità di accesso all'origine esistente creata nella [Fase 3](#) (ad esempio, **S3-OAI**).
7. In Bucket policy (Policy del bucket), scegli Yes, update the bucket policy (Sì, aggiorna la policy del bucket).
8. In Funzionamento cache predefinito, nella sezione Policy protocollo visualizzatore, scegli Reindirizza HTTP a HTTPS.

Questo significa che le richieste HTTP vengono reindirizzate automaticamente a HTTPS per proteggere il tuo sito Web e proteggere i dati degli spettatori.

9. Per le altre impostazioni nella sezione Default Cache Behavior Settings (Modifica impostazioni comportamento cache), accettare i valori predefiniti.

(Facoltativo) Puoi controllare per quanto tempo il file rimane nella CloudFront cache prima di CloudFront inoltrare un'altra richiesta all'origine. Riducendo la durata, puoi distribuire contenuti dinamici. Aumentando la durata, i visualizzatori otterranno prestazioni migliori, poiché è più probabile che i file vengano distribuiti direttamente dalla cache edge. Una durata maggiore riduce anche il carico sul server di origine. Per ulteriori informazioni, consulta [Gestire la durata della permanenza dei contenuti nella cache \(scadenza\)](#) nella Amazon CloudFront Developer Guide.

10. Per le altre sezioni, mantieni le impostazioni rimanenti impostate sui valori predefiniti.

Per ulteriori informazioni sulle diverse opzioni di impostazione, consulta [Valori specificati durante la creazione o l'aggiornamento di una distribuzione](#) nella Amazon CloudFront Developer Guide.

11. Scegli Create Distribution (Crea distribuzione).
12. Nella scheda Generale della CloudFront distribuzione, in Dettagli, il valore della colonna Ultima modifica per la distribuzione cambia da Distribuzione al timestamp dell'ultima modifica della distribuzione. In genere sono necessari pochi minuti.

Revisione della policy del bucket

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco dei bucket, scegli il nome del bucket che hai usato in precedenza come origine della tua CloudFront distribuzione (ad esempio,). **tutorial-bucket**
4. Scegli la scheda Autorizzazioni.
5. Nella casella di testo Bucket policy (Policy del bucket) conferma di visualizzare una formulazione simile alla seguente:

```
{
  "Version": "2008-10-17",
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
Identity EH1HDMB1FH2TC"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::tutorial-bucket/*"
    }
  ]
}
```

Questa è la dichiarazione che la CloudFront distribuzione ha aggiunto alla tua policy bucket quando hai scelto Sì, aggiorna la policy del bucket in precedenza.

Questo aggiornamento della policy del bucket indica che la CloudFront distribuzione è stata configurata correttamente per limitare l'accesso al bucket S3. A causa di questa restrizione, è possibile accedere agli oggetti nel bucket solo tramite la distribuzione. CloudFront

Fase 5: Accedi al video tramite la distribuzione CloudFront

Ora CloudFront puoi servire il video archiviato nel tuo bucket S3. Per accedere al tuo video tramite CloudFront, devi combinare il nome del tuo dominio di CloudFront distribuzione con il percorso del video nel bucket S3.

Per creare un URL per il video S3 utilizzando il nome di dominio di distribuzione CloudFront

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Nel riquadro di navigazione a sinistra, scegliere Distribuzioni.
3. Per ottenere il nome di dominio della distribuzione, procedi come indicato di seguito:
 - a. Nella colonna Origini, trova la CloudFront distribuzione corretta cercando il nome di origine, che inizia con il bucket S3 che hai creato nel [passaggio 1](#) (ad esempio, **tutorial-bucket**).
 - b. Dopo aver trovato la distribuzione nell'elenco, amplia la colonna Nome di dominio per copiare il valore del nome di dominio per la distribuzione. CloudFront
4. In una nuova scheda del browser, incolla il nome di dominio della distribuzione copiato in precedenza.
5. Torna alla scheda precedente del browser e apri la console S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
6. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
7. Nell'elenco Buckets (Bucket) scegli il nome del bucket creato nella [Fase 1](#) (ad esempio, **tutorial-bucket**).
8. Nell'elenco Objects (Oggetti) scegli il nome del video che hai caricato nella [Fase 2](#) ai fini dello streaming (ad esempio, `sample.mp4`).
9. Nella pagina prodotto dell'oggetto, nella Panoramica dell'oggetto sezione, copiare il valore della Chiave. Questo valore è il percorso dell'oggetto video caricato nel bucket S3.
10. Torna alla scheda del browser in cui hai precedentemente incollato il nome del dominio di distribuzione, inserisci una barra di inoltro (/) dopo il nome del dominio di distribuzione, quindi incolla il percorso al video copiato in precedenza (ad esempio, `sample.mp4`).

Ora, il tuo video S3 è accessibile CloudFront al pubblico e ospitato tramite un URL simile al seguente:


```
https://CloudFront distribution domain name/Path to the S3 video
```

Sostituisci *CloudFront distribution domain name* e *Path to the S3 video* con i valori appropriati. Un esempio di URL è **https://d111111abcdef8.cloudfront.net/sample.mp4**.

Passaggio 6: configura la CloudFront distribuzione per utilizzare il tuo nome di dominio personalizzato

Per utilizzare il tuo nome di dominio anziché il nome di CloudFront dominio nell'URL per accedere al video S3, aggiungi un nome di dominio alternativo alla tua CloudFront distribuzione.

Fasi secondarie

- [Richiesta di un certificato SSL](#)
- [Aggiungi il nome di dominio alternativo alla tua distribuzione CloudFront](#)
- [Crea un record DNS per indirizzare il traffico dal tuo nome di dominio alternativo al nome di dominio della tua distribuzione CloudFront](#)
- [Controllo dell'abilitazione di IPv6 per la distribuzione ed eventuale creazione di un altro registro DNS](#)

Richiesta di un certificato SSL

Per consentire ai tuoi spettatori di utilizzare HTTPS e il tuo nome di dominio personalizzato nell'URL per lo streaming video, utilizza AWS Certificate Manager (ACM) per richiedere un certificato Secure Sockets Layer (SSL). Il certificato SSL stabilisce una connessione di rete crittografata al sito Web.

1. Accedi Console di gestione AWS e apri la console ACM all'indirizzo. <https://console.aws.amazon.com/acm/>
2. Se viene visualizzata la pagina introduttiva, in Provision certificates (Fornisci certificati), scegli Get Started (Inizia).
3. Nella pagina Richiedi un certificato scegli Richiedi un certificato pubblico e poi di nuovo Richiedi un certificato.
4. Nella pagina Aggiungi nomi di dominio, inserisci il nome di dominio completo (FQDN) del sito che desideri proteggere con un certificato. SSL/TLS Utilizza un asterisco (*) per

richiedere un certificato jolly che protegge diversi nomi di siti nello stesso dominio. In questo tutorial, digita * e il nome di dominio personalizzato configurato in [Prerequisiti](#). Ad esempio, immettere *.example.come quindi scegliere Successivo.

Per ulteriori informazioni, consulta [Per richiedere un certificato pubblico ACM \(console\)](#) nella Guida per l'utente di AWS Certificate Manager .

5. Nella pagina Select validation method (Seleziona metodo di convalida), scegli DNS validation (Convalida DNS). Quindi, seleziona Successivo.

Se si è in grado di modificare la configurazione DNS, si consiglia di utilizzare la convalida del dominio DNS anziché la convalida email. La convalida del DNS offre diversi vantaggi rispetto alla convalida dell'email. Per ulteriori informazioni, consulta [Opzione 1: convalida DNS](#) nella AWS Certificate Manager Guida per l'utente di.

6. (Facoltativo) Nella pagina Aggiungi tag puoi contrassegnare facoltativamente il certificato con metadati.
7. Scegli Rivedi.
8. Nella pagina Revisione, verifica che le informazioni presenti in Nome dominio e Metodo di convalida siano corrette. Dopodiché, seleziona Confirm and request (Conferma e richiedi).

La pagina Convalida mostra che la richiesta è in fase di elaborazione e che il dominio certificato viene convalidato. I certificati in attesa di convalida hanno lo stato Pending validation (Convalida in attesa).

9. Nella pagina Convalida, scegli la freccia verso il basso a sinistra del nome di dominio personalizzato e seleziona Crea registro in Route 53 per convalidare la proprietà del dominio tramite DNS.

In questo modo viene aggiunto un record CNAME fornito da AWS Certificate Manager alla configurazione DNS.

10. Nella casella di dialogo Create record in Route 53 (Crea registro in Route 53), scegli Create (Crea).

La pagina di convalida dovrebbe visualizzare una notifica sullo stato di successo.

11. Scegli Continue (Continua) per visualizzare la pagina elenco Certificates (Certificati).

Lo Stato del nuovo certificato passerà da Convalida in attesa a Emesso entro 30 minuti.

Aggiungi il nome di dominio alternativo alla tua distribuzione CloudFront

1. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Nel riquadro di navigazione a sinistra, scegliere Distribuzioni.
3. Scegli l'ID della distribuzione creata nella [Fase 4](#).
4. Sul General tab, vai all'Impostazioni sezione, e scegli Modificare.
5. Nella pagina Modifica impostazioni, per Nome di dominio alternativo (CNAME) - opzionale , scegli Aggiungi elemento per aggiungere i nomi di dominio personalizzati che desideri utilizzare nell'URL del video S3 fornito da questa distribuzione. CloudFront

In questo tutorial, ad esempio, se desideri instradare il traffico a un sottodominio, ad esempio `www.example.com`, inserisci il nome del sottodominio (`www`) con il nome di dominio (`example.com`). In particolare, inserisci **`www.example.com`**.

Note

Il nome di dominio alternativo (CNAME) che aggiungi deve essere coperto dal certificato SSL che hai precedentemente allegato alla tua distribuzione. CloudFront

6. In Certificato SSL personalizzato - facoltativo, scegli il certificato SSL richiesto in precedenza (ad esempio, **`*.example.com`**).

Note

Se il certificato SSL non viene visualizzato immediatamente dopo averlo richiesto, attendi 30 minuti, quindi aggiorna l'elenco fino a quando il certificato SSL diventa disponibile per la selezione.

7. Mantieni le impostazioni rimanenti impostate sui valori predefiniti. Scegli Save changes (Salva modifiche).
8. Nella scheda Generale per la distribuzione, attendi che il valore di Ultima modifica passi da Implementazione in corso al timestamp dell'ultima modifica della distribuzione.

Crea un record DNS per indirizzare il traffico dal tuo nome di dominio alternativo al nome di dominio della tua distribuzione CloudFront

1. Accedi Console di gestione AWS e apri la console Route 53 all'indirizzo. <https://console.aws.amazon.com/route53/>
2. Nel riquadro di navigazione a sinistra, scegliere Hosted zones (Zone ospitate).
3. Nella pagina Zone ospitate seleziona il nome della zona ospitata creata da Route 53 in [Prerequisiti](#) (ad esempio, **example.com**).
4. Scegliere Creare recorde quindi usa il Creazione rapida record metodo.
5. Per Record name, mantieni il valore del nome del record uguale al nome di dominio alternativo della CloudFront distribuzione che hai aggiunto in precedenza.

In questo tutorial, per instradare il traffico a un sottodominio, ad esempio `www.example.com`, inserisci il nome del sottodominio senza il nome di dominio. Ad esempio, inserisci solo **www** nel campo di testo prima del nome di dominio personalizzato.

6. Per Tipo di record, scegli A - Indirizza il traffico verso un indirizzo IPv4 e alcune risorse. AWS
7. In Valore, scegli l'attivazione/disattivazione Alias per abilitare la risorsa Alias.
8. In Instrada il traffico verso, scegli Alias alla CloudFront distribuzione dall'elenco a discesa.
9. Nella casella di ricerca che dice Scegli la distribuzione, scegli il nome di dominio della CloudFront distribuzione che hai creato nel [passaggio 4](#).

Per trovare il nome di dominio della tua CloudFront distribuzione, procedi come segue:

- a. In una nuova scheda del browser, accedi a Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v3/home>.
 - b. Nel riquadro di navigazione a sinistra, scegliere Distribuzioni.
 - c. Nella colonna Origini, trova la CloudFront distribuzione corretta cercando il nome di origine, che inizia con il bucket S3 che hai creato nel [passaggio 1](#) (ad esempio, **tutorial-bucket**).
 - d. Dopo aver trovato la distribuzione nell'elenco, allarga la colonna Nome di dominio per visualizzare il valore del nome di dominio per la tua distribuzione. CloudFront
10. Sul Creare record Nella console Route 53, per le impostazioni rimanenti, mantenere i valori predefiniti.
 11. Scegli Crea record.

Controllo dell'abilitazione di IPv6 per la distribuzione ed eventuale creazione di un altro registro DNS

Se IPv6 è abilitato per la distribuzione, devi creare un altro registro DNS.

1. Per verificare se IPv6 è abilitato per la distribuzione, procedi come indicato di seguito:

- a. Accedi a Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
- b. Nel riquadro di navigazione a sinistra, scegliere Distribuzioni.
- c. Scegli l'ID della CloudFront distribuzione che hai creato nel [passaggio 4](#).
- d. Nella scheda Generale, in Impostazioni, controlla se IPv6 è impostato su Abilitato.

Se IPv6 è abilitato per la distribuzione, devi creare un altro registro DNS.

2. Se IPv6 è abilitato per la distribuzione, crea un registro DNS eseguendo le seguenti operazioni:

- a. Accedi Console di gestione AWS e apri la console Route 53 all'indirizzo <https://console.aws.amazon.com/route53/>.
- b. Nel riquadro di navigazione a sinistra, scegliere Hosted zones (Zone ospitate).
- c. Nella pagina Zone ospitate seleziona il nome della zona ospitata creata da Route 53 in [Prerequisiti](#) (ad esempio, **example.com**).
- d. Scegliere Creare recorde quindi usa il Creazione rapida record metodo.
- e. In Nome registro, nel campo di testo che precede il nome di dominio personalizzato, digita lo stesso valore inserito quando hai creato in precedenza il registro DNS IPv4. Ad esempio, in questo tutorial, per instradare il traffico a `www.example.com`, inserisci solo **www**.
- f. In Tipo di record, seleziona AAAA - Instrada il traffico su un indirizzo IPv6 e su alcune risorse AWS.
- g. In Valore, scegli l'attivazione/disattivazione Alias per abilitare la risorsa Alias.
- h. In Indirizza il traffico verso, scegli Alias da CloudFront distribuire dall'elenco a discesa.
- i. Nella casella di ricerca che dice Scegli la distribuzione, scegli il nome di dominio della CloudFront distribuzione che hai creato nel [passaggio 4](#).
- j. Mantieni le impostazioni rimanenti impostate sui valori di default.
- k. Scegli Crea record.

Passaggio 7: accedi al video S3 tramite la CloudFront distribuzione con il nome di dominio personalizzato

Per accedere al video S3 utilizzando l'URL personalizzato, devi combinare il nome di dominio alternativo con il percorso del video nel bucket S3.

Per creare un URL personalizzato per accedere al video S3 tramite la distribuzione CloudFront

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Nel riquadro di navigazione a sinistra, scegliere Distribuzioni.
3. Per ottenere il nome di dominio alternativo della tua CloudFront distribuzione, procedi come segue:
 - a. Nella colonna Origini, trova la CloudFront distribuzione corretta cercando il nome di origine, che inizia con il nome del bucket S3 per il bucket che hai creato nel [passaggio 1](#) (ad esempio,). **tutorial-bucket**
 - b. Dopo aver trovato la distribuzione nell'elenco, amplia la colonna Nomi di dominio alternativi per copiare il valore del nome di dominio alternativo della tua distribuzione. CloudFront
4. In una nuova scheda del browser, incolla il nome di dominio alternativo della distribuzione. CloudFront
5. Torna alla scheda precedente del browser e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
6. Trova il percorso per il video S3, come spiegato nella [Fase 5](#).
7. Torna alla scheda del browser in cui hai precedentemente incollato il nome di dominio alternativo, continua digitando / e incolla il percorso al video S3 (ad esempio, sample.mp4).

Ora, il tuo video S3 è accessibile CloudFront al pubblico e ospitato tramite un URL personalizzato simile al seguente:

```
https://CloudFront distribution alternate domain name/Path to the S3 video
```

Sostituisci *CloudFront distribution alternate domain name* e *Path to the S3 video* con i valori appropriati. Un esempio di URL è **https://www.example.com/sample.mp4**.

(Facoltativo) Fase 8: Visualizza i dati sulle richieste ricevute dalla tua CloudFront distribuzione

Per visualizzare i dati sulle richieste ricevute dalla CloudFront distribuzione

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Nel pannello di navigazione sulla sinistra, in Report e analisi dei dati, scegli i report dalla console, che vanno da Statistiche sulla cache, Oggetti popolari, Referrer principali, Utilizzo e Visualizzatori.

Puoi filtrare il pannello di controllo di ogni report. Per ulteriori informazioni, consulta [CloudFront Reports nella Console](#) nella Amazon CloudFront Developer Guide.

3. Per filtrare i dati, scegli l'ID della CloudFront distribuzione che hai creato nel [passaggio 4](#).

Fase 9: Pulizia

Se hai ospitato un video in streaming S3 utilizzando CloudFront Route 53 solo come esercizio di apprendimento, elimina le AWS risorse che hai allocato in modo da non accumulare più addebiti.

Note

Quando registri un dominio, il costo è immediato ed è irreversibile. Puoi scegliere di non rinnovare automaticamente il dominio, ma il pagamento è anticipato e resti proprietario per un anno. Per maggiori informazioni, consulta [Registrazione di un nuovo dominio](#) nella Guida per gli sviluppatori di Amazon Route 53.

Fasi secondarie

- [Elimina la distribuzione CloudFront](#)
- [Eliminazione del registro DNS](#)
- [Eliminazione della zona ospitata pubblica per il dominio personalizzato](#)
- [Eliminazione del nome di dominio personalizzato da Route 53](#)
- [Eliminazione del video originale nel bucket S3 di origine](#)
- [Eliminazione del bucket S3 di origine](#)

Elimina la distribuzione CloudFront

1. Accedi Console di gestione AWS e apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Nel riquadro di navigazione a sinistra, scegliere Distribuzioni.
3. Nella colonna Origini, trova la CloudFront distribuzione corretta cercando il nome di origine, che inizia con il nome del bucket S3 per il bucket che hai creato nel [passaggio 1](#) (ad esempio,). **tutorial-bucket**
4. Per eliminare la CloudFront distribuzione, devi prima disabilitarla.
 - Se il valore della colonna Stato è Abilitato e il valore di Ultima modifica è il timestamp dell'ultima modifica della distribuzione, procedi a disabilitare la distribuzione prima di eliminarla.
 - Se il valore di Stato è Abilitato e il valore di Ultima modifica è In corso di implementazione, attendi fino a quando il valore di Stato passa al timestamp dell'ultima modifica della distribuzione. Quindi procedi a disabilitare la distribuzione prima di eliminarla.
5. Per disabilitare la CloudFront distribuzione, procedi come segue:
 - a. Nella Distribuzioni Selezionare la casella di controllo accanto all'ID della distribuzione che si desidera eliminare.
 - b. Per disabilitare la distribuzione, scegli Disabilita (e poi di nuovo Disabilita per confermare).

Se disabiliti una distribuzione a cui è associato un nome di dominio alternativo, CloudFront smette di accettare traffico per quel nome di dominio (ad esempio `www.example.com`), anche se un'altra distribuzione ha un nome di dominio alternativo con un carattere jolly (*) che corrisponde allo stesso dominio (ad esempio). `*.example.com`
 - c. Il valore di Status (Stato) cambia immediatamente in Disabled (Disabilitato). Attendere fino a quando il valore di Ultima modifica passa da Implementazione in corso al timestamp dell'ultima modifica della distribuzione.

Poiché è CloudFront necessario propagare questa modifica a tutte le edge location, potrebbero essere necessari alcuni minuti prima che l'aggiornamento sia completo e sia disponibile l'opzione Elimina per eliminare la distribuzione.
6. Per eliminare la distribuzione disabilitata, procedi come indicato di seguito:
 - a. Selezionare la casella di controllo accanto all'ID della distribuzione che si desidera eliminare.
 - b. Scegli Elimina e seleziona Elimina per confermare.

Eliminazione del registro DNS

Se si desidera eliminare la zona ospitata pubblica per il dominio (incluso il record DNS), vedere [Eliminazione della zona ospitata pubblica per il dominio personalizzato](#) nella Guida per sviluppatori di Amazon Route 53. Se desideri solo eliminare il registro DNS creato nella [Fase 6](#), procedi come segue:

1. Accedi a Console di gestione AWS e apri la console Route 53 all'indirizzo <https://console.aws.amazon.com/route53/>.
2. Nel riquadro di navigazione a sinistra, scegliere Hosted zones (Zone ospitate).
3. Nella pagina Zone ospitate seleziona il nome della zona ospitata creata da Route 53 in [Prerequisiti](#) (ad esempio, **example.com**).
4. Nell'elenco dei registri, seleziona quelli che desideri eliminare (i registri creati nella [Fase 6](#)).

Note

Non è possibile eliminare i record con un valore di Tipo pari a NS o SOA.

5. Seleziona Delete records (Elimina registri).
6. Per confermare l'eliminazione, scegliere Delete (Elimina).

Le modifiche ai registri richiedono tempo per propagarsi ai server DNS di Route 53. Attualmente, l'unico modo per verificare che le modifiche si siano propagate è utilizzare l'azione [GetChange](#) API. In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

Eliminazione della zona ospitata pubblica per il dominio personalizzato

Warning

Se desideri mantenere la registrazione del tuo dominio ma interrompere il routing del traffico Internet sul tuo sito o applicazione Web, ti consigliamo di eliminare i registri nella zona ospitata (come sopra) invece di eliminare la zona ospitata.

Inoltre, se elimini una zona ospitata, qualcuno potrebbe utilizzare il dominio e instradare il traffico verso le proprie risorse utilizzando il tuo nome di dominio.

Se elimini una zona ospitata, non puoi annullarne l'eliminazione. Devi creare una nuova zona ospitata e aggiornare i server di nomi per la registrazione del tuo dominio, operazione che può richiedere fino a 48 ore per rendere effettiva la modifica.

Se desideri rendere il dominio non disponibile su Internet, per prima cosa puoi trasferire il servizio DNS su un servizio DNS gratuito e quindi eliminare la zona ospitata di Route 53. In questo modo si impedisce che query DNS future vengano instradate in modo non corretto.

1. Se il dominio è registrato con Route 53, consulta [Aggiunta o modifica di server di nomi e glue record per un dominio](#) nella Guida per gli sviluppatori di Amazon Route 53 per informazioni su come sostituire i server di nomi di Route 53 con i server di nomi per il nuovo servizio DNS.
2. Se il dominio è registrato con un altro registrar, utilizza il metodo fornito dal registrar per modificare i server di nomi per il dominio.

 Note

Se stai eliminando una zona ospitata per un sottodominio (`www.example.com`), non devi modificare i server di nomi per il dominio (`example.com`).

1. Accedi Console di gestione AWS e apri la console Route 53 all'indirizzo <https://console.aws.amazon.com/route53/>.
2. Nel riquadro di navigazione a sinistra, scegliere Hosted zones (Zone ospitate).
3. Nella pagina Hosted zones (Zone ospitate), scegli il nome della zona ospitata che desideri eliminare.
4. Nella scheda Records (Registri) della zona ospitata, conferma che la zona ospitata che desideri eliminare contiene solo un registro NS e uno SOA.

Se contiene registri aggiuntivi, eliminali.

Se hai creato record NS per sottodomini nella zona ospitata, elimina anche questi.

5. Nella scheda DNSSEC signing (Firma DNSSEC) per la zona ospitata, disabilita la firma DNSSEC, se abilitata. Per ulteriori informazioni, consulta [Registrazione delle query DNS](#) nella Guida per sviluppatori di Amazon Route 53.
6. Nella pagina dei dettagli della zona ospitata, scegli Elimina zona.
7. Per confermare l'eliminazione immetti **delete**, quindi scegli Elimina.

Eliminazione del nome di dominio personalizzato da Route 53

Per la maggior parte dei domini di primo livello (TLD), è possibile eliminare la registrazione, se non è più necessaria. Se elimini una registrazione di nome di dominio da Route 53 prima della scadenza prevista per la registrazione, AWS non viene rimborsata la quota di registrazione. Per maggiori informazioni, consulta [Eliminazione della registrazione di un nome di dominio](#) nella Guida per gli sviluppatori di Amazon Route 53.

Important

Se desideri trasferire il dominio da un altro registrar Account AWS o trasferirlo a un altro registrar, non eliminare il dominio e aspettati di registrarlo nuovamente immediatamente. Al contrario, consulta la documentazione relativo nella sezione Guida per sviluppatori di Amazon Route 53:

- [Trasferimento di un dominio a un altro Account AWS](#)
- [Trasferimento di un dominio da Amazon Route 53 a un altro registrar](#)

Eliminazione del video originale nel bucket S3 di origine

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Nome bucket scegli il nome del bucket in cui hai caricato il video originale nella [Fase 2](#) (ad esempio, **tutorial-bucket**).
4. Nella scheda Oggetti, seleziona la casella di controllo a sinistra del nome dell'oggetto da eliminare (ad esempio, `sample.mp4`).
5. Scegliere Elimina.
6. **UNDER**Eliminare permanentemente gli oggetti?, immettere **permanently delete** per confermare di voler eliminare questo oggetto.
7. Scegliere Delete objects (Elimina oggetti).

Eliminazione del bucket S3 di origine

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).
3. Nell'elenco Bucket scegli il pulsante di opzione accanto al nome del bucket creato nella [Fase 1](#) (ad esempio, **tutorial-bucket**).
4. Scegliere Elimina.
5. Nella pagina Delete bucket (Elimina bucket) conferma che desideri eliminare il bucket inserendone il nome nel campo di testo e quindi scegli Delete bucket (Elimina bucket).

Fasi successive

Dopo aver completato questo tutorial, puoi esplorare altri casi d'uso correlati:

- Transcodifica i video S3 nei formati di streaming necessari per un particolare televisore o dispositivo connesso prima di ospitare questi video con una distribuzione. CloudFront

Per utilizzare Amazon S3 Batch Operations AWS Lambda e transcodificare AWS Elemental MediaConvert in batch una raccolta di video in una varietà di formati multimediali di output, consulta. [Tutorial: video con S3 Batch Operations Batch-transcoding](#)

- Ospita altri oggetti archiviati in S3, come immagini, audio, grafica animata, fogli di stile, HTML, JavaScript app React e così via, utilizzando e Route 53. CloudFront

Per un esempio, consulta [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#) e [Velocizza il tuo sito Web con Amazon CloudFront](#).

- Utilizza [Amazon S3 Transfer Acceleration](#) per configurare trasferimenti di file veloci e sicuri. Transfer Acceleration può velocizzare il caricamento dei video nel bucket S3 per il trasferimento a lunga distanza di video di grandi dimensioni. Transfer Acceleration migliora le prestazioni di trasferimento indirizzando il traffico attraverso le edge location distribuite CloudFront a livello globale e sulle AWS reti backbone. Utilizza anche ottimizzazioni del protocollo di rete. Per ulteriori informazioni, consulta [Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration](#).

Esercitazione: configurazione di un sito Web statico su Amazon S3

Important

Amazon S3 ora applica la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) come livello di base della crittografia per ogni bucket di Amazon S3. A partire dal

5 gennaio 2023, tutti i caricamenti di nuovi oggetti su Amazon S3 vengono crittografati automaticamente senza costi aggiuntivi e senza alcun impatto sulle prestazioni. Lo stato di crittografia automatico per la configurazione di crittografia predefinita del bucket S3 e per il caricamento di nuovi oggetti è disponibile nei CloudTrail log, in S3 Inventory, S3 Storage Lens, nella console Amazon S3 e come intestazione di risposta dell'API Amazon S3 aggiuntiva nella e. AWS CLI AWS SDKs Per ulteriori informazioni, consulta [Domande frequenti sulla crittografia predefinita](#).

È possibile configurare un bucket Amazon S3 in modo da funzionare come un sito web. Questo esempio guida attraverso le fasi di hosting di un sito web su Amazon S3.

Important

Il seguente tutorial richiede la disabilitazione dell'opzione Blocco dell'accesso pubblico. È consigliabile mantenere l'impostazione Blocco dell'accesso pubblico abilitata. Se desideri mantenere abilitate tutte e quattro le impostazioni Block Public Access e ospitare un sito Web statico, puoi utilizzare Amazon CloudFront Origin Access Control (OAC). Amazon CloudFront offre le funzionalità necessarie per configurare un sito Web statico sicuro. I siti Web statici Amazon S3 supportano solo gli endpoint HTTP. Amazon CloudFront utilizza lo storage durevole di Amazon S3 fornendo al contempo intestazioni di sicurezza aggiuntive, come HTTPS. HTTPS aggiunge sicurezza crittografando una normale richiesta HTTP e proteggendo contro o più comuni attacchi informatici. Per ulteriori informazioni, consulta la sezione [Guida introduttiva a un sito Web statico sicuro](#) nella Amazon CloudFront Developer Guide.

Argomenti

- [Fase 1: creazione di un bucket](#)
- [Fase 2: abilitazione dell'hosting di un sito Web statico](#)
- [Fase 3: modificare le impostazioni di blocco dell'accesso pubblico](#)
- [Fase 4: aggiunta di una policy del bucket che renda il contenuto del bucket disponibile pubblicamente](#)
- [Fase 5: configurazione di un documento indice](#)
- [Fase 6: configurare un documento di errore](#)
- [Fase 7: testare l'endpoint del sito Web](#)

- [Fase 8: Pulizia](#)

Fase 1: creazione di un bucket

Le istruzioni riportate di seguito forniscono una panoramica su come creare i bucket per l'hosting di siti Web. Per step-by-step istruzioni dettagliate sulla creazione di un bucket, consulta [Creazione di un bucket per uso generico](#).

Per creare un bucket

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegliere Create bucket (Crea bucket).
3. Specifica Nome del bucket (ad esempio, **example.com**).
4. Scegliere la regione in cui creare il bucket.

Scegli una regione geografica vicina a te per ridurre al minimo la latenza e i costi e soddisfare i requisiti normativi. La regione scelta determina l'endpoint del sito web Amazon S3. Per ulteriori informazioni, consulta [Endpoint del sito Web](#).

5. Per accettare le impostazioni predefinite e creare il bucket, scegliere Create (Crea).

Fase 2: abilitazione dell'hosting di un sito Web statico

Dopo aver creato un bucket, è possibile abilitare l'hosting di siti Web statici per il bucket. Puoi creare un nuovo bucket o utilizzare un bucket esistente.

Per abilitare l'hosting di un sito Web statico

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
3. Nell'elenco dei bucket, seleziona il nome del bucket per cui desideri abilitare l'hosting di siti web statici.
4. Scegliere Properties (Proprietà).
5. In Hosting di siti Web statici, seleziona Modifica.
6. Seleziona Utilizza questo bucket per l'hosting di un sito Web.

7. In Hosting di siti Web statici, seleziona Abilita.
8. In Documento di indice immettere il nome file del documento di indice, in genere `index.html`.

Il nome del documento indice fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome del file del documento indice HTML che si prevede di caricare nel bucket S3. Quando si configura un bucket per l'hosting di siti Web, è necessario specificare un documento di indice. Amazon S3 restituisce questo documento di indice quando si eseguono richieste per il dominio root o per una delle sottocartelle. Per ulteriori informazioni, consulta [Configurazione di un documento indice](#).

9. Per fornire il tuo documento di errore personalizzato per gli errori di classe 4XX, specifica il nome file del documento in Documento di errore.

Il nome del documento di errore fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome del file del documento di errore HTML che si prevede di caricare nel bucket S3. Se non si specifica un documento di errore personalizzato e si verifica un errore, Amazon S3 restituisce un documento di errore HTML predefinito. Per ulteriori informazioni, consulta [Configurazione di un documento di errore personalizzato](#).

10. (Facoltativo) Per specificare regole di reindirizzamento avanzate, utilizza JSON per descrivere le regole in Regole reindirizzamento.

Ad esempio, è possibile instradare le richieste in base a prefissi o nomi della chiave dell'oggetto specifici nella richiesta. Per ulteriori informazioni, consulta [Configurazione delle regole di reindirizzamento per utilizzare i reindirizzamenti condizionali avanzati](#).

11. Seleziona Salva modifiche.

Amazon S3 abilita l'hosting statico del sito web per il tuo bucket. Nella parte inferiore della pagina, in Hosting di siti Web statici, viene visualizzato l'endpoint del sito web per il bucket.

12. In Hosting sito Web statico, prendi nota dell'endpoint.

Endpoint è l'endpoint del sito web Amazon S3 per il bucket. Dopo aver configurato il bucket come sito Web statico, è possibile utilizzare questo endpoint per testare il sito Web.

Fase 3: modificare le impostazioni di blocco dell'accesso pubblico

Per impostazione predefinita, Amazon S3 blocca l'accesso pubblico all'account e ai bucket. Per utilizzare un bucket per ospitare un sito Web statico, puoi seguire questa procedura per modificare le impostazioni di blocco dell'accesso pubblico:

⚠ Warning

Prima di completare questi passaggi, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#) per assicurarsi di aver compreso e accettato i rischi connessi alla concessione dell'accesso pubblico. Quando si disattivano le impostazioni di blocco dell'accesso pubblico per rendere pubblico il bucket, chiunque su Internet può accedere al bucket. Consigliamo di bloccare tutti gli accessi pubblici ai bucket.

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Seleziona il nome del bucket configurato come sito Web statico.
3. Seleziona Autorizzazioni.
4. In Blocca accesso pubblico (impostazioni bucket), seleziona Modifica.
5. Deseleziona Blocca tutto l'accesso pubblico, quindi seleziona Salva modifiche.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 

**Account settings for Block Public Access are currently turned on**

[Account settings for Block Public Access](#) that are enabled apply even if they are disabled for this bucket.

- ☐ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
 - ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
 - ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
 - ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
 - ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Amazon S3 disattiva le impostazioni di blocco dell'accesso pubblico per il bucket. Per creare un sito web pubblico statico, potrebbe essere necessario [modificare anche le impostazioni di blocco dell'accesso pubblico](#) per l'account prima di aggiungere una policy del bucket. Se le impostazioni dell'account per il blocco dell'accesso pubblico sono attualmente attivate, verrà visualizzata una nota in Blocca accesso pubblico (impostazioni bucket).

Fase 4: aggiunta di una policy del bucket che renda il contenuto del bucket disponibile pubblicamente

Dopo aver modificato le impostazioni di blocco dell'accesso pubblico S3, è possibile aggiungere una policy del bucket per concedere l'accesso pubblico in lettura al bucket. Quando concedi l'accesso pubblico in lettura, chiunque su Internet può accedere al bucket.

Important

La policy seguente è solo un esempio e consente l'accesso completo ai contenuti del bucket. Prima di continuare con questa fase, esamina l'argomento relativo a [come proteggere i file nel bucket Amazon S3](#) per assicurarti di comprendere le best practice per la protezione dei file nel bucket S3 e i rischi connessi alla concessione dell'accesso pubblico .

1. In Bucket, scegli il nome del bucket.
2. Seleziona Autorizzazioni.
3. In Policy del bucket, seleziona Modifica.
4. Per concedere l'accesso in lettura pubblico al sito Web, copiare la policy del bucket seguente e incollarla in Editor della policy del bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
    }
  ],
}
```

```
        "Resource": [
            "arn:aws:s3:::Bucket-Name/*"
        ]
    }
]
```

5. Aggiorna Resource al tuo nome bucket.

Nell'esempio precedente, bucket policy, *Bucket-Name* è un segnaposto per il nome del bucket. Per utilizzare questa policy di bucket con il proprio bucket, è necessario aggiornare il nome in modo che corrisponda al bucket.

6. Seleziona Salva modifiche.

Viene visualizzato un messaggio che indica che la policy del bucket è stata aggiunta correttamente.

Se viene visualizzato l'errore `Policy has invalid resource`, conferma che il nome del bucket nella policy di bucket corrisponde al nome del bucket. Per informazioni sull'aggiunta di una policy del bucket, consulta [In che modo aggiungere una policy del bucket S3?](#)

Se viene visualizzato un messaggio di errore e non è possibile salvare la policy di bucket, controlla le impostazioni di blocco dell'accesso pubblico all'account e al bucket per confermare che consenti l'accesso pubblico al bucket.

Fase 5: configurazione di un documento indice

Quando si abilita l'hosting statico di siti Web per il bucket, si immette il nome del documento di indice (ad esempi, **index.html**). Dopo aver abilitato l'hosting di siti Web statici per il bucket, si carica un file HTML con il nome del documento di indice nel bucket.

Per configurare il documento di indice

1. Creare un file `index.html`

Se non si dispone di un file `index.html`, è possibile utilizzare il seguente codice HTML per crearne uno:

```
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
```

```
<title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
</html>
```

2. Salva il file indice in locale.

Il nome del file del documento indice deve corrispondere esattamente al nome del documento indice immesso nella finestra di dialogo Hosting sito Web statico. Il nome del documento indice distingue tra maiuscole e minuscole. Ad esempio, se si immette `index.html` per il nome del documento Indice nella finestra di dialogo Hosting sito Web statico, anche il nome del file del documento indice deve essere `index.html` e non `Index.html`.

3. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
4. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
5. Nell'elenco dei bucket, seleziona il nome del bucket che desideri utilizzare per l'hosting di un sito web statico.
6. Abilitare l'hosting di siti Web statici per il bucket e inserire il nome esatto del documento di indice (ad esempi, `index.html`). Per ulteriori informazioni, consulta [Abilitazione dell'hosting di siti Web](#).

Dopo aver abilitato l'hosting di siti Web statici, procedere alla fase 6.

7. Per caricare il documento di indice nel bucket, eseguire una delle operazioni seguenti:
 - Trascinare e rilasciare il file di indice nell'elenco bucket della console.
 - Scegliere Upload (Carica) e seguire le istruzioni per scegliere e caricare il file di indice.

Per step-by-step istruzioni, consulta [Caricamento degli oggetti](#).

8. (Opzionale) Caricare altri contenuti del sito Web nel bucket.

Fase 6: configurare un documento di errore

Quando abiliti l'hosting di siti Web statici per il tuo bucket, specifichi il nome del documento di errore (ad esempio, **404.html**). Dopo avere abilitato l'hosting di siti Web statici per il bucket, carichi un file HTML con il nome del documento di errore nel bucket.

Per configurare un documento di errore

1. Crea un documento di errore, ad esempio `404.html`.
2. Salva il file del documento di errore in locale.

Il nome del documento di errore fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome immesso quando hai attivato l'hosting statico di siti Web. Ad esempio, se specifichi `404.html` per il nome del documento di errore nella finestra di dialogo Hosting sito Web statico, anche il nome file del documento di errore dovrà essere `404.html`.

3. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
4. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
5. Nell'elenco dei bucket, seleziona il nome del bucket che desideri utilizzare per l'hosting di un sito web statico.
6. Abilita l'hosting di siti Web statici per il bucket e inserisci il nome esatto del documento di errore (ad esempio, `404.html`). Per ulteriori informazioni, consultare [Abilitazione dell'hosting di siti Web](#) e [Configurazione di un documento di errore personalizzato](#).

Dopo aver abilitato l'hosting di siti Web statici, procedere alla fase 6.

7. Per caricare il documento di errore nel bucket, completa una delle operazioni riportate di seguito:
 - Trascina e rilascia il file del documento di errore nell'elenco dei bucket della console.
 - Scegliere Upload (Carica) e seguire le istruzioni per scegliere e caricare il file di indice.

Per step-by-step istruzioni, consulta [Caricamento degli oggetti](#).

Fase 7: testare l'endpoint del sito Web

Dopo aver configurato l'hosting di siti Web statici per il bucket, puoi testare l'endpoint del sito Web.

 Note

Amazon S3 non supporta l'accesso HTTPS al sito web. Se desideri utilizzare HTTPS, puoi utilizzare Amazon CloudFront per servire un sito Web statico ospitato su Amazon S3.

Per ulteriori informazioni, consulta [Come si usa CloudFront per servire un sito Web statico ospitato su Amazon S3?](#) e [Richiede HTTPS per la comunicazione tra gli spettatori e](#)

CloudFront

1. In Bucket, scegli il nome del bucket.
2. Scegliere Properties (Proprietà).
3. Nella parte inferiore della pagina, in Static website hosting (Hosting di siti Web statici), scegliere il proprio Bucket website endpoint (Endpoint del sito web Bucket).

Il documento indice viene aperto in una finestra del browser separata.

Ora hai un sito Web ospitato su Amazon S3. Questo sito web è disponibile nell'endpoint del sito web Amazon S3. Tuttavia, potresti disporre di un dominio, come `example.com`, che desideri utilizzare per fornire il contenuto dal sito Web creato. Inoltre, potresti voler utilizzare il supporto del dominio root Amazon S3 per servire richieste di `http://www.example.com` e `http://example.com`. Ciò richiede ulteriori fasi. Per un esempio, consulta [Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53](#).

Fase 8: Pulizia

Se hai creato il sito Web statico solo come esercizio di apprendimento, elimina le risorse AWS che hai allocato per non accumulare più addebiti. Dopo aver eliminato le AWS risorse, il sito Web non è più disponibile. Per ulteriori informazioni, consulta [Eliminazione di un bucket per uso generico](#).

Tutorial: Configurazione di un sito Web statico utilizzando un dominio personalizzato registrato con Route 53

Supponiamo che si desideri effettuare l'hosting di un sito Web statico su Amazon S3. Hai registrato un dominio su Amazon Route 53 (ad esempio `example.com`) e desideri che le richieste `http://www.example.com` e `http://example.com` vengano inviate dai tuoi contenuti Amazon S3. È possibile utilizzare questa procedura dettagliata per informazioni su come ospitare un sito web statico e creare reindirizzamenti su Amazon S3 per un sito web con un nome di dominio personalizzato

registrato con Route 53. È possibile utilizzare un sito Web esistente che si desidera ospitare su Amazon S3 o utilizzare questa procedura dettagliata per iniziare da zero.

Dopo aver completato questa procedura dettagliata, puoi opzionalmente utilizzare Amazon CloudFront per migliorare le prestazioni del tuo sito web. Per ulteriori informazioni, consulta [Velocizza il tuo sito Web con Amazon CloudFront](#).

Note

Gli endpoint del sito Web di Amazon S3 non supportano HTTPS o access point. Se desideri utilizzare HTTPS, puoi utilizzare Amazon CloudFront per servire un sito Web statico ospitato su Amazon S3.

Per un tutorial su come ospitare i tuoi contenuti in modo sicuro con CloudFront Amazon S3, consulta [Tutorial: Hosting di video in streaming su richiesta con Amazon S3 CloudFront, Amazon e Amazon Route 53](#) Per ulteriori informazioni, consulta [Come si usa CloudFront per servire un sito Web statico ospitato su Amazon S3?](#) e [Richiede HTTPS per la comunicazione tra gli spettatori e](#) CloudFront

Automatizzazione della configurazione di siti Web statici con un CloudFormation modello

È possibile utilizzare un CloudFormation modello per automatizzare la configurazione statica del sito Web. Il CloudFormation modello configura i componenti necessari per ospitare un sito Web statico sicuro in modo che possiate concentrarvi maggiormente sui contenuti del sito Web e meno sulla configurazione dei componenti.

Il CloudFormation modello include i seguenti componenti:

- Amazon S3 – Crea un bucket Amazon S3 per ospitare il tuo sito Web statico.
- CloudFront — Crea una CloudFront distribuzione per velocizzare il tuo sito web statico.
- Lambda@Edge – Utilizza [Lambda@Edge](#) per aggiungere intestazioni di sicurezza a ogni risposta del server. Le intestazioni di sicurezza sono un gruppo di intestazioni nella risposta del server Web che indicano ai browser Web di adottare ulteriori precauzioni di sicurezza. Per ulteriori informazioni, consulta il post del blog [Aggiungere intestazioni di sicurezza HTTP usando Lambda @Edge e Amazon](#). CloudFront

Questo CloudFormation modello può essere scaricato e utilizzato. Per informazioni e istruzioni, consulta la sezione Guida [introduttiva a un sito Web statico sicuro](#) nella Amazon CloudFront Developer Guide.

Argomenti

- [Prima di iniziare](#)
- [Fase 1: registrazione di un dominio personalizzato con Route 53](#)
- [Fase 2: creare due bucket](#)
- [Fase 3: configurazione di un bucket del dominio root per l'hosting di siti Web](#)
- [Fase 4: configurare un bucket del sottodominio per il reindirizzamento del sito Web](#)
- [Fase 5: configurare la registrazione del traffico del sito Web](#)
- [Fase 6: caricare l'indice e il contenuto del sito Web](#)
- [Fase 7: caricare un documento di errore](#)
- [Fase 8: modificare le impostazioni dell'accesso pubblico ai blocchi S3](#)
- [Fase 9: collegare una policy del bucket](#)
- [Fase 10: testare l'endpoint del dominio](#)
- [Fase 11: aggiungere record alias per il dominio e il sottodominio](#)
- [Fase 12: testare il sito Web](#)
- [Velocizza il tuo sito Web con Amazon CloudFront](#)
- [Pulizia delle risorse di esempio](#)

Prima di iniziare

Seguendo l'esempio si utilizzeranno i seguenti servizi:

Amazon Route 53 – Usa Route 53 per registrare domini e definire dove instradare il traffico internet per il dominio. L'esempio illustra come creare record di alias Route 53 che instradano il traffico per il dominio (`example.com`) e il sottodominio (`www.example.com`) a un bucket Amazon S3 contenente un file HTML.

Amazon S3 – Viene utilizzato per creare bucket Amazon S3, caricare una pagina di esempio del sito Web, configurare le autorizzazioni per permettere agli utenti di visualizzare il contenuto e configurare i bucket per l'hosting di siti Web.

Fase 1: registrazione di un dominio personalizzato con Route 53

Se non si dispone già di un nome di dominio registrato, ad esempio `example.com`, registrarne uno con Route 53. Per maggiori informazioni, consulta [Registrazione di un nuovo dominio](#) nella Guida per gli sviluppatori di Amazon Route 53. Dopo aver registrato il nome di dominio, è possibile creare e configurare i bucket Amazon S3 per l'hosting di siti Web.

Fase 2: creare due bucket

Per le richieste di supporto del dominio root e del sottodominio, occorre creare due bucket:

- Bucket del dominio – `example.com`
- Bucket del sottodominio – `www.example.com`

Questi nomi di bucket devono corrispondere esattamente al nome di dominio. In questo esempio, il nome di dominio è `example.com`. Il contenuto viene ospitato al di fuori del bucket del dominio root (`example.com`). Viene creata una richiesta di reindirizzamento per il bucket del sottodominio (`www.example.com`). In altre parole, se qualcuno accede a `www.example.com` dal proprio browser, viene reindirizzato a `example.com` e visualizza il contenuto ospitato nel bucket Amazon S3 con quel nome.

Per creare i bucket per l'hosting di siti Web

Le istruzioni riportate di seguito forniscono una panoramica su come creare i bucket per l'hosting di siti Web. Per istruzioni dettagliate sulla creazione di un bucket, consulta [Creazione di un bucket per uso generico](#).

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Seleziona il bucket del dominio root:
 - a. Nella barra di navigazione, scegli il nome del file attualmente visualizzato Regione AWS. Quindi, scegli la Regione in cui creare un bucket.

Note

Scegli una regione nelle tue vicinanze per ridurre al minimo la latenza e i costi o essere conforme ai requisiti normativi. Gli oggetti archiviati in una regione non la lasciano mai a meno che non vengano trasferiti esplicitamente in un'altra regione.

Per un elenco di Amazon S3 Regioni AWS, consulta gli [Servizio AWS endpoint](#) in. Riferimenti generali di Amazon Web Services

- b. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
- c. Scegliere Create bucket (Crea bucket). Viene visualizzata la pagina Create bucket (Crea bucket).
- d. Specifica Nome del bucket (ad esempio, **example.com**).
- e. Scegliere la regione in cui creare il bucket.

Scegli una regione geografica vicina a te per ridurre al minimo la latenza e i costi e soddisfare i requisiti normativi. La regione scelta determina l'endpoint del sito web Amazon S3. Per ulteriori informazioni, consulta [Endpoint del sito Web](#).

- f. Per accettare le impostazioni predefinite e creare il bucket, scegliere Create (Crea).
3. Crea il tuo bucket del sottodominio:
- a. Scegliere Create bucket (Crea bucket).
 - b. Specifica Nome del bucket (ad esempio, **www.example.com**).
 - c. Scegliere la regione in cui creare il bucket.

Scegli una regione geografica vicina a te per ridurre al minimo la latenza e i costi e soddisfare i requisiti normativi. La regione scelta determina l'endpoint del sito web Amazon S3. Per ulteriori informazioni, consulta [Endpoint del sito Web](#).

- d. Per accettare le impostazioni predefinite e creare il bucket, scegliere Create (Crea).

Nella fase seguente **example.com** viene configurato per l'hosting di siti Web.

Fase 3: configurazione di un bucket del dominio root per l'hosting di siti Web

In questa fase, configuri il bucket del dominio root (**example.com**) come sito Web. Questo bucket conterrà i contenuti del sito Web. Quando si configura un bucket per l'hosting di siti Web, è possibile accedere al sito web utilizzando il [Endpoint del sito Web](#).

Per abilitare l'hosting di un sito Web statico

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.

3. Nell'elenco dei bucket, seleziona il nome del bucket per cui desideri abilitare l'hosting di siti web statici.
4. Scegliere Properties (Proprietà).
5. In Hosting di siti Web statici, seleziona Modifica.
6. Seleziona Utilizza questo bucket per l'hosting di un sito Web.
7. In Hosting di siti Web statici, seleziona Abilita.
8. In Documento di indice immettere il nome file del documento di indice, in genere `index.html`.

Il nome del documento indice fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome del file del documento indice HTML che si prevede di caricare nel bucket S3. Quando si configura un bucket per l'hosting di siti Web, è necessario specificare un documento di indice. Amazon S3 restituisce questo documento di indice quando si eseguono richieste per il dominio root o per una delle sottocartelle. Per ulteriori informazioni, consulta [Configurazione di un documento indice](#).

9. Per fornire il tuo documento di errore personalizzato per gli errori di classe 4XX, specifica il nome file del documento in Documento di errore.

Il nome del documento di errore fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome del file del documento di errore HTML che si prevede di caricare nel bucket S3. Se non si specifica un documento di errore personalizzato e si verifica un errore, Amazon S3 restituisce un documento di errore HTML predefinito. Per ulteriori informazioni, consulta [Configurazione di un documento di errore personalizzato](#).

10. (Facoltativo) Per specificare regole di reindirizzamento avanzate, utilizza JSON per descrivere le regole in Regole reindirizzamento.

Ad esempio, è possibile instradare le richieste in base a prefissi o nomi della chiave dell'oggetto specifici nella richiesta. Per ulteriori informazioni, consulta [Configurazione delle regole di reindirizzamento per utilizzare i reindirizzamenti condizionali avanzati](#).

11. Seleziona Salva modifiche.

Amazon S3 abilita l'hosting statico del sito web per il tuo bucket. Nella parte inferiore della pagina, in Hosting di siti Web statici, viene visualizzato l'endpoint del sito web per il bucket.

12. In Hosting sito Web statico, prendi nota dell'endpoint.

Endpoint è l'endpoint del sito web Amazon S3 per il bucket. Dopo aver configurato il bucket come sito Web statico, è possibile utilizzare questo endpoint per testare il sito Web.

Dopo aver [modificato le impostazioni di blocco dell'accesso pubblico](#) e aver [aggiunto una policy del bucket](#) che consente l'accesso pubblico in lettura, potrai utilizzare l'endpoint del sito Web per accedere al sito Web.

Nella fase successiva viene configurato il sottodominio (`www.example.com`) per reindirizzare le richieste al dominio (`example.com`).

Fase 4: configurare un bucket del sottodominio per il reindirizzamento del sito Web

Una volta che il bucket del dominio root è stato configurato per l'hosting di siti Web, è possibile configurare il bucket del sottodominio per reindirizzare tutte le richieste al dominio. In questo esempio, tutte le richieste per `www.example.com` vengono reindirizzate a `example.com`.

Per configurare una richiesta di reindirizzamento

1. Nella console di Amazon S3, nell'elenco Bucket per uso generico, seleziona il bucket del sottodominio (in questo esempio, `www.example.com`).
2. Scegliere Properties (Proprietà).
3. In Hosting di siti Web statici, seleziona Modifica.
4. Seleziona Reindirizza richieste per un oggetto.
5. Nella casella Target bucket (Bucket di destinazione) immettere il dominio root, ad esempio, **example.com**.
6. In Protocol (Protocollo), scegliere HTTP.
7. Seleziona Salva modifiche.

Fase 5: configurare la registrazione del traffico del sito Web

Per tenere traccia del numero di visitatori che accedono al sito Web, puoi abilitare facoltativamente la registrazione per il bucket del dominio root. Per ulteriori informazioni, consulta [Registrazione delle richieste con registrazione dell'accesso al server](#). Se prevedi di utilizzare Amazon CloudFront per velocizzare il tuo sito Web, puoi anche utilizzare CloudFront la registrazione.

Per abilitare la registrazione dell'accesso al server per il bucket del dominio root

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nella stessa regione in cui è stato creato il bucket configurato come sito Web statico, creare un bucket per la registrazione, ad esempio `logs.example.com`.

3. Creare una cartella per i file di registrazione degli accessi al server (ad esempio, logs).
4. (Facoltativo) Se desideri utilizzarla CloudFront per migliorare le prestazioni del tuo sito Web, crea una cartella per i file di CloudFront registro (ad esempio,cdn).

 Important

Quando crei o aggiorni una distribuzione e abiliti la CloudFront registrazione, CloudFront aggiorna l'elenco di controllo degli accessi ai bucket (ACL) per concedere all'awslogsdeliveryaccount le FULL_CONTROL autorizzazioni per scrivere i log nel bucket. Per ulteriori informazioni, consulta la sezione [Autorizzazioni necessarie per configurare la registrazione standard e accedere ai file di registro](#) nella Amazon CloudFront Developer Guide. Se il bucket che memorizza i log utilizza l'impostazione imposta dal proprietario del bucket per S3 Object Ownership per disabilitare gli ACL, non può scrivere log nel bucket. CloudFront Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

5. Nell'elenco Buckets (Bucket) scegliere il bucket del dominio root.
6. Scegliere Properties (Proprietà).
7. In Registrazione accesso server, seleziona Modifica.
8. Scegli Enable (Abilita).
9. In Bucket di destinazione, seleziona la destinazione del bucket e della cartella per i log di accesso al server:
 - Individua la cartella e il percorso del bucket:
 1. Seleziona Sfoglia S3.
 2. Scegli il nome del bucket, quindi seleziona la cartella dei log.
 3. Seleziona Scegli percorso.
 - Specifica il percorso del bucket S3, ad esempio, s3://logs.example.com/logs/.
10. Seleziona Salva modifiche.

Nel bucket di log, ora puoi accedere ai tuoi log. Amazon S3 scrive i log di accesso del sito web nel bucket log ogni due ore.

Fase 6: caricare l'indice e il contenuto del sito Web

In questo passaggio carichi il documento di indice e il contenuto facoltativo del sito Web nel bucket del dominio root.

Quando si abilita l'hosting statico di siti Web per il bucket, si immette il nome del documento di indice (ad esempi, **index.html**). Dopo aver abilitato l'hosting di siti Web statici per il bucket, si carica un file HTML con il nome del documento di indice nel bucket.

Per configurare il documento di indice

1. Creare un file `index.html`

Se non si dispone di un file `index.html`, è possibile utilizzare il seguente codice HTML per crearne uno:

```
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
  <title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
</html>
```

2. Salva il file indice in locale.

Il nome del file del documento indice deve corrispondere esattamente al nome del documento indice immesso nella finestra di dialogo Hosting sito Web statico. Il nome del documento indice distingue tra maiuscole e minuscole. Ad esempio, se si immette `index.html` per il nome del documento Indice nella finestra di dialogo Hosting sito Web statico, anche il nome del file del documento indice deve essere `index.html` e non `Index.html`.

3. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
4. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
5. Nell'elenco dei bucket, seleziona il nome del bucket che desideri utilizzare per l'hosting di un sito web statico.

6. Abilitare l'hosting di siti Web statici per il bucket e inserire il nome esatto del documento di indice (ad esempi, `index.html`). Per ulteriori informazioni, consulta [Abilitazione dell'hosting di siti Web](#).

Dopo aver abilitato l'hosting di siti Web statici, procedere alla fase 6.

7. Per caricare il documento di indice nel bucket, eseguire una delle operazioni seguenti:
 - Trascinare e rilasciare il file di indice nell'elenco bucket della console.
 - Scegliere Upload (Carica) e seguire le istruzioni per scegliere e caricare il file di indice.

Per istruzioni dettagliate, consulta [Caricamento degli oggetti](#).

8. (Opzionale) Caricare altri contenuti del sito Web nel bucket.

Fase 7: caricare un documento di errore

Quando abiliti l'hosting di siti Web statici per il tuo bucket, specifichi il nome del documento di errore (ad esempio, **404.html**). Dopo avere abilitato l'hosting di siti Web statici per il bucket, carichi un file HTML con il nome del documento di errore nel bucket.

Per configurare un documento di errore

1. Crea un documento di errore, ad esempio `404.html`.
2. Salva il file del documento di errore in locale.

Il nome del documento di errore fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome immesso quando hai attivato l'hosting statico di siti Web. Ad esempio, se specifichi `404.html` per il nome del documento di errore nella finestra di dialogo Hosting sito Web statico, anche il nome file del documento di errore dovrà essere `404.html`.

3. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
4. Nel riquadro di navigazione sinistro, scegli Bucket per uso generico.
5. Nell'elenco dei bucket, seleziona il nome del bucket che desideri utilizzare per l'hosting di un sito web statico.
6. Abilita l'hosting di siti Web statici per il bucket e inserisci il nome esatto del documento di errore (ad esempio, `404.html`). Per ulteriori informazioni, consultare [Abilitazione dell'hosting di siti Web](#) e [Configurazione di un documento di errore personalizzato](#).

Dopo aver abilitato l'hosting di siti Web statici, procedere alla fase 6.

7. Per caricare il documento di errore nel bucket, completa una delle operazioni riportate di seguito:
 - Trascina e rilascia il file del documento di errore nell'elenco dei bucket della console.
 - Scegliere Upload (Carica) e seguire le istruzioni per scegliere e caricare il file di indice.

Per istruzioni dettagliate, consulta [Caricamento degli oggetti](#).

Fase 8: modificare le impostazioni dell'accesso pubblico ai blocchi S3

In questo esempio, è possibile modificare le impostazioni di blocco dell'accesso pubblico per il bucket di dominio (example.com) per consentire l'accesso pubblico.

Per impostazione predefinita, Amazon S3 blocca l'accesso pubblico all'account e ai bucket. Per utilizzare un bucket per ospitare un sito Web statico, puoi seguire questa procedura per modificare le impostazioni di blocco dell'accesso pubblico:

Warning

Prima di completare questi passaggi, consulta [Blocco dell'accesso pubblico allo storage Amazon S3](#) per assicurarsi di aver compreso e accettato i rischi connessi alla concessione dell'accesso pubblico. Quando si disattivano le impostazioni di blocco dell'accesso pubblico per rendere pubblico il bucket, chiunque su Internet può accedere al bucket. Consigliamo di bloccare tutti gli accessi pubblici ai bucket.

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Seleziona il nome del bucket configurato come sito Web statico.
3. Seleziona Autorizzazioni.
4. In Blocca accesso pubblico (impostazioni bucket), seleziona Modifica.
5. Deseleziona Blocca tutto l'accesso pubblico, quindi seleziona Salva modifiche.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 



Account settings for Block Public Access are currently turned on

Account settings for Block Public Access that are enabled apply even if they are disabled for this bucket.

- ☐ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
 - ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
 - ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
 - ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
 - ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Amazon S3 disattiva le impostazioni di blocco dell'accesso pubblico per il bucket. Per creare un sito web pubblico statico, potrebbe essere necessario [modificare anche le impostazioni di blocco dell'accesso pubblico](#) per l'account prima di aggiungere una policy del bucket. Se le impostazioni dell'account per il blocco dell'accesso pubblico sono attualmente attivate, verrà visualizzata una nota in Blocca accesso pubblico (impostazioni bucket).

Fase 9: collegare una policy del bucket

In questo esempio, si collega una policy del bucket al bucket di dominio (example.com) per consentire l'accesso pubblico in lettura. Ad esempio, sostituisci la policy del bucket dell'esempio con il nome del bucket del tuo dominio. *Bucket-Name* example.com

Dopo aver modificato le impostazioni di blocco dell'accesso pubblico S3, è possibile aggiungere una policy del bucket per concedere l'accesso pubblico in lettura al bucket. Quando concedi l'accesso pubblico in lettura, chiunque su Internet può accedere al bucket.

 Important

La policy seguente è solo un esempio e consente l'accesso completo ai contenuti del bucket. Prima di continuare con questa fase, esamina l'argomento relativo a [come proteggere i file nel bucket Amazon S3](#) per assicurarti di comprendere le best practice per la protezione dei file nel bucket S3 e i rischi connessi alla concessione dell'accesso pubblico .

1. In Bucket, scegli il nome del bucket.
2. Seleziona Autorizzazioni.
3. In Policy del bucket, seleziona Modifica.
4. Per concedere l'accesso in lettura pubblico al sito Web, copiare la policy del bucket seguente e incollarla in Editor della policy del bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::Bucket-Name/*"
      ]
    }
  ]
}
```

5. Aggiorna Resource al tuo nome bucket.

Nell'esempio precedente, bucket policy, *Bucket-Name* è un segnaposto per il nome del bucket. Per utilizzare questa policy di bucket con il proprio bucket, è necessario aggiornare il nome in modo che corrisponda al bucket.

6. Seleziona Salva modifiche.

Viene visualizzato un messaggio che indica che la policy del bucket è stata aggiunta correttamente.

Se viene visualizzato l'errore `Policy has invalid resource`, conferma che il nome del bucket nella policy di bucket corrisponde al nome del bucket. Per informazioni sull'aggiunta di una policy del bucket, consulta [In che modo aggiungere una policy del bucket S3?](#)

Se viene visualizzato un messaggio di errore e non è possibile salvare la policy di bucket, controlla le impostazioni di blocco dell'accesso pubblico all'account e al bucket per confermare che consenti l'accesso pubblico al bucket.

Nella prossima fase, è possibile determinare gli endpoint del sito Web e testare l'endpoint del dominio.

Fase 10: testare l'endpoint del dominio

Dopo aver configurato il bucket di dominio per ospitare un sito Web pubblico, puoi testare l'endpoint. Per ulteriori informazioni, consulta [Endpoint del sito Web](#). Sarai in grado di testare l'endpoint solo per il bucket di dominio, poiché il bucket del sottodominio è impostato per il reindirizzamento del sito Web e non per l'hosting statico del sito Web.

Note

Amazon S3 non supporta l'accesso HTTPS al sito web. Se desideri utilizzare HTTPS, puoi utilizzare Amazon CloudFront per servire un sito Web statico ospitato su Amazon S3. Per ulteriori informazioni, consulta [Come si usa CloudFront per servire un sito Web statico ospitato su Amazon S3?](#) e [Richiede HTTPS per la comunicazione tra gli spettatori e CloudFront](#).

1. In Bucket, scegli il nome del bucket.
2. Scegliere Properties (Proprietà).
3. Nella parte inferiore della pagina, in Static website hosting (Hosting di siti Web statici), scegliere il proprio Bucket website endpoint (Endpoint del sito web Bucket).

Il documento indice viene aperto in una finestra del browser separata.

Nella prossima fase ci si servirà di Amazon Route 53 per consentire ai clienti di utilizzare entrambi gli URL personalizzati per spostarsi nel sito.

Fase 11: aggiungere record alias per il dominio e il sottodominio

In questa fase, creare i record alias che si aggiungono alla zona ospitata per le mappe di dominio `example.com` e `www.example.com`. Aniché usare indirizzi IP, i record alias utilizzano gli endpoint dei siti Web Amazon S3. Amazon Route 53 conserva la mappatura dei record alias e degli indirizzi IP dove risiedono i bucket Amazon S3. Creare due record di alias, uno per il dominio root e uno per il sottodominio.

Aggiungere un record di alias per il dominio root e il sottodominio

Per aggiungere un record di alias per il tuo dominio principale (`example.com`)

1. Apri la console Route 53 all'indirizzo. <https://console.aws.amazon.com/route53/>

Note

Se non utilizzi già Route 53, consulta la [Fase 1: registrare un dominio](#) nella Guida per gli sviluppatori di Amazon Route 53. Dopo la configurazione, puoi tornare alle istruzioni.

2. Scegli Hosted Zones (Zone ospitate).
3. Nell'elenco delle zone ospitate, scegli il nome della zona ospitata corrispondente al nome di dominio.
4. Scegli Create record (Crea record).
5. Seleziona Passa alla procedura guidata.

Note

Se desideri utilizzare la creazione rapida per creare i record alias, consulta [Configurazione di Route 53 per instradare il traffico a un bucket S3](#).

6. Scegli Simple routing (Instradamento semplice) e scegli Next (Successivo).
7. Scegli Define simple record (Definisci record semplice).
8. In Record name (Nome del record) accetta il valore predefinito, che è il nome della zona ospitata e del dominio.

9. In Value/Route Traffic to, scegli Alias to S3 Website Endpoint.
10. Scegli la regione.
11. Scegli il bucket S3.

Il nome del bucket deve corrispondere al nome visualizzato nella casella Name (Nome).

Nell'elenco Scegli bucket S3, il nome del bucket viene visualizzato con l'endpoint del sito Web di Amazon S3 per la regione in cui è stato creato il bucket, ad esempio, `s3-website-us-west-1.amazonaws.com` (`example.com`).

Scegli bucket S3 riporta un bucket se:

- Hai configurato il bucket come sito Web statico.
- Il nome del bucket è uguale al nome del record che stai creando.
- La corrente ha Account AWS creato il bucket.

Se il bucket non viene visualizzato nell'elenco Scegli bucket S3, specifica l'endpoint del sito Web di Amazon S3 per la regione in cui è stato creato il bucket, ad esempio **`s3-website-us-west-2.amazonaws.com`**. Per un elenco completo degli endpoint dei siti Web Amazon S3, consulta [Endpoint di siti Web Amazon S3](#). Per ulteriori informazioni sull'alias target, consulta [Value/route traffic to](#) nella Amazon Route 53 Developer Guide.

12. In Tipo di record, scegli A - Indirizza il traffico verso un indirizzo IPv4 e alcune risorse. AWS
13. Per Evaluate target health (Valuta integrità target), seleziona No.
14. Scegli Define simple record (Definisci record semplice).

Per aggiungere un record di alias per il sottodominio (`www.example.com`)

1. In Configura record, seleziona Definisci record semplice.
2. In Record name (Nome del record) per il sottodominio digita `www`.
3. In Value/Route Traffic to, scegli Alias to S3 Website Endpoint.
4. Scegli la Regione.
5. Seleziona il bucket S3, ad esempi, `s3-website-us-west-2.amazonaws.com` (`www.example.com`).

Se il bucket non viene visualizzato nell'elenco Scegli bucket S3, specifica l'endpoint del sito Web di Amazon S3 per la regione in cui è stato creato il bucket, ad esempio **`s3-website-us-`**

west-2.amazonaws.com. Per un elenco completo degli endpoint dei siti Web Amazon S3, consulta [Endpoint di siti Web Amazon S3](#). Per ulteriori informazioni sull'alias target, consulta [Value/route traffic to](#) nella Amazon Route 53 Developer Guide.

6. In Tipo di record, scegli A - Indirizza il traffico verso un indirizzo IPv4 e alcune risorse. AWS
7. Per Evaluate target health (Valuta integrità target), seleziona No.
8. Scegli Define simple record (Definisci record semplice).
9. Nella pagina Configura record, scegli Crea record.

Note

In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, potrai instradare il traffico al tuo bucket Amazon S3 utilizzando i nomi dei record alias creati in questa procedura.

Aggiungi un record di alias per il dominio root e il sottodominio (vecchia console Route 53)

Per aggiungere un record di alias per il tuo dominio principale (example.com)

La console Route 53 è stata riprogettata. Nella console Route 53 è possibile utilizzare temporaneamente la vecchia console. Se scegli di lavorare con la vecchia console Route 53, attenersi alla procedura riportata di seguito.

1. Apri la console Route 53 all'indirizzo. <https://console.aws.amazon.com/route53/>

Note

Se non utilizzi già Route 53, consulta la [Fase 1: registrare un dominio](#) nella Guida per gli sviluppatori di Amazon Route 53. Dopo la configurazione, puoi tornare alle istruzioni.

2. Scegli Hosted Zones (Zone ospitate).
3. Nell'elenco delle zone ospitate, scegli il nome della zona ospitata corrispondente al nome di dominio.
4. Scegliere Create Record Set (Crea set di record).
5. Specifica i seguenti valori:

Nome

Accetta il valore predefinito, che è il nome della zona ospitata e del dominio.

Per il dominio root, non è necessario aggiungere ulteriori informazioni nel campo Name (Nome).

Tipo

Selezionare A – IPv4 address (A – indirizzo IPv4).

Alias

Scegliere Yes (Sì).

Destinazione alias

Nella sezione endpoint del sito Web S3 dell'elenco, scegliere il nome del bucket.

Il nome del bucket deve corrispondere al nome visualizzato nella casella Name (Nome). Nell'elenco Alias Target (Destinazione alias), il nome bucket è seguito dall'endpoint del sito web Amazon S3 per la regione in cui è stato creato il bucket, ad esempio `example.com (s3-website-us-west-2.amazonaws.com)`. Alias Target (Destinazione alias) elenca un bucket se:

- Hai configurato il bucket come sito Web statico.
- Il nome del bucket è uguale al nome del record che stai creando.
- La corrente Account AWS ha creato il bucket.

Se il bucket non viene visualizzato nell'elenco di Alias target (Target alias), immetti l'endpoint del sito Web Amazon S3 per la regione in cui è stato creato il bucket, ad esempio `s3-website-us-west-2`. Per un elenco completo degli endpoint dei siti Web Amazon S3, consulta [Endpoint di siti Web Amazon S3](#). Per ulteriori informazioni sull'alias target, consulta [Value/route traffic to](#) nella Amazon Route 53 Developer Guide.

Policy di instradamento

Accettare il valore predefinito Simple (Semplice).

Valutazione dello stato target

Accettare il valore predefinito No.

6. Seleziona Crea.

Per aggiungere un record di alias per il tuo sottodominio (www.example.com)

1. Nella zona ospitata del dominio root (example.com), scegliere Create Record Set (Crea set di record).
2. Specifica i seguenti valori:

Nome

Per il sottodominio, immettere www nella casella.

Tipo

Selezionare A – IPv4 address (A – indirizzo IPv4).

Alias

Scegliere Yes (Sì).

Destinazione alias

Nella sezione S3 website endpoints (Endpoint del sito web S3) dell'elenco scegliere lo stesso nome di bucket visualizzato nel campo Name (Nome), ad esempio www.example.com (s3-website-us-west-2.amazonaws.com).

Policy di instradamento

Accettare il valore predefinito Simple (Semplice).

Valutazione dello stato target

Accettare il valore predefinito No.

3. Seleziona Crea.

Note

In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, potrai instradare il traffico al tuo bucket Amazon S3 utilizzando i nomi dei record alias creati in questa procedura.

Fase 12: testare il sito Web

Verificare che il sito Web e il reindirizzamento funzionino correttamente. Nel browser, immettere gli URL. In questo esempio, vengono testati i seguenti URL:

- Dominio (<http://example.com>) – Visualizza il documento indice nel bucket `example.com`.
- Sottodominio (<http://www.example.com>) – Reindirizza la richiesta a <http://example.com>. Viene visualizzato il documento di indice nel bucket `example.com`.

Se il tuo sito web o i link di reindirizzamento non funzionano, puoi provare quanto segue:

- Cancella cache – Cancella la cache del tuo browser Web.
- Controlla i server dei nomi – Se la pagina Web e i collegamenti di reindirizzamento non funzionano dopo avere cancellato la cache, puoi confrontare i server dei nomi per il dominio e i server dei nomi per la zona ospitata. Se i server dei nomi non corrispondono, potrebbe essere necessario aggiornare i server dei nomi di dominio in modo che corrispondano a quelli elencati nella zona ospitata. Per ulteriori informazioni, consulta [Aggiunta o modifica di server dei nomi e associazione di record per un dominio](#).

Dopo aver testato con successo il dominio principale e il sottodominio, puoi configurare una CloudFront distribuzione [Amazon](#) per migliorare le prestazioni del tuo sito Web e fornire log da utilizzare per esaminare il traffico del sito Web. Per ulteriori informazioni, consulta [Velocizza il tuo sito Web con Amazon CloudFront](#).

Velocizza il tuo sito Web con Amazon CloudFront

Puoi usare [Amazon CloudFront](#) per migliorare le prestazioni del tuo sito Web Amazon S3. CloudFront rende disponibili i file del tuo sito web (come HTML, immagini e video) dai data center di tutto il mondo (note come edge location). Quando un visitatore richiede un file del sito Web, CloudFront reindirizza automaticamente la richiesta a una copia del file nella posizione di confine più vicina. Ciò determina tempi di download più rapidi rispetto alla richiesta di contenuto da un data center situato più lontano da parte del visitatore.

CloudFront memorizza nella cache i contenuti nelle edge location per un periodo di tempo specificato dall'utente. Se un visitatore richiede contenuti che sono stati memorizzati nella cache per un periodo superiore alla data di scadenza, CloudFront controlla il server di origine per verificare se è disponibile una versione più recente del contenuto. Se è disponibile una versione più recente, CloudFront copia

la nuova versione nell'edge location. Le modifiche apportate ai contenuti originali vengono replicate nelle edge location quando i visitatori richiedono i contenuti.

Utilizzo CloudFront senza Route 53

Il tutorial in questa pagina utilizza Route 53 per indicare la tua CloudFront distribuzione. Tuttavia, se desideri fornire contenuti ospitati in un bucket Amazon S3 CloudFront senza utilizzare Route 53, consulta [Amazon CloudFront Tutorials: Configurazione di una distribuzione dinamica dei contenuti per Amazon S3](#). Quando servi contenuti ospitati in un bucket Amazon S3 utilizzando CloudFront, puoi utilizzare qualsiasi nome di bucket e sono supportati sia HTTP che HTTPS.

Configurazione automatica con un modello CloudFormation

Per ulteriori informazioni sull'utilizzo di un CloudFormation modello per configurare un sito Web statico sicuro che crea una CloudFront distribuzione al servizio del tuo sito Web, consulta la sezione Guida [introduttiva a un sito Web statico sicuro](#) nella Amazon CloudFront Developer Guide.

Argomenti

- [Fase 1: Creare una CloudFront distribuzione](#)
- [Passaggio 2: aggiornare il set di record per il dominio e sottodominio](#)
- [\(Facoltativo\) Fase 3: controllare i file di log](#)

Fase 1: Creare una CloudFront distribuzione

Innanzitutto, crei una CloudFront distribuzione. Ciò rende il sito Web accessibile a data center di tutto il mondo.

Per creare una distribuzione con un'origine Amazon S3

1. Apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Scegliere Create Distribution (Crea distribuzione).
3. Nella pagina Create Distribution (Crea distribuzione), nella sezione Origin Settings (Impostazioni origine), digitare l'endpoint del sito Web Amazon S3 per il bucket in Origin Domain Name (Nome dominio di origine), ad esempio **example.com.s3-website.us-west-1.amazonaws.com**.

CloudFront compila l'Origin ID per te.

4. Lasciare i valori predefiniti in Default Cache Behavior Settings (Impostazioni predefinite comportamento cache).

Con le impostazioni predefinite per Viewer Protocol Policy (Policy protocollo visualizzatore), è possibile utilizzare HTTPS per il sito Web statico. Per ulteriori informazioni su queste opzioni di configurazione, consulta [Valori che specifichi quando crei o aggiorni una distribuzione Web](#) nella Amazon CloudFront Developer Guide.

5. In Impostazioni distribuzione, esegui quanto indicato di seguito:

- a. Lascia Classe prezzo impostato su Utilizza tutte le edge location (prestazioni migliori).
- b. Imposta i nomi di dominio alternativi (CNAMEs) sul dominio principale e sul `www` sottodominio. In questo tutorial, questi sono rappresentati da `example.com` e `www.example.com`.

 Important

Prima di eseguire questo passaggio, prendete nota dei [requisiti per l'utilizzo di nomi di dominio alternativi](#), in particolare della necessità di un certificato valido. SSL/TLS

- c. Per SSL Certificate (Certificato SSL), scegliere Custom SSL Certificate (example.com) (Certificato SSL personalizzato (example.com)), quindi scegliere il certificato personalizzato che copre i nomi di dominio e sottodominio.

Per ulteriori informazioni, consulta il [certificato SSL](#) nella Amazon CloudFront Developer Guide.

- d. In Default Root Object (Oggetto root predefinito), immettere il nome del documento indice, ad esempio `index.html`.

Se l'URL utilizzato per accedere alla distribuzione non contiene un nome di file, la CloudFront distribuzione restituisce il documento indice. L'oggetto root predefinito deve corrispondere esattamente al nome del documento indice per il sito Web statico. Per ulteriori informazioni, consulta [Configurazione di un documento indice](#).

- e. Imposta Log su On.

 Important

Quando crei o aggiorni una distribuzione e abiliti la CloudFront registrazione, CloudFront aggiorna l'elenco di controllo degli accessi ai bucket (ACL) per concedere all'`awslogsdeliveryaccount` le `FULL_CONTROL` autorizzazioni per scrivere i log nel bucket. Per ulteriori informazioni, consulta la sezione [Autorizzazioni](#)

[necessarie per configurare la registrazione standard e accedere ai file di registro](#) nella Amazon CloudFront Developer Guide. Se il bucket che memorizza i log utilizza l'impostazione imposta dal proprietario del bucket per disabilitare S3 Object Ownership ACLs, CloudFront non può scrivere log nel bucket. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione degli ACL per il bucket](#).

- f. In Bucket per log, scegli il bucket log creato.

Per ulteriori informazioni sulla configurazione di un bucket di registrazione, consulta [\(Facoltativo\) Registrazione del traffico Web](#).

- g. Per archiviare i log generati dal traffico della distribuzione CloudFront in una cartella, in Log Prefix (Prefisso log), immetti il nome della cartella.
- h. Mantieni i valori predefiniti di tutte le altre impostazioni.

6. Scegliere Create Distribution (Crea distribuzione).
7. Per visualizzare lo stato attuale della distribuzione, cercare la distribuzione nella console e controllare la colonna Status (Stato).

Lo stato InProgress indica che la distribuzione non è ancora completamente distribuita.

Quando la tua distribuzione è distribuita, si può fare riferimento ai propri contenuti con il nuovo nome dominio CloudFront.

8. Registra il valore del nome di dominio mostrato nella console, ad esempio. CloudFront `dj4p1rv6mvubz.cloudfront.net`
9. Per verificare che la CloudFront distribuzione funzioni, inserisci il nome di dominio della distribuzione in un browser web.

Se il tuo sito web è visibile, la CloudFront distribuzione funziona. Se il tuo sito Web ha un dominio personalizzato registrato con Amazon Route 53, avrai bisogno del nome di CloudFront dominio per aggiornare il record impostato nel passaggio successivo.

Passaggio 2: aggiornare il set di record per il dominio e sottodominio

Ora che hai creato correttamente una CloudFront distribuzione, aggiorna il record di alias in Route 53 in modo che punti alla nuova CloudFront distribuzione.

Per aggiornare il record di alias in modo che punti a una distribuzione CloudFront

1. Apri la console Route 53 all'indirizzo <https://console.aws.amazon.com/route53/>.
2. Nel riquadro di navigazione a sinistra, scegliere Hosted zones (Zone ospitate).
3. Nella pagina Hosted Zones (Zone ospitate), scegliere la hosted zone creata per il sottodominio, per esempio `www.example.com`.
4. In Records, selezionare il record A creato per il sottodominio.
5. In Record details (Dettagli record), scegliere Edit record (Modifica record).
6. In Instrada il traffico verso, scegli Alias per la CloudFront distribuzione.
7. In Scegli la distribuzione, scegli la CloudFront distribuzione.
8. Scegli Save (Salva).
9. Per reindirizzare il record A per il dominio radice alla CloudFront distribuzione, ripeti questa procedura per il dominio radice, `example.com` ad esempio.

L'aggiornamento ai set di record avviene entro 2-48 ore.

10. Per verificare se i nuovi record A sono effettivi, in un browser Web immetti l'URL del sottodominio, ad esempio `http://www.example.com`.

Se il browser non reindirizza più al dominio root, ad esempio `http://example.com`, i nuovi record A sono effettivi. Quando il nuovo record A ha effetto, il traffico indirizzato dal nuovo record A alla CloudFront distribuzione non viene reindirizzato al dominio radice. Tutti i visitatori che fanno riferimento al sito utilizzando `http://example.com` o `http://www.example.com` vengono reindirizzati alla CloudFront edge location più vicina, dove possono usufruire di tempi di download più rapidi.

 Tip

I browser possono effettuare il caching delle impostazioni di reindirizzamento. Se pensi che le impostazioni del nuovo record A dovrebbero essere diventate effettive ma il tuo browser reindirizza ancora `http://www.example.com` a `http://example.com`, prova a svuotare la cache e a eliminare la cronologia del browser, a chiudere e riaprire la tua applicazione browser o a utilizzare un browser Web differente.

(Facoltativo) Fase 3: controllare i file di log

I log di accesso indicano quante persone stanno visitando il sito Web. Inoltre contengono preziosi dati aziendali che si possono analizzare con altri servizi, come [Amazon EMR](#).

CloudFront i log vengono archiviati nel bucket e nella cartella scelti quando crei una CloudFront distribuzione e abiliti la registrazione. CloudFront scrive i log nel tuo bucket di log entro 24 ore da quando vengono effettuate le richieste corrispondenti.

Per visualizzare i file di log del sito Web

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegliere il nome del bucket log per il tuo sito web.
3. Scegli la cartella dei CloudFront log.
4. Scarica i .gzip file scritti da CloudFront prima di aprirli.

Se hai creato il tuo sito Web solo come esercizio di apprendimento, puoi eliminare le risorse che hai allocato per non accumulare più addebiti. A questo proposito, consulta [Pulizia delle risorse di esempio](#). Una volta eliminate le risorse AWS , il sito Web non è più disponibile.

Pulizia delle risorse di esempio

Se il sito Web statico è stato creato come esercizio di apprendimento, elimina le risorse AWS che allocate per non accumulare più addebiti. Una volta eliminate le risorse AWS , il sito Web non è più disponibile.

Processi

- [Passaggio 1: eliminare la CloudFront distribuzione Amazon](#)
- [Passaggio 2: eliminare la zona ospitata Route 53](#)
- [Fase 3: disabilitare la registrazione ed eliminare il bucket S3](#)

Passaggio 1: eliminare la CloudFront distribuzione Amazon

Prima di eliminare una CloudFront distribuzione Amazon, devi disabilitarla. Una distribuzione disattivata non è più funzionante e non accumula addebiti. Puoi attivare una distribuzione disattivata in qualsiasi momento. Una volta eliminata una distribuzione disattivata, non è più disponibile.

Per disabilitare ed eliminare una CloudFront distribuzione

1. Apri la CloudFront console all'indirizzo <https://console.aws.amazon.com/cloudfront/v4/home>.
2. Selezionare la distribuzione che si vuole disattivare e scegliere Disable (Disattiva).
3. Quando viene richiesta la conferma, seleziona Sì, disattiva.
4. Selezionare la distribuzione disattivata e scegliere Delete (Elimina).
5. Quando viene richiesta la conferma, seleziona Sì, elimina.

Passaggio 2: eliminare la zona ospitata Route 53

Prima di eliminare la hosted zone, devi eliminare i set di record creati. Non è necessario eliminare i record NS e SOA; vengono eliminati automaticamente quando elimini la hosted zone.

Per eliminare i set di record

1. Apri la console Route 53 all'indirizzo <https://console.aws.amazon.com/route53/>.
2. Nell'elenco dei nomi di dominio, selezionare il nome di dominio, quindi selezionare Vai a set di record.
3. Nell'elenco dei set di record, selezionare le caselle che corrispondono ai record A creati.

Il tipo di ciascun set di record è elencato nella colonna Tipo.

4. Seleziona Elimina set di record.
5. Quando viene richiesta la conferma, seleziona Conferma.

Per eliminare una zona ospitata Route 53

1. Continuando dalla procedura precedente, selezionare Back to Hosted Zones (Torna a zone ospitate).
2. Selezionare il nome di dominio, quindi selezionare Delete Hosted Zone (Elimina hosted zone).
3. Quando viene richiesta la conferma, seleziona Conferma.

Fase 3: disabilitare la registrazione ed eliminare il bucket S3

Prima di eliminare il bucket S3 in uso, accertarsi che le attività di logging siano disattivate per quel bucket. Altrimenti, AWS continua a scrivere i log nel bucket mentre lo elimini.

Per disattivare il log per un bucket

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. In Buckets (Bucket), scegliere il nome del bucket e quindi scegliere Properties (Proprietà).
3. Da Properties (Proprietà), selezionare Log.
4. Deseleziona la casella Attivato.
5. Scegliere Save (Salva).

È possibile ora eliminare il bucket. Per ulteriori informazioni, consulta [Eliminazione di un bucket per uso generico](#).

Implementazione di un sito Web statico per AWS Amplifica l'hosting da un bucket S3 per uso generico

Ti consigliamo di utilizzare [Hosting AWS Amplify](#) per ospitare contenuti di siti web statici archiviati su S3. Amplify Hosting è un servizio completamente gestito che semplifica l'implementazione dei tuoi siti Web su una rete di distribuzione di contenuti (CDN) disponibile a livello globale basata su Amazon CloudFront, consentendo un hosting statico sicuro di siti Web senza una configurazione estesa. Con AWS Amplify Hosting, puoi selezionare la posizione dei tuoi oggetti all'interno del tuo bucket generico, distribuire i tuoi contenuti su un CDN gestito e generare un URL HTTPS pubblico affinché il tuo sito Web sia accessibile ovunque. L'implementazione di un sito web statico utilizzando Hosting Amplify offre i seguenti vantaggi e funzionalità:

- L'implementazione sulla rete di distribuzione AWS dei contenuti (CDN) basata su Amazon CloudFront. CloudFront è un servizio web che accelera la distribuzione dei tuoi contenuti web statici e dinamici ai tuoi utenti. CloudFront distribuisce i tuoi contenuti attraverso una rete mondiale di data center denominati edge locations. Quando un utente richiede il contenuto che state servendo CloudFront, la richiesta viene indirizzata all'edge location che offre la latenza più bassa (ritardo), in modo che il contenuto venga distribuito con le migliori prestazioni possibili, maggiore affidabilità e disponibilità. Per ulteriori informazioni, consulta [How delivery CloudFront content](#) nella Amazon CloudFront Developer Guide.
- Supporto HTTPS: fornisce comunicazioni e trasferimento di dati sicuri tra il proprio sito web e il browser web dell'utente.
- Domini personalizzati: consente di collegare facilmente il sito web a un URL personalizzato acquistato da un registrar di dominio come Amazon Route 53.

- **Certificati SSL personalizzati:** quando si configura un dominio personalizzato, è possibile utilizzare il certificato gestito predefinito fornito da Amplify oppure è possibile utilizzare un certificato personalizzato acquistato dall'autorità di certificazione di terze parti di propria scelta.
- **Metriche e CloudWatch monitoraggio integrati:** monitora il traffico, gli errori, il trasferimento dei dati e la latenza del tuo sito web.
- **Protezione con password:** limita l'accesso al sito web impostando un nome utente e una password nella console Amplify.
- **Reindirizzamenti e riscritture:** consentono di creare regole di reindirizzamento e riscrittura nella console Amplify per permettere a un server web di reindirizzare la navigazione da un URL all'altro.

Quando distribuisce la tua applicazione da un bucket Amazon S3 per uso generico ad Amplify Hosting, i AWS costi si basano sul modello di prezzo di Amplify. Per ulteriori informazioni, consulta [AWS Amplify Prezzi](#).

 Important

Amplify Hosting non è disponibile in tutti i Paesi in cui Amazon S3 è disponibile. Regioni AWS Per implementare un sito web statico su Hosting Amplify, il bucket Amazon S3 per uso generico contenente il sito web deve trovarsi in una Regione in cui è disponibile Amplify. Per l'elenco delle Regioni in cui è disponibile Amplify, consulta [Endpoint Amplify](#) in Riferimenti generali di Amazon Web Services.

Puoi avviare il processo di distribuzione dalla console Amazon S3, dalla console Amplify, dalla AWS CLI o dagli SDK. AWS È possibile eseguire l'implementazione su Amplify solo da un bucket per uso generico situato nel proprio account. Amplify non supporta l'accesso a un bucket tra account.

Utilizza le seguenti istruzioni per implementare un sito web statico da un bucket Amazon S3 per uso generico su Hosting Amplify a partire dalla console Amazon S3.

Implementazione di un sito web statico su Amplify dalla console S3

Per implementare un sito web statico dalla console Amazon S3

1. Accedi Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel pannello di navigazione a sinistra, scegli Buckets (Bucket).

3. Nell'elenco Bucket, scegli il bucket per uso generico che contiene il sito web che desideri implementare su Hosting Amplify.
4. Scegliere la scheda Properties (Proprietà).
5. In Hosting di siti Web statici, scegli Crea l'app Amplify. A questo punto, il processo di implementazione passerà alla console Amplify.
6. Nella pagina Deploy with S3 (Implementa con S3), procedi nel seguente modo.
 - a. Per il Nome dell'app, inserire il nome dell'app o del sito web.
 - b. Per il Nome del ramo, inserire il nome del backend dell'app.
 - c. Per Posizione S3 degli oggetti da ospitare, inserisci il percorso della directory del bucket per uso generico o scegliere Sfoglia S3 per individuarlo e selezionarlo.
7. Scegliere Save and deploy (Salva e distribuisci).

Note

Se si aggiorna uno qualsiasi degli oggetti di un sito web statico nel bucket per uso generico ospitato su Amplify, è necessario implementare nuovamente l'applicazione su Hosting Amplify per rendere effettive le modifiche. Hosting Amplify non rileva automaticamente le modifiche apportate al bucket. Per ulteriori informazioni, consulta [Updating a static website deployed to Amplify from an S3 bucket](#) nella Guida per l'utente di Hosting AWS Amplify.

Per iniziare direttamente dalla console Amplify, consulta [Deploying a static website from S3 using the Amplify console](#) nella Guida per l'utente di Hosting AWS Amplify.

Per iniziare a utilizzare gli AWS SDK, consulta [Creazione di una policy bucket per distribuire un sito Web statico da S3 utilizzando gli AWS SDK](#) nella Amplify Hosting User Guide. AWS

Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi (ABAC)

Un AWS tag è una coppia chiave-valore che contiene metadati. I tag vengono associati alle risorse Amazon S3, ad esempio i bucket. Puoi aggiungere i tag quando crei la risorsa oppure gestire quelli di una risorsa esistente. Non sono previsti costi aggiuntivi per l'utilizzo dei tag oltre alle tariffe di richiesta API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Come funzionano i tag

Amazon S3 supporta due tipi di tag:

- Tag generati da AWS: AWS applica automaticamente questi tag e non è possibile modificarli o rimuoverli. Per ulteriori informazioni sui tag AWS-generated, consulta [Utilizzo dei tag -generated AWS](#).
- User-defined tag: applichi questi tag alle tue risorse S3 e li gestisci.

User-defined tag

Un tag definito dall'utente è una coppia chiave-valore che usi per etichettare le tue risorse. User-defined i tag sono costituiti da una chiave obbligatoria e da un valore opzionale. Un tag definito dall'utente ha i seguenti componenti principali:

Chiave del tag

La chiave di tag corrisponde al nome obbligatorio del tag. Ad esempio, `project` è la chiave del tag nella seguente coppia chiave-valore del tag:

Chiave	Valore
<code>project</code>	<code>Trinity</code>

La chiave del tag è una stringa che fa distinzione tra maiuscole e minuscole e deve contenere tra 1 e 128 caratteri Unicode. Le chiavi possono contenere solo lettere o numeri Unicode, spazi bianchi e i simboli seguenti:

- `_`: carattere di sottolineatura
- `.`: punto
- `::`: due punti
- `/`: barra
- `=`: segno uguale
- `+`: segno più
- `@`: chiocciola
- `-`: dash

Valore del tag

Il valore del tag è una stringa opzionale. Ad esempio, `Trinity` è il valore del tag in questa coppia chiave-valore del tag:

Chiave	Valore
<code>project</code>	<code>Trinity</code>

Il valore del tag è una stringa che fa distinzione tra maiuscole e minuscole, contenente tra 0 e 256 caratteri Unicode. I valori possono contenere solo lettere o numeri Unicode, spazi bianchi e i simboli seguenti:

- `_`: carattere di sottolineatura
- `.`: punto
- `::`: due punti
- `/`: barra
- `=`: segno uguale
- `+`: segno più
- `@`: chiocciola
- `-`: dash

Per informazioni dettagliate sui caratteri consentiti nei tag definiti dall'utente e su altre restrizioni, consulta Restrizioni relative ai [User-Defined tag](#) nella Guida per l'Gestione costi e fatturazione AWS utente.

Set di tag

Ogni risorsa S3 ha un set di tag che contiene tutte le coppie di chiavi di tag e valore assegnate a quel bucket. Un set di tag può essere vuoto o può contenere fino a 50 tag definiti dall'utente, tranne nel caso di assegnazione di tag agli oggetti. È possibile avere un massimo di 10 tag per oggetto.

Sebbene ogni chiave debba essere univoca in un set di tag, è possibile utilizzare lo stesso valore più volte. Ad esempio, si può avere lo stesso valore `Trinity`, per le seguenti due chiavi di tag:

Chiave	Valore
<code>project</code>	<code>Trinity</code>
<code>cost-center</code>	<code>Trinity</code>

Se si aggiunge un tag con la stessa chiave di un tag esistente, il nuovo valore sovrascrive quello precedente.

AWS non applica alcun significato semantico ai tuoi tag. I tag sono interpretati prettamente come stringhe di caratteri.

Per aggiungere, elencare, modificare o eliminare i tag, puoi utilizzare la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI) o l'API Amazon S3.

Modi comuni per utilizzare i tag

Si utilizzano i tag sulle risorse S3 per:

1. Allocazione dei costi: monitorare i costi di archiviazione in base al tag del bucket in Gestione costi e fatturazione AWS.
2. Attribute-based controllo degli accessi (ABAC): ridimensiona le autorizzazioni di accesso e concedi l'accesso alle risorse S3 in base ai relativi tag.

 Note

È possibile utilizzare gli stessi tag sia per l'allocazione dei costi che per il controllo degli accessi.

Utilizzo dei tag per l'allocazione dei costi

È possibile tenere traccia dei costi di archiviazione di Amazon S3 applicando i tag alle risorse S3 e attivandoli per l'allocazione dei costi.

Per iniziare a tenere traccia dei costi:

1. Aggiungi i tag alle risorse S3 o utilizza i tag esistenti. Ad esempio, è possibile etichettare i bucket con un tag che identifica un progetto o un gruppo di progetti.
2. Attiva i tag per l'allocazione dei costi nella console. Gestione costi e fatturazione AWS Consulta [Attivazione dei tag per l'allocazione dei costi definiti dall'utente](#) nella Guida per l'utente di Gestione costi e fatturazione AWS . È possibile attivare i tag definiti dall'utente o generati AWS dall'utente. Per ulteriori informazioni, vedere [Organizzazione e monitoraggio dei costi utilizzando i tag di allocazione AWS dei costi](#).

AWS utilizza i tag attivati per organizzare i costi delle risorse in vari strumenti di fatturazione e gestione dei costi, come:

- Report di allocazione dei costi

Fornisce una visualizzazione di alto livello dei costi organizzati in base ai tag attivati. Per ulteriori informazioni, consulta [Utilizzo del report mensile di allocazione dei costi](#) nella Guida per l'utente di AWS .

- Report di costi e utilizzo

Fornisce la serie più dettagliata di dati su AWS costi e utilizzo, inclusa la suddivisione dei costi basata su tag. Per ulteriori informazioni, consulta [Cosa sono i report sui AWS costi e sull'utilizzo?](#) nella Guida per l'utente di AWS Data Export.

Risorse Amazon S3 che supportano il monitoraggio dei costi con tag

Le seguenti risorse Amazon S3 supportano il monitoraggio dei costi di archiviazione utilizzando i tag.

- Benne S3 per uso generico

Per ulteriori informazioni, consulta [Utilizzo di tag con bucket S3 per uso generico](#).

- Bucket S3 Directory

Per ulteriori informazioni, consulta [Utilizzo di tag con i bucket di directory S3](#).

- Tabelle S3

Per ulteriori informazioni, consulta [Utilizzo dei tag con le tabelle S3](#).

- Indice vettoriale S3

Per ulteriori informazioni, consulta [Utilizzo di tag con indici vettoriali S3](#)

Utilizzo dei tag per il controllo degli accessi basato su attributi (ABAC)

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, ad esempio i tag. Puoi allegare tag a entità AWS Identity and Access Management (IAM) (utenti o ruoli) e a AWS risorse, come gli access point Amazon S3 e i bucket di directory. Quindi, è possibile controllare le autorizzazioni a queste risorse utilizzando condizioni basate su tag nelle policy di controllo degli accessi per consentire o negare le operazioni quando tali condizioni sono soddisfatte.

Con ABAC, utilizzi chiavi di condizione basate su tag nelle policy delle risorse AWS aziendali, IAM e S3. Per le aziende, ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle policy IAM, è possibile controllare l'accesso alle risorse S3 in base ai tag del bucket utilizzando le [chiavi di condizione](#).

Chiavi di condizione supportate

Puoi utilizzare le seguenti chiavi di AWS condizione per tutte le risorse Amazon S3 che supportano ABAC.

- `aws:ResourceTag/key-name`
- `aws:RequestTag/key-name`
- `aws:TagKeys`

Alcune risorse supportano chiavi di condizione di Amazon S3 aggiuntive. Per un elenco completo delle chiavi di condizione che possono essere utilizzate per ABAC e delle policy di esempio, consulta i seguenti argomenti relativi ai tag della risorsa.

Risorse Amazon S3 che supportano ABAC

Le seguenti risorse Amazon S3 supportano il controllo degli accessi basato su attributi (ABAC) con tag.

- Secchi S3 per uso generico

Per ulteriori informazioni, consulta [Utilizzo di tag con bucket S3 per uso generico](#).

- Punti di accesso

Per ulteriori informazioni, consulta [Utilizzo di tag con punti di accesso S3 per bucket per uso generico](#) e [Utilizzo di tag con Punti di accesso S3 per bucket di directory](#).

- Processi di operazioni batch

Per ulteriori informazioni, consulta [Controllo dei lavori di accesso ed etichettatura mediante tag](#).

- bucket S3 Directory

Per ulteriori informazioni, consulta [Utilizzo di tag con i bucket di directory S3](#).

- Oggetti

Per ulteriori informazioni, consulta [Etichettare i tuoi oggetti](#).

- Sovvenzioni di accesso a S3

Per ulteriori informazioni, consulta [Gestione dei tag per S3 Access Grants](#).

- Gruppi Storage Lens S3

Per ulteriori informazioni, consulta [Gestione AWS tag di risorse con gruppi Storage Lens](#).

- Secchi e tavoli da tavolo S3

Per ulteriori informazioni, consulta [Utilizzo dei tag con i bucket di tabelle S3](#) e [Utilizzo dei tag con le tabelle S3](#).

- Bucket e indici vettoriali S3

Per ulteriori informazioni, consulta [Utilizzo di tag con bucket vettoriali S3](#) e [Utilizzo di tag con indici vettoriali S3](#).

Pianificazione della strategia di tagging

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Con un set di chiavi di tag coerente, la gestione delle risorse risulta semplificata. Puoi cercare e filtrare le risorse in base ai tag aggiunti. Per ulteriori informazioni su come implementare un'efficace strategia di etichettatura delle risorse, consulta il white paper sulle migliori pratiche di etichettatura.

[AWS](#)

Best practice per l'utilizzo dei tag delle risorse Amazon S3

Quando si utilizzano i tag, è consigliabile attenersi alle seguenti best practice:

- Documentare le convenzioni per l'utilizzo dei tag che devono essere seguite da tutti i team dell'organizzazione. In particolare, è necessario assicurarsi che i nomi siano descrittivi e coerenti. Ad esempio, standardizzare il formato `environment:prod` anziché utilizzare il tag `env:production` per alcune risorse.

Important

Non memorizzare informazioni personali identificabili o altre informazioni riservate o sensibili nei tag.

- Automatizzare l'utilizzo dei tag per garantire la coerenza. Ad esempio, puoi includere tag in un modello. CloudFormation Quando le risorse vengono create con il modello, i tag vengono automaticamente applicati.
- Utilizzare i tag solo quando necessario. Evitare la proliferazione e la complessità non necessarie dei tag.
- Controllare periodicamente i tag per verificarne la pertinenza e la precisione. Rimuovere o modificare i tag obsoleti secondo necessità.
- Prendi in considerazione la possibilità di creare tag con il AWS Tag Editor nella Console di AWS gestione. Puoi utilizzare il Tag Editor per aggiungere tag a più AWS risorse supportate, incluse le risorse Amazon S3, contemporaneamente. Per ulteriori informazioni, consulta [Tag Editor](#) nella Guida per l'utente di AWS Resource Groups.

Gestione dei tag per risorse Amazon S3

Per ulteriori informazioni su come gestire i tag per le risorse Amazon S3, consulta gli argomenti seguenti:

- [Utilizzo di tag con punti di accesso S3 per bucket per uso generico](#)
- [Utilizzo di tag con Punti di accesso S3 per bucket di directory](#)
- [Controllo dei lavori di accesso ed etichettatura mediante tag](#)
- [Utilizzo di tag con i bucket di directory S3](#)
- [Utilizzo dei tag per l'allocazione dei costi per i bucket S3](#)
- [Etichettare i tuoi oggetti](#)
- [Gestione dei tag per S3 Access Grants](#)
- [Gestione AWS tag di risorse con gruppi Storage Lens](#)
- [Utilizzo di tag con bucket S3 per uso generico.](#)
- [Utilizzo di tag con bucket vettoriali S3](#)
- [Utilizzo di tag con indici vettoriali S3](#)

Utilizzo di tag con bucket S3 per uso generico

Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso i bucket generici di Amazon S3. Puoi etichettare i bucket S3 quando li crei o gestire i tag sui bucket esistenti. Per informazioni generali sui tag, consulta [Tagging per l'allocazione dei costi o il controllo degli accessi basato su attributi \(ABAC\)](#).

Note

Non sono previsti costi aggiuntivi per l'utilizzo dei tag nei bucket oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Modi comuni per utilizzare i tag con i bucket

Usa i tag sui tuoi bucket S3 per:

1. Allocazione dei costi: monitorare i costi di archiviazione in base al tag del bucket in Gestione costi e fatturazione AWS. Per ulteriori informazioni, consultare [Utilizzo dei tag per l'allocazione dei costi](#).
2. Attribute-based controllo degli accessi (ABAC): ridimensiona le autorizzazioni di accesso e concedi l'accesso ai bucket S3 in base ai relativi tag. Per ulteriori informazioni, consulta [Utilizzo dei tag per ABAC](#).

Note

Per i bucket generici, l'ABAC non è abilitato per impostazione predefinita. Per abilitare l'ABAC per i bucket per uso generico, vedere [Abilitazione dell'ABAC in bucket generici](#). Per le risorse Amazon S3 come punti di accesso e bucket di directory, ABAC è abilitato per impostazione predefinita. È possibile utilizzare gli stessi tag sia per l'allocazione dei costi che per il controllo degli accessi.

ABAC per bucket S3 per uso generico

I bucket per uso generico Amazon S3 supportano il controllo degli accessi basato sugli attributi (ABAC) tramite tag. Usa le chiavi di condizione basate su tag nelle policy delle tue AWS

organizzazioni, in IAM e nei bucket S3. Per le aziende, ABAC in Amazon S3 supporta l'autorizzazione su più account. AWS

Nelle tue policy IAM, puoi controllare l'accesso ai bucket S3 in base ai tag del bucket utilizzando le seguenti chiavi di condizione globali: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html#condition-keys-tagkeys

- `aws:ResourceTag/key-name`
 - Usa questa chiave di condizione per confrontare la coppia chiave-valore del tag specificata nella policy con la coppia chiave-valore associata alla risorsa. S3 valuta questa chiave di condizione solo dopo aver abilitato ABAC sul bucket. Ad esempio, puoi richiedere che l'accesso a una risorsa sia consentito solo se la risorsa dispone di una chiave di tag Dept collegata al valore Marketing. Per ulteriori informazioni, vedere [Controllo dell'accesso alle risorse. AWS](#)
- `aws:RequestTag/key-name`
 - Utilizzate questa chiave di condizione per confrontare la coppia chiave-valore del tag passata nella richiesta con la coppia di tag specificata nella policy. Ad esempio, è possibile controllare che la richiesta includa la chiave del tag Dept e che abbia il valore Accounting. Per ulteriori informazioni, consulta [Controllo dell'accesso durante AWS le richieste](#). È possibile utilizzare questa chiave di condizione per limitare quali coppie chiave-valore di tag possono essere passate durante le operazioni API TagResource e CreateBucket.
- `aws:TagKeys`
 - Usa questa chiave condizionale per confrontare le chiavi dei tag in una richiesta con le chiavi specificate nella policy. Nell'utilizzo delle policy per controllare gli accessi tramite tag, è consigliabile utilizzare la chiave di condizione `aws:TagKeys` per definire le chiavi di tag ammesse. Per esempi di policy e ulteriori informazioni, consulta [Controllo dell'accesso in base alle chiavi di tag](#).
- `s3:BucketTag/tag-key`
 - Usa questa chiave di condizione per concedere le autorizzazioni a dati specifici nei bucket utilizzando i tag. Questa chiave di condizione è applicabile solo dopo aver abilitato l'ABAC sul bucket. Quando si accede a un bucket utilizzando un punto di accesso, la chiave di `aws:ResourceTag/tag-key` condizione fa riferimento ai tag sul bucket sia durante l'autorizzazione sull'access point che sul bucket. `s3:BucketTag/tag-key` Farà riferimento solo ai tag del bucket per cui viene autorizzata.

 Note

Quando crei bucket con tag, tieni presente che le condizioni basate sui tag per accedere al tuo bucket utilizzando le chiavi di BucketTag condizione aws: ResourceTag e s3: sono applicabili solo dopo aver abilitato ABAC sul bucket. Per ulteriori informazioni, consulta [Abilitazione dell'ABAC in bucket generici](#).

Esempi di politiche ABAC per i bucket

Vedi il seguente esempio di politiche ABAC per i bucket Amazon S3.

1.1 - Policy IAM per creare o modificare bucket con tag specifici

In questa policy IAM, gli utenti o i ruoli con questa policy possono creare bucket S3 solo se etichettano il bucket con la chiave `project` e il valore `Trinity` del tag nella richiesta di creazione del bucket. Possono anche aggiungere o modificare tag su bucket S3 esistenti purché la `TagResource` richiesta includa la coppia tag chiave-valore. `project:Trinity` Questa policy non fornisce autorizzazioni di lettura, scrittura o eliminazione sui bucket o sui relativi oggetti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateBucketWithTags",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
            "Trinity"
          ]
        }
      }
    }
  ]
}
```

1.2 - Politica dei bucket per limitare le operazioni

In questa policy del bucket, i principali IAM (utenti e ruoli) vengono `s3:ListBucket` negati e `s3:PutObject` le azioni sul bucket vengono eseguite solo se il valore del `project` tag sul bucket corrisponde al valore del tag sul project bucket. `s3:GetObject`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyObjectOperations",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:ListBucket",
                 "s3:GetObject",
                 "s3:PutObject"],
      "Resource": "arn:aws:s3:::aws-s3-demo/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}
```

1.3 - Politica IAM per modificare i tag sulle risorse esistenti

In questa policy IAM, i principali IAM (utenti o ruoli) possono modificare i tag su un bucket solo se il valore del tag `project` del bucket corrisponde al valore del tag `project` del principale. Per questi bucket sono consentiti solo i quattro tag `project` `environmentowner`, e `cost-center` specificati nelle chiavi di `aws:TagKeys` condizione. Ciò aiuta a rafforzare la governance dei tag, impedisce modifiche non autorizzate dei tag e mantiene lo schema di tagging coerente tra i bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
```

```

        "s3:TagResource",
        "s3:CreateBucket"
    ],
    "Resource": "*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": [
                "project",
                "environment",
                "owner",
                "cost-center"
            ]
        }
    }
}
]
}

```

1.4 - Uso della chiave s3: condition BucketTag

In questa policy IAM, l'istruzione condition consente l'accesso ai dati del aws-s3-demo bucket solo se il bucket ha la chiave del tag Environment e il valore del tag. Production

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessViaSpecificBucket",
      "Effect": "Allow",
      "Action": "*",
      "Resource": ["arn:aws:s3:::aws-s3-demo", "arn:aws:s3:::aws-s3-demo/*"],
      "Condition": {
        "StringEquals": {
          "s3:BucketTag/Environment": "Production"
        }
      }
    }
  ]
}

```

Gestione dei tag per i bucket per uso generico

Puoi aggiungere o gestire tag per i bucket S3 utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (CLI), gli AWS SDK o utilizzando le API S3:, e. [TagResource](#) [UntagResource](#) [ListTagsForResource](#) Per ulteriori informazioni, consulta:

Abilitazione dell'ABAC in bucket generici

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che utilizzi per definire le autorizzazioni in base agli attributi, ad esempio i tag. Per impostazione predefinita, l'ABAC è disabilitato per tutti i bucket generici di Amazon S3. Per utilizzare ABAC per bucket generici, devi abilitarlo.

Prima di abilitare ABAC per il tuo bucket generico, ti consigliamo di completare innanzitutto le attività descritte nei seguenti argomenti:

Argomenti

- [Esecuzione di audit sulle policy prima dell'abilitazione dell'ABAC](#)

Esecuzione di audit sulle policy prima dell'abilitazione dell'ABAC

Prima di abilitare l'ABAC per il bucket, se il bucket contiene tag, verifica le politiche di controllo degli accessi per verificare se le condizioni basate sui tag fanno riferimento a uno dei tag esistenti nei bucket. In tal caso, verifica che queste politiche siano configurate come previsto e che l'attivazione del controllo degli accessi basato su tag non crei modifiche involontarie alle autorizzazioni ai flussi di lavoro di Amazon S3. Ciò ti aiuterà a garantire che le tue policy funzionino come previsto dopo l'attivazione dell'ABAC sui tuoi bucket. Per esempi di utilizzo di condizioni basate su attributi con tag, vedere. [Utilizzo di tag con bucket S3 per uso generico](#)

Includere le autorizzazioni richieste nelle politiche IAM

Sono necessarie le seguenti autorizzazioni Amazon S3 per abilitare l'ABAC per il tuo bucket:

- `s3:PutBucketAbac`— Aggiorna lo stato ABAC per il tuo bucket per uso generico.
- `s3:GetBucketAbac`— Visualizza lo stato ABAC del tuo bucket per uso generico

Dopo aver abilitato l'ABAC, le autorizzazioni utilizzate in precedenza per aggiungere tag a un bucket o eliminare tag da un bucket, `PutBucketTagging` o `DeleteBucketTagging`, non funzioneranno più. Utilizza invece le `UntagResource` API `TagResource` and per eseguire queste attività.

Ti consigliamo di utilizzare le `UntagResource` API `TagResource` and per gestire i tag prima di abilitare ABAC sui tuoi bucket. La console Amazon S3 e CloudFormation ora utilizzano le API and per impostazione predefinita. `TagResource` `UntagResource` Puoi anche disabilitare ABAC sul tuo bucket utilizzando l'API. `PutBucketAbac` Puoi utilizzarlo `GetBucketTagging` per elencare i tag nei tuoi bucket. Questa API continuerà a funzionare dopo aver abilitato l'ABAC per i tuoi bucket. In alternativa puoi anche usarla `ListTagsForResource` per elencare tutti i tag sui tuoi bucket.

Avrai bisogno delle seguenti autorizzazioni per applicare e rimuovere i tag dai bucket generici.

- `s3:TagResource`- Aggiungi tag a una AWS risorsa, ad esempio un bucket Amazon S3 per uso generico.
- `s3:UntagResource`- Rimuovi i tag da una AWS risorsa, ad esempio un bucket per uso generico Amazon S3.
- `s3:ListTagsForResource`- Visualizza i tag applicati a una AWS risorsa, ad esempio un bucket per uso generico Amazon S3.

La seguente politica IAM concede l'autorizzazione per abilitare ABAC e visualizzarne lo stato per il bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutBucketAbac",
        "s3:GetBucketAbac"
      ],
      "Resource": "arn:aws:s3:::my-s3-bucket/*"
    }
  ]
}
```

Per ulteriori informazioni sull'etichettatura dei bucket per uso generico ed esempi di politiche ABAC per i bucket generici, consulta. [Utilizzo di tag con bucket S3 per uso generico](#)

Fasi

Se disponi `s3:PutBucketAbac` dell'autorizzazione per un bucket generico, puoi abilitare ABAC per il bucket utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per abilitare ABAC per un bucket generico utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli `bucket`.
3. Scegliere il nome del bucket.
4. Scegliere la scheda Properties (Proprietà).
5. Nel pannello Bucket ABAC e scegli Modifica.
6. Scegli l'interruttore `Abilita`.
7. Rivedi e riconosci le autorizzazioni necessarie per gestire i tag dopo aver abilitato ABAC: `TagResource`, `UntagResource` e `ListTagsForResource`
8. Scegli `Save changes` (Salva modifiche).

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come aggiungere l'abilitazione ABAC per un bucket generico utilizzando il. AWS SDK for Java 2.x Per utilizzare il comando, sostituisci il *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.AbacStatus;
import software.amazon.awssdk.services.s3.model.GetBucketAbacRequest;
import software.amazon.awssdk.services.s3.model.GetBucketAbacResponse;
import software.amazon.awssdk.services.s3.model.PutBucketAbacRequest;
import software.amazon.awssdk.services.s3.model.PutBucketAbacResponse;
import software.amazon.awssdk.regions.Region;

public class BucketAbac {
    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
```

```

        S3Client s3 = S3Client.builder()
            .region(region)
            .build();

        putBucketAbac(s3, "amzn-s3-demo-bucket", "Enabled");
        getBucketAbac(s3, "amzn-s3-demo-bucket");

        putBucketAbac(s3, "amzn-s3-demo-bucket", "Disabled");
        getBucketAbac(s3, "amzn-s3-demo-bucket");
    }

    /**
     * Sets the ABAC (Attribute-Based Access Control) status for a specified S3
     bucket.
     *
     * @param s3 The S3Client instance to use for the API call
     * @param bucketName The name of the S3 bucket to update
     * @param status The desired ABAC status ("Enabled" or "Disabled")
     */
    public static void putBucketAbac(S3Client s3, String bucketName, String status)
    {
        try {
            AbacStatus abacStatus = AbacStatus.builder()
                .abacStatus(status)
                .build();
            PutBucketAbacRequest request = PutBucketAbacRequest.builder()
                .bucket(bucketName)
                .abacStatus(abacStatus)
                .build();
            s3.putBucketAbac(request);
        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Retrieves the current ABAC (Attribute-Based Access Control) status for a
     specified S3 bucket.
     *
     * @param s3 The S3Client instance to use for the API call
     * @param bucketName The name of the S3 bucket to query
     */
    public static void getBucketAbac(S3Client s3, String bucketName) {

```

```
    try {  
        GetBucketAbacRequest request = GetBucketAbacRequest.builder()  
            .bucket(bucketName)  
            .build();  
        GetBucketAbacResponse response = s3.getBucketAbac(request);  
    } catch (S3Exception e) {  
        System.err.println(e.awsErrorDetails().errorMessage());  
        System.exit(1);  
    }  
}
```

Questo esempio mostra come aggiungere enable ABAC per un bucket generico utilizzando l'AWS SDK per Java 2.x. Per utilizzare il comando, sostituisci il file `user input placeholders` con le tue informazioni.

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'aggiunta di tag a un bucket generico, consulta la seguente sezione nell'Amazon Simple Storage Service API Reference:

- [PutBucketAbac](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio di CLI mostra come abilitare ABAC per un bucket generico utilizzando. AWS CLI Per utilizzare il comando, sostituisci il *`user input placeholders`* con le tue informazioni.

Richiesta:

```
# Enable ABAC on a general purpose bucket  
  
aws s3api put-bucket-abac --bucket amzn-s3-demo-bucket --abac-status Status=Enabled --  
region us-east-2  
  
# Disable ABAC on a general purpose bucket
```

```
aws s3api put-bucket-abac --bucket amzn-s3-demo-bucket --abac-status Status=Disabled --
region us-east-2

# Get ABAC status on a general purpose bucket

aws s3api get-bucket-abac --bucket amzn-s3-demo-bucket --region us-east-2
```

Creazione di bucket generici con tag

Puoi etichettare i bucket generici di Amazon S3 quando li crei. Non sono previsti costi aggiuntivi per l'utilizzo dei tag nei bucket oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sull'etichettatura dei bucket, consulta. [Utilizzo di tag con bucket S3 per uso generico](#)

Permissions

Per creare un bucket con tag, devi disporre delle seguenti autorizzazioni:

- s3:CreateBucket
- s3:TagResource

Console Amazon S3 e CloudFormation ora utilizza questa funzionalità per creare bucket con tag.

Risoluzione degli errori

Se riscontri un errore durante il tentativo di creare un bucket con tag, puoi fare quanto segue:

- Verifica di avere i requisiti [Permissions](#) per creare il bucket e aggiungervi un tag.
- Controlla la tua policy IAM per le chiavi `aws:TagKeys` di `aws:RequestTag/key-name` condizione. Potrebbe esserti richiesto di etichettare i bucket solo con chiavi e valori di tag specifici. Per ulteriori informazioni, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

Note

Amazon S3 e CloudFormation ora utilizza questa funzionalità per creare bucket con tag. Quando crei bucket con tag, tieni presente che le condizioni basate sui tag per accedere al bucket utilizzando `aws:ResourceTag` e le chiavi di `s3:BucketTag` condizione sono

applicabili solo dopo aver abilitato ABAC sul bucket. Per ulteriori informazioni, consulta [Abilitazione dell'ABAC in bucket generici](#).

Fasi

Puoi creare un bucket con i tag applicati utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per creare un bucket con tag utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli **bucket**.
3. Scegli **crea bucket** per creare un nuovo bucket.
4. Crea un bucket, un bucket per uso generico, come faresti normalmente; vedi. [Creazione di un bucket per uso generico](#)
5. Nella pagina **Crea bucket**, **Tags** è un'opzione per creare un nuovo bucket.
6. Inserisci un nome per il bucket. Per ulteriori informazioni, consulta [Regole di denominazione dei bucket per uso generico](#).
7. Scegli **Aggiungi nuovo tag** per aprire l'editor di tag e inserisci una coppia chiave-valore di tag. La chiave di tag è obbligatoria, mentre il valore è facoltativo.
8. Per aggiungere un altro tag, scegli nuovamente **Aggiungi nuovo tag**. È possibile inserire fino a 50 coppie chiave-valore di tag.
9. Dopo aver specificato le opzioni per il nuovo bucket, scegli **Crea bucket**.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come creare un bucket generico con tag utilizzando. AWS SDK for Java 2.x Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
```

```
import software.amazon.awssdk.services.s3.model.BucketLocationConstraint;
import software.amazon.awssdk.services.s3.model.CreateBucketConfiguration;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.CreateBucketResponse;
import software.amazon.awssdk.services.s3.model.Tag;

public class CreateBucketWithTagsExample {
    public static void createBucketWithTagsExample() {
        S3Client s3 = S3Client.builder().region(Region.US_WEST_2).build();

        CreateBucketConfiguration bucketConfiguration =
        CreateBucketConfiguration.builder()
            .locationConstraint(BucketLocationConstraint.US_WEST_2)
            .tags(Tag.builder().key("MyTagKey").value("MyTagValue").build())
            .build();

        CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
            .bucket("mybucket")
            .createBucketConfiguration(bucketConfiguration)
            .build();

        CreateBucketResponse response = s3.createBucket(createBucketRequest);
        System.out.println("Status code (should be 200):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la creazione di un bucket generico con tag, consulta la seguente sezione nell'Amazon Simple Storage Service API Reference:

- [CreateBucket](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come creare un bucket con tag utilizzando AWS CLI. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Quando si crea un bucket, è necessario fornire i dettagli di configurazione e utilizzare la seguente convenzione di denominazione: *amzn-s3-demo-bucket*

Richiesta:

```
aws s3api create-bucket \  
--bucket mybucket \  
--create-bucket-configuration 'LocationConstraint=us-  
west-2,Tags=[{Key=MyTagKey,Value=MyTagValue}]' --region us-west-2"
```

Risposta:

```
{  
  "Location": "http://mybuckets3.amazonaws.com/"  
}
```

Aggiungere un tag a un bucket

Puoi aggiungere tag ai bucket Amazon S3 e modificare questi tag. Non sono previsti costi aggiuntivi per l'utilizzo dei tag nei bucket oltre alle tariffe di richiesta dell'API S3 standard. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#). Per ulteriori informazioni sull'etichettatura dei bucket, consulta [Utilizzo di tag con bucket S3 per uso generico](#)

Permissions

Per aggiungere un tag a un bucket, devi disporre della seguente autorizzazione:

- s3:TagResource

Risoluzione degli errori

Se si verifica un errore quando si tenta di aggiungere un tag a un bucket, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per aggiungere un tag a un bucket.
- Se hai tentato di aggiungere una chiave tag che inizia con il prefisso AWS riservato `aws :`, modifica la chiave del tag e riprova.

Fasi

Puoi aggiungere tag ai bucket utilizzando la console Amazon S3, l'interfaccia a riga di AWS comando (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per aggiungere tag a un bucket utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli `bucket`.
3. Scegliere il nome del bucket.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri la sezione Tag e scegli Aggiungi nuovo tag.
6. Viene visualizzata la pagina Aggiungi tag. È possibile inserire fino a 50 coppie chiave-valore di tag.
7. Se si aggiunge un nuovo tag con lo stesso nome di chiave di un tag esistente, il valore del nuovo tag sovrascrive il valore del tag esistente.
8. In questa pagina è anche possibile modificare i valori dei tag esistenti.
9. Dopo aver aggiunto i tag, scegli Salva le modifiche.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come aggiungere tag a un bucket generico utilizzando il. AWS SDK for Java 2.x Per utilizzare il comando, sostituisci il *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;
import software.amazon.awssdk.services.s3control.model.TagResourceResponse;

public class TagResourceExample {
    public static void tagResourceExample() {
```



```
S3ControlClient s3Control =
S3ControlClient.builder().region(Region.US_WEST_2).build();

TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
    .resourceArn("arn:aws:s3:::bucket/my-bucket")
    .accountId("111122223333")
    .tags(Tag.builder().key("MyTagKey").value("MyTagValue").build())
    .build();

TagResourceResponse response = s3Control.tagResource(tagResourceRequest);
System.out.println("Status code (should be 204):");
System.out.println(response.sdkHttpResponse().statusCode());
}
}
```

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'aggiunta di tag a un bucket generico, consulta la seguente sezione nell'Amazon Simple Storage Service API Reference:

- [TagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come aggiungere tag a un bucket generico utilizzando il. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control tag-resource --resource-arn arn:aws:s3:::amzn-s3-demo-bucket --region us-east-2 --account-id 444455556666 --tags '[{"Key":"mykey","Value":"myvalue"}]'
```

Visualizzazione dei bucket tag

È possibile visualizzare o elencare i tag applicati ai bucket S3. Per ulteriori informazioni sui tag, consulta [Utilizzo di tag con bucket S3 per uso generico](#).

Permissions

Per visualizzare i tag applicati a un bucket, è necessario disporre delle seguenti autorizzazioni:

- `s3:ListTagsForResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di elencare o visualizzare i tag di un bucket, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per visualizzare o elencare i tag del bucket.

Fasi

Puoi visualizzare i tag applicati ai bucket utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK. AWS

Utilizzo della console S3

Per visualizzare i tag applicati a un bucket utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli `bucket`.
3. Scegliere il nome del bucket.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag per visualizzare tutti i tag applicati al bucket generico.
6. La sezione Tag mostra i User-defined tag per impostazione predefinita. Puoi selezionare la scheda dei tag AWS generati per visualizzare i tag applicati al bucket dai AWS servizi.

Utilizzo di AWS SDK

Questa sezione fornisce un esempio di come visualizzare i tag applicati a un bucket generico utilizzando gli SDK. AWS

SDK for Java 2.x

Questo esempio mostra come visualizzare i tag applicati a un bucket generico utilizzando il AWS SDK for Java 2.x

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResourceExample {
    public static void listTagsForResourceExample() {
        S3ControlClient s3Control =
            S3ControlClient.builder().region(Region.US_WEST_2).build();

        ListTagsForResourceRequest listTagsForResourceRequest =
            ListTagsForResourceRequest.builder()
                .resourceArn("arn:aws::s3::bucket/my-bucket")
                .accountId("111122223333")
                .build();

        ListTagsForResourceResponse response =
            s3Control.listTagsForResource(listTagsForResourceRequest);
        System.out.println("Tags on my resource:");
        System.out.println(response.toString());
    }
}
```

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per la visualizzazione dei tag applicati a un bucket generico, consulta la seguente sezione nel riferimento alle API di Amazon Simple Storage Service:

- [ListTagsforResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI](#) nella Guida per l'utente. AWS Command Line Interface

Il seguente esempio CLI mostra come visualizzare i tag applicati a un bucket. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control list-tags-for-resource \  
--account-id 111122223333 \  
--resource-arn arn:aws::s3:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3 \  

```

Risposta con tag:

```
{  
  "Tags": [  
    {  
      "Key": "MyKey1",  
      "Value": "MyValue1"  
    },  
    {  
      "Key": "MyKey2",  
      "Value": "MyValue2"  
    },  
    {  
      "Key": "MyKey3",  
      "Value": "MyValue3"  
    }  
  ]  
}
```

Risposta senza tag:

```
{  
  "Tags": []  
}
```

Eliminare un tag da un bucket

Puoi rimuovere i tag dai bucket S3. Un AWS tag è una coppia chiave-valore che contiene metadati sulle risorse, in questo caso i bucket Amazon S3. Per ulteriori informazioni sui tag, consulta [Utilizzo di tag con bucket S3 per uso generico](#).

 Note

Se elimini un tag e in seguito scopri che è stato utilizzato per tenere traccia dei costi o per il controllo degli accessi, puoi aggiungere nuovamente il tag al bucket.

Permissions

Per eliminare un tag da un bucket, devi disporre della seguente autorizzazione:

- `s3:UntagResource`

Risoluzione degli errori

Se si verifica un errore quando si tenta di eliminare un tag da un bucket, è possibile effettuare le seguenti operazioni:

- Verifica di avere i requisiti [Permissions](#) per eliminare un tag da un bucket.

Fasi

Puoi eliminare i tag dai bucket utilizzando la console Amazon S3, AWS Command Line Interface (AWS CLI), l'API REST di Amazon S3 e gli SDK AWS.

Utilizzo della console S3

Per eliminare i tag da un bucket utilizzando la console Amazon S3:

1. Accedi alla console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione a sinistra, scegli `bucket`.
3. Scegliere il nome del bucket.
4. Scegliere la scheda Properties (Proprietà).
5. Scorri fino alla sezione Tag e seleziona la casella di controllo accanto al tag o ai tag che desideri eliminare.
6. Scegliere Elimina.
7. Viene visualizzato il pop-up Elimina tag definiti dall'utente che chiede di confermare l'eliminazione del tag o dei tag selezionati.

8. Seleziona Elimina per confermare.

Utilizzo di AWS SDK

SDK for Java 2.x

Questo esempio mostra come eliminare i tag da un bucket generico utilizzando il AWS SDK for Java 2.x. Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;
import software.amazon.awssdk.services.s3control.model.UntagResourceResponse;

public class UntagResourceExample {
    public static void untagResourceExample() {
        S3ControlClient s3Control =
            S3ControlClient.builder().region(Region.US_WEST_2).build();

        UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
            .resourceArn("arn:aws:s3:::bucket/my-bucket")
            .accountId("111122223333")
            .tagKeys("myTagKey")
            .build();

        UntagResourceResponse response =
            s3Control.untagResource(untagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilizzo della REST API

Per informazioni sul supporto dell'API REST di Amazon S3 per l'eliminazione di tag da un bucket generico, consulta la seguente sezione nell'Amazon Simple Storage Service API Reference:

- [UntagResource](#)

Utilizzo di AWS CLI

Per installare la AWS CLI, consulta [Installazione della AWS CLI nella Guida per l'utente](#). AWS Command Line Interface

Il seguente esempio CLI mostra come eliminare i tag da un bucket generico utilizzando il. AWS CLI Per utilizzare il comando, sostituisci il file *user input placeholders* con le tue informazioni.

Richiesta:

```
aws s3control untag-resource \  
--resource-arn arn:aws:s3:::amzn-s3-demo-bucket --region us-east-2 --account-  
id 111122223333 \  
--tag-keys "tagkey1" "tagkey2"
```

Quote

Il tuo Account AWS dispone di quote di default, precedentemente definite limiti, per ogni servizio AWS. Le quote di Amazon S3 includono il numero di bucket generici, bucket di directory, punti di accesso e altro ancora. È possibile richiedere un aumento per alcune quote, ma non per tutte. Gli aumenti non vengono concessi immediatamente, quindi potrebbero essere necessari un paio di giorni perché diventino effettivi.

Per un elenco delle quote Amazon S3 e dei relativi valori predefiniti, consulta [Quote di Amazon S3](#) in Riferimenti generali di AWS.

Aumenti delle quote

Per richiedere un aumento delle quote

È possibile richiedere un aumento di quota utilizzando una delle seguenti opzioni:

- Dalla Console di gestione AWS: aprire la [console Service Quotas](#). Nel pannello di navigazione, scegliere servizi AWS. Seleziona Amazon S3, seleziona una quota e segu le istruzioni per richiedere l'aumento della quota. Per istruzioni, consulta [Richiesta di un aumento di quota](#) nella Guida per l'utente delle Service Quotas.
- Dalla AWS CLI: utilizzare il comando [request-service-quota-increase](#) della AWS CLI. Per istruzioni, consulta [Richiesta di un aumento di quota](#) nella Guida per l'utente delle Service Quotas.

Riferimento

Oltre alla console Amazon S3, è possibile lavorare con Amazon S3 a livello di codice utilizzando le REST API di Amazon S3, gli SDK AWS o l'AWS Command Line Interface (AWS CLI).

- [Documentazione di riferimento delle API di Amazon Simple Storage Service](#)
- [Esempi di codice](#) nella Documentazione di riferimento delle API di Amazon Simple Storage Service
- [Interfaccia della linea di comando AWS](#) nella Guida per l'utente dell'AWS Command Line Interface.
- [AWS SDK](#)

Documentazione sugli SDK	Esempi di codice
AWS SDK per C++	AWS SDK per C++ Esempi di codice
AWS CLI	Esempi di codice AWS CLI.
AWS SDK per Go	AWS SDK per Go Esempi di codice
AWS SDK per Java	AWS SDK per Java Esempi di codice
AWS SDK per JavaScript	AWS SDK per JavaScript Esempi di codice
AWS SDK per Kotlin	AWS SDK per Kotlin Esempi di codice
AWS SDK per .NET	AWS SDK per .NET Esempi di codice
AWS SDK per PHP	AWS SDK per PHP Esempi di codice
AWS Strumenti per PowerShell	Strumenti per esempi di codice PowerShell
AWS SDK per Python (Boto3)	AWS SDK per Python (Boto3) Esempi di codice
AWS SDK per Ruby	AWS SDK per Ruby Esempi di codice
AWS SDK per Rust	AWS SDK per Rust Esempi di codice
AWS SDK per SAP ABAP	AWS SDK per SAP ABAP Esempi di codice

Documentazione sugli SDK	Esempi di codice
AWS SDK per Swift	AWS SDK per Swift Esempi di codice

Cronologia dei documenti

- Versione API corrente: 2006-03-01

Nella tabella seguente vengono descritte le modifiche importanti apportate a ciascuna versione della Documentazione di riferimento delle API di Amazon Simple Storage Service e della Guida per l'utente di Amazon S3. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile iscriversi a un feed RSS.

Modifica	Descrizione	Data
Amazon S3 Express One Zone aggiunge nuove policy gestite AWS	Amazon S3 Express One Zone ha aggiunto nuove politiche AWS gestite denominate e. <code>AmazonS3ExpressFullAccess</code> <code>AmazonS3ExpressReadOnlyAccess</code> Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon S3 Express One Zone .	3 aprile 2026
S3 Tables ha aggiornato la policy <code>AmazonS3TablesFullAccess</code> AWS gestita per S3 Tables	S3 Tables ha aggiornato la politica gestita AWS denominata. <code>AmazonS3TablesFullAccess</code> Questa policy ora concede le autorizzazioni per passare un ruolo al servizio S3 Tables Replication. Per ulteriori informazioni, consulta Policy gestite da AWS per Tabelle S3 .	2 dicembre 2025
S3 Tables ora supporta la replica automatica	S3 Tables ora supporta la replica automatica delle tabelle	2 dicembre 2025

Apache Iceberg archiviate nei bucket di tabelle Amazon S3. Per ulteriori informazioni, consulta Replicating S3 tables. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-tables-replication-tables.html>

[S3 Tables ora supporta i Intelligent-Tiering livelli di accesso](#)

S3 Tables ora supporta i livelli di Intelligent-Tiering accesso che monitorano continuamente i modelli di accesso e spostano automaticamente i dati delle tabelle tra i livelli di accesso. Per ulteriori informazioni, consulta Ottimizzazione dei [costi per le tabelle con Intelligent-Tiering](#)

2 dicembre 2025

[Supporto per oggetti di grandi dimensioni](#)

Amazon S3 ha aumentato la dimensione massima di un oggetto che puoi archiviare in un bucket S3 da 5 TB a 50 TB. Per caricare questi oggetti più grandi, devi implementare l'API REST Multipart Upload per caricare oggetti in parti e, quando scarichi questi oggetti, utilizza `GetObject` richieste simultanee, poiché le singole richieste GET sono limitate a 5 TB. Per ulteriori informazioni, vedere [Caricamento di oggetti e Scaricamento di oggetti](#).
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/download-objects.html>

2 dicembre 2025

[I metadati di Amazon S3 sono ora disponibili in altri 22 Regioni AWS](#)

Per ulteriori informazioni, consulta [Amazon S3 Metadata. Regioni AWS](#)

26 novembre 2025

[La console Amazon S3 aggiunge l'integrazione con Amazon SageMaker Unified Studio per Amazon S3 Tables](#)

Ora puoi interrogare i tuoi dati in S3 Tables utilizzando un ricco editor SQL fornito da Amazon SageMaker Unified Studio, accessibile direttamente dalla console S3 con pochi clic. In SageMaker Unified Studio, puoi scrivere query SQL o porre domande utilizzando il linguaggio naturale e una query SQL viene generata automaticamente in base al contesto dei tuoi dati. Quindi, puoi pianificare le query per automatizzare l'elaborazione dei dati. Per ulteriori informazioni, consulta [Utilizzo delle tabelle S3 con SageMaker Unified Studio](#).

21 novembre 2025

[Amazon S3 ora supporta i tag sulle tabelle S3 per il controllo degli accessi basato sugli attributi \(ABAC\) e l'allocazione dei costi](#)

6 novembre 2025

Amazon S3 ora supporta l'etichettatura delle tabelle S3 per il controllo degli accessi basato sugli attributi (ABAC) e l'allocazione dei costi. Puoi utilizzare i tag per ABAC per gestire automaticamente le autorizzazioni per utenti e ruoli che accedono a bucket e tabelle di tabelle, eliminando i frequenti aggiornamenti delle policy basate sulle risorse di IAM o S3 Tables e semplificando il modo in cui gestisci l'accesso su larga scala. Puoi anche aggiungere tag alle singole tabelle per tracciare e organizzare i costi utilizzando la fatturazione e la gestione dei costi. AWS AWS Amazon S3 supporta i tag su S3 Tables in tutti i Regioni AWS casi in cui S3 Tables è disponibile. Puoi iniziare a utilizzare i tag utilizzando la console di AWS gestione, l'SDK, l'API o l'interfaccia a riga di comando. Per ulteriori informazioni, vedere [Tagging for cost allocation o Attribute-Based Access Control \(ABAC\)](#).

[I metadati di Amazon S3 sono ora disponibili in tre versioni aggiuntive Regioni AWS](#)

I metadati di Amazon S3 sono ora disponibili in altri tre Regioni AWS: Europa (Francoforte), Europa (Irlanda) e Asia Pacifico (Tokyo). Per ulteriori informazioni, consulta [Amazon S3 Metadata. Regioni AWS](#)

22 ottobre 2025

[Lambda per oggetti S3 non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025](#)

Lambda per oggetti S3 non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzare Lambda per oggetti S3, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [Modifica della disponibilità di Lambda per oggetti Amazon S3](#).

7 ottobre 2025

[Amazon S3 ora supporta le eliminazioni condizionali nei bucket per uso generico](#)

16 settembre 2025

Amazon S3 ora supporta le eliminazioni condizionali nei bucket per uso generico. Le eliminazioni condizionali verificano che un oggetto non sia stato modificato prima di eliminarlo. L'utilizzo di eliminazioni condizionali consente di prevenire eliminazioni accidentali in scenari con elevata concorrenza e più writer. Ora puoi eseguire eliminazioni condizionali utilizzando l'intestazione HTTP `if-match` con un valore ETag. Amazon S3 consente che la richiesta di eliminazione abbia esito positivo solo se l'ETag fornito corrisponde a quello dell'oggetto. Inoltre, è possibile utilizzare la chiave di condizione `s3:if-match` nelle policy di bucket S3 per applicare operazioni di eliminazione condizionale. Ad esempio, è possibile richiedere ai client di utilizzare l'intestazione HTTP `if-match` in entrambe le richieste delle operazioni API `DeleteObject` e `DeleteObjects`, in modo da ridurre al minimo il rischio di eliminare accidentalmente oggetti nel bucket. Per ulteriori informazioni, consulta

[Amazon S3 Batch Operations ora supporta la gestione di oggetti all'interno di un bucket S3, prefisso, suffisso o altro, in un solo passaggio nella console Amazon S3](#)

[Come eseguire le eliminazioni condizionali.](#)

15 settembre 2025

Quando si crea un processo di Operazioni in batch S3, è possibile specificare gli oggetti su cui eseguire l'operazione. Con questa funzionalità, è possibile invece specificare un intero bucket, un prefisso, un suffisso, una data di creazione o una classe di archiviazione. Operazioni in batch applica quindi l'operazione a tutti gli oggetti corrispondenti e avvisa quando il processo è terminato. Per ulteriori informazioni, consulta [Esecuzione di operazioni sugli oggetti in blocco con le operazioni in batch.](#)

[Amazon S3 ora supporta i tag Access Points per il controllo degli accessi basato sugli attributi \(ABAC\)](#)

Amazon S3 ora supporta il tagging dei punti di accesso sia per bucket per uso generico sia per bucket di directory. Aggiungi i tag ai punti di accesso e utilizza il controllo degli accessi basato su attributi (ABAC) per scalare l'accesso. Puoi iniziare a etichettare gli access point utilizzando la console di AWS gestione, l'API REST S3, la CLI o l'SDK. AWS AWS Per ulteriori informazioni sull'utilizzo dei tag per ABAC, consulta [Utilizzo dei tag per il controllo degli accessi basato su attributi \(ABAC\)](#).

31 luglio 2025

[Amazon S3 Vectors \(anteprima\)](#)

Amazon S3 Vectors offre un'archiviazione vettoriale personalizzata e ottimizzata in termini di costi per le applicazioni di ricerca semantica e intelligenza artificiale. S3 Vectors introduce un nuovo tipo di bucket, il bucket vettoriale, ottimizzato per un'archiviazione vettoriale durevole e a basso costo. Per ulteriori informazioni, consulta [Utilizzo di S3 Vectors e bucket di vettori](#).

15 luglio 2025

[Amazon S3 Metadata ora supporta gli oggetti esistenti](#)

15 luglio 2025

Amazon S3 Metadata crea e gestisce metadati che forniscono informazioni sui set di dati archiviati in S3, in modo da poter individuare e utilizzare e più facilmente i dati S3. In precedenza, S3 Metadata supportava oggetti nuovi e aggiornati. Ora, S3 Metadata crea e gestisce i metadati per tutti i dati S3 esistenti. S3 Metadata ora crea e gestisce due tabelle Apache Iceberg che offrono una visualizzazione sottoponibile a query e continuamente aggiornata dei metadati associati agli oggetti in un bucket per uso generico. Una tabella del diario registra le modifiche apportate ai dati pressoché in tempo reale, aiutando a individuare i nuovi dati caricati nel bucket, tracciare gli oggetti eliminati di recente, monitorare e le transizioni del ciclo di vita S3 e altro ancora. Una nuova tabella di inventario in tempo reale fornisce e mantiene una visualizzazione aggiornata di tutti gli oggetti nel bucket. Entrambe le tabelle di metadati S3 sono archiviate in un bucket di tabelle Iceberg AWS gestito nel tuo account e possono

essere interrogate utilizzando SQL standard tramite servizi di AWS analisi, come Amazon Athena o Amazon EMR, e strumenti open source, come e. DuckDB Pylceberg. Per ulteriori informazioni, consulta [Accelerazione dell'individuazione dei dati con S3 Metadata](#).

[Amazon S3 Express One Zone ora supporta i tag per l'allocazione dei costi e il controllo degli accessi basato sugli attributi](#)

2 luglio 2025

Amazon S3 Express One Zone, una classe di archiviazione S3 ad alte prestazioni, ora supporta i tag per l'allocazione dei costi e il controllo degli accessi basato su attributi (ABAC). Puoi aggiungere tag ai bucket di directory S3 per tracciare e organizzare i costi utilizzando AWS Gestione costi e fatturazione AWS. Inoltre, con il supporto ABAC, è possibile scalare il controllo degli accessi ai bucket di directory utilizzando i tag. S3 Express One Zone supporta i tag sui bucket di directory in ogni Regione AWS in cui è disponibile la classe di archiviazione. Puoi iniziare a taggare utilizzando la console di AWS gestione, l'API REST S3, la AWS CLI o l'SDK. AWS Per ulteriori informazioni sull'utilizzo dei tag per semplificare l'allocazione dei costi o ABAC, consulta [Utilizzo di tag con i bucket di directory S3](#).

[S3 Tables ora supporta eventi per le operazioni di manutenzione CloudTrail](#)

S3 Tables ora supporta AWS CloudTrail gli eventi per le operazioni di manutenzione. Ora puoi tracciare e controllare le attività di manutenzione eseguite sulle tue risorse S3 Tables tramite i CloudTrail log. Per ulteriori informazioni, consulta [Manutenzione di Tabelle S3](#).

30 giugno 2025

[Gli access point ora supportano il collegamento a un volume FSx for OpenZFS](#)

Puoi creare e collegare un punto di accesso a un volume FSx per OpenZFS utilizzando la console o l'API di Amazon FSx. AWS CLI Una volta collegato, si possono utilizzare le API degli oggetti S3 per accedere ai dati dei file. I dati continuano a risiedere nel file system Amazon FSx e continuano a essere direttamente accessibili per i carichi di lavoro esistenti. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi con punti di accesso](#).

25 giugno 2025

[S3 Tables ora supporta nuove strategie di compattazione per le tabelle](#)

Tabelle S3 ora supporta diverse strategie di compattazione per ottimizzare le prestazioni delle query in base a diversi modelli di accesso ai dati. Le nuove strategie includono Sort e Z-order. Per ulteriori informazioni, consulta [Strategie di compattazione per le tabelle](#).

18 giugno 2025

[Messaggi di errore di
accesso negato avanzati
per le richieste della stessa
organizzazione](#)

Amazon S3 ora include un contesto aggiuntivo negli errori di accesso negato (HTTP 403 Forbidden) per le richieste effettuate a risorse all'interno della stessa organizzazione in AWS Organizations. Questo nuovo contesto include il tipo di policy che ha negato l'accesso, il motivo del rifiuto e le informazioni sull'utente o sul ruolo AWS Identity and Access Management (IAM) che ha richiesto l'accesso alla risorsa. Questo contesto consente di risolvere i problemi di accesso, identificare la causa principale degli errori di accesso negato e correggere i controlli di accesso errati aggiornando le policy pertinenti. Questo contesto aggiuntivo è disponibile anche nei AWS CloudTrail log. I messaggi di errore di accesso negato avanzato per le richieste relative alla stessa organizzazione sono ora disponibili in tutte le Regioni AWS, comprese le regioni cinesi AWS GovCloud (US) Regions e cinesi. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi agli errori di accesso](#)

16 giugno 2025

[negato \(403 Accesso negato\) in Amazon S3.](#)

[S3 Tables aggiunge una nuova politica AWS gestita per S3 Tables](#)

S3 Tables ha aggiunto una nuova politica gestita AWS denominata. AmazonS3TablesLakeFormationServiceRole. Questa policy fornisce autorizzazioni che consentono al ruolo di servizio Lake Formation di accedere alle tabelle e ai bucket di tabelle Amazon S3. Per ulteriori informazioni, consulta [Policy gestite da AWS per Tabelle S3](#).

19 maggio 2025

[S3 Tables ora supporta l' SSE-KMS utilizzo di chiavi gestite dal cliente](#)

S3 Tables ora supporta la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS) utilizzando chiavi gestite dal cliente. È possibile applicare SSE-KMS la crittografia a livello di bucket e tabella. Per ulteriori informazioni, vedere [Utilizzo della crittografia lato server con AWS KMS keys \(SSE-KMS\) nei bucket di tabella](#).

16 aprile 2025

[I punti di accesso per i bucket di directory sono disponibili nelle zone locali AWS](#)

I bucket di directory ora supportano i punti di accesso per semplificare la gestione dell'accesso ai dati su larga scala per i set di dati condivisi in Amazon S3. Grazie a questa nuova funzionalità, è possibile creare centinaia di punti di accesso per bucket, ognuno con un nome distinto e autorizzazioni personalizzate per ogni applicazione. Per ulteriori informazioni, consulta [Gestione dell'accesso a set di dati condivisi in bucket di directory con punti di accesso.](#)

31 marzo 2025

[L'integrazione dei bucket di tabelle S3 con Amazon SageMaker Lakehouse è ora disponibile a livello generale](#)

13 marzo 2025

Puoi integrare i bucket di tabelle S3 con Amazon SageMaker Lakehouse per accedere alle tabelle da servizi di AWS analisi, come Amazon Athena, Amazon Redshift e Quick. Amazon SageMaker Lakehouse unifica i tuoi dati tra data lake Amazon S3 e data warehouse Amazon Redshift, così puoi creare applicazioni di analisi, apprendimento automatico (ML) e intelligenza artificiale generativa su una singola copia dei dati. L'integrazione li compila AWS Glue Data Catalog con le risorse della tua tabella e federa l'accesso a queste risorse con. AWS Lake Formation L'integrazione consente un controllo degli accessi dettagliato tramite Lake Formation per garantire ulteriore sicurezza . Per ulteriori informazioni sull'integrazione, consulta [Utilizzo di tabelle Amazon S3 con servizi di analisi. AWS](#) Se si configura l'integrazione con la versione di anteprima , è possibile continuare a utilizzare l'integrazione attuale. Tuttavia, il processo di integrazione aggiornato offre miglioramenti delle

prestazioni, quindi è consigliabile effettuare la migrazione. Per migrare all'integrazione aggiornata, consulta [Migrazione e al processo di integrazione aggiornata](#).

[Aggiunta del supporto per la creazione di tabelle e query di Tabelle S3 alla console Amazon S3](#)

Tabelle S3 ora supporta le operazioni di creazione di tabelle e query di tabelle direttamente dalla console Amazon S3 tramite Amazon Athena. Con questa nuova funzionalità, ora è possibile creare una tabella, popolarla con dati e sottoporla a query con pochi passaggi nella console Amazon S3. Per ulteriori informazioni, consulta [Creazione di una tabella di Amazon S3](#) e [Query di tabelle Amazon S3 con Athena](#).

13 marzo 2025

[S3 Tables aggiunge il supporto per l'aggiunta di schemi durante la creazione di tabelle](#)

Ora è possibile utilizzare l'operazione API CreateTable di Tabelle S3 per creare tabelle con schemi aggiungendo un flag di metadati facoltativo. Per ulteriori informazioni, consulta [Creazione di una tabella Amazon S3](#).

30 gennaio 2025

[S3 Metadata è ora disponibile a livello generale](#)

Amazon S3 Metadata è ora disponibile a livello generale. S3 Metadata consente di individuare e comprendere facilmente i dati S3 con metadati automatizzati e sottoponibili a query che si aggiornano pressoché in tempo reale. Con S3 Metadata, puoi curare, identificare e utilizzare i tuoi dati S3 per l'analisi aziendale, la formazione di modelli di intelligenza artificiale e machine learning (AI/ML) e altro ancora. S3 Metadata supporta i metadati degli oggetti, che includono informazioni definite dal sistema, ad esempio la dimensione e l'origine dell'oggetto, e i metadati personalizzati, ad esempio tag con informazioni come SKU dei prodotti, ID delle transazioni o classificazioni dei contenuti. Per ulteriori informazioni, consulta [Accelerazione dell'individuazione dei dati con S3 Metadata](#).

27 gennaio 2025

[AWS politiche gestite: nuove politiche](#)

S3 Tables ha aggiunto due nuove politiche AWS gestite.

6 dicembre 2024

Tabelle S3

Tabelle Amazon S3 fornisce l'archiviazione S3 ottimizzata per carichi di lavoro di analisi, con funzionalità che migliorano le prestazioni delle query, riducono i costi di archiviazione per le tabelle e semplificano il funzionamento dei data lake su larga scala. Tabelle S3 introduce un nuovo tipo di bucket: i bucket di tabelle, creati appositamente per archiviare le tabelle Apache Iceberg come risorse secondarie. I bucket di tabelle offrono transazioni al secondo (TPS) più elevate e un throughput di query migliore rispetto alle tabelle autogestite nei bucket per uso generico di S3. Puoi integrare automaticamente i tuoi bucket di tabelle con servizi di AWS analisi, come Athena, Amazon Redshift Quick e altri. Per ulteriori informazioni, consulta [Utilizzo di Tabelle Amazon S3 e dei bucket di tabelle](#).

3 dicembre 2024

[Anteprima di S3 Metadata](#)

3 dicembre 2024

Amazon S3 Metadata consente di individuare e comprendere facilmente i dati S3 con metadati automatizzati e sottoponibili a query che si aggiornano pressoché in tempo reale. Con S3 Metadata, puoi curare, identificare e utilizzare i tuoi dati S3 per l'analisi aziendale, la formazione e sui modelli di intelligenza artificiale e machine learning () e altro ancora. AI/ML S3 Metadata supporta i metadati degli oggetti, che includono informazioni definite dal sistema, ad esempio la dimensione e l'origine dell'oggetto, e i metadati personalizzati, ad esempio tag con informazioni come SKU dei prodotti, ID delle transazioni o classificazioni dei contenuti. Per ulteriori informazioni, consulta [Accelerazione dell'individuazione dei dati con S3 Metadata](#).

[Storage Browser per S3](#)

Storage Browser per S3 è un componente open source che è possibile aggiungere alle applicazioni web per fornire agli utenti finali un'interfaccia semplice per i dati archiviati in S3. Per ulteriori informazioni, consulta [Storage Browser per S3](#).

1 dicembre 2024

[Nuovo algoritmo di checksum di Amazon S3 e funzionalità di integrità del checksum migliorate](#)

Amazon S3 aggiunge l'algoritmo di checksum CRC-64NVM e funzionalità di integrità del checksum migliorate. Per ulteriori informazioni, consulta [Verifica dell'integrità degli oggetti in Amazon S3](#).

1 dicembre 2024

[Carichi di lavoro di residenza dei dati](#)

In Zone locali dedicate, è possibile creare bucket di directory S3 per archiviare i dati per i casi d'uso relativi alla residenza e all'isolamento dei dati. Per ulteriori informazioni, consulta [Carichi di lavoro di residenza dei dati](#).

1 dicembre 2024

[Nuove chiavi di condizione per applicare le scritture condizionali](#)

Amazon S3 aggiunge nuove chiavi di condizione `s3:if-match` e `s3:if-none-match` da utilizzare nelle policy dei bucket per forzare i client a utilizzare l'intestazione HTTP `If-None-Match` o `If-Match`. Per ulteriori informazioni, consulta l'argomento relativo all'[applicazione delle scritture condizionali sui bucket Amazon S3](#).

25 novembre 2024

[Nuova intestazione HTTP per le scritture condizionali per verificare se l'oggetto è cambiato](#)

Amazon S3 aggiunge l'intestazione HTTP `If-Match` per controllare il tag di entità (ETag) di un oggetto prima di scrivere un oggetto per alcune operazioni API. Con questa intestazione, Amazon S3 confronta il valore ETag fornito con il valore ETag dell'oggetto in S3. Se i valori ETag non corrispondono, l'operazione non riesce. Per ulteriori informazioni, consulta [Come prevenire la sovrascrittura degli oggetti con le scritture condizionali](#).

25 novembre 2024

[Amazon Redshift ora si integra con S3 Access Grants](#)

I clienti di Amazon Redshift possono ora utilizzare S3 Access Grants per scalare e gestire le autorizzazioni per i dati S3. Ciò consente ai clienti di Amazon Redshift di scalare le autorizzazioni S3 per le identità aziendali utilizzando Centro identità AWS IAM e per utenti e gruppi IAM. Per ulteriori informazioni, consulta [Integrazione di Amazon Redshift con Amazon S3 Access Grants](#).

15 novembre 2024

[AWS Organizations gli account membri possono ora riottenere l'accesso ai bucket Amazon S3 bloccati accidentalmente](#)

AWS Organizations gli account membri possono ora utilizzare una semplice procedura tramite AWS Identity and Access Management (IAM) per riottenere l'accesso ai bucket Amazon S3 bloccati accidentalmente. Per ulteriori informazioni, consulta [Eseguire un'attività privilegiata su un account AWS Organizations membro](#) nella Guida per l'utente. AWS Identity and Access Management

14 novembre 2024

[Le politiche di controllo delle risorse \(RCP\), un nuovo tipo di policy di autorizzazione, sono disponibili anche per i bucket Amazon S3 AWS Organizations](#)

Policy di controllo delle risorse (RCP), una nuova policy di autorizzazione gestita in AWS Organizations , può essere utilizzata per impostare le autorizzazioni massime disponibili sui bucket Amazon S3 all'interno dell'intera organizzazione. Per ulteriori informazioni, consulta [Policy di controllo delle risorse \(RCP\)](#) nella Guida per l'utente di AWS Organizations .

13 novembre 2024

[Amazon S3 ora approva automaticamente gli aumenti di quota dei bucket fino a 1.000 bucket](#)

Amazon S3 ora approva automaticamente gli aumenti di quota dei bucket fino a 1.000 bucket. Per visualizzare l'utilizzo del bucket o richiedere un aumento, visitare la [console Service Quotas](#).

30 settembre 2024

[Nuovo comportamento predefinito di transizione delle dimensioni minime degli oggetti per le configurazioni del ciclo di vita di Amazon S3](#)

Amazon S3 ora applica un comportamento predefinito alle configurazioni del ciclo di vita S3 che impedisce la transizione di oggetti di dimensioni inferiori a 128 KB a qualsiasi classe di storage. Per informazioni su come sostituire questo comportamento, consulta [Consentire la transizione di oggetti di dimensioni inferiori a 128 KB](#).

24 settembre 2024

[I bucket di directory ora supportano SSE-KMS l'utilizzo di chiavi gestite dal cliente.](#)

I bucket di directory ora supportano la crittografia lato server con AWS Key Management Service (AWS KMS) keys (SSE-KMS) utilizzando chiavi gestite dal cliente. Sono disponibili più opzioni per crittografare e gestire la sicurezza dei dati nei bucket di directory. Per ulteriori informazioni, consulta [Protezione e crittografia dei dati nei bucket di directory.](#)

17 settembre 2024

[S3 Access Grants supporta un'operazione API che elenca le concessioni di accesso del chiamante](#)

Le identità IAM e le identità delle directory aziendali del Centro identità IAM possono ora utilizzare l'API `ListCallerAccessGrants` per elencare tutti i bucket, i prefissi e gli oggetti di Amazon S3 a cui possono accedere, come definito da S3 Access Grants. Utilizzare questa API per scoprire tutti i dati S3 a cui un'identità IAM o di directory aziendale può accedere tramite S3 Access Grants all'interno di un determinato Account AWS. Per ulteriori informazioni, consulta [Elencare le concessioni di accesso del chiamante.](#)

5 settembre 2024

[Messaggi di errore di accesso negato migliorati per le richieste dello stesso account](#)

21 agosto 2024

Amazon S3 ora include un contesto aggiuntivo negli errori di accesso negato (HTTP 403 Forbidden) per le richieste effettuate alle risorse all'interno dello stesso Account AWS. Questo nuovo contesto include il tipo di policy che ha negato l'accesso, il motivo del rifiuto e le informazioni sull'utente o sul ruolo AWS Identity and Access Management (IAM) che ha richiesto l'accesso alla risorsa. Questo contesto consente di risolvere i problemi di accesso, identificare la causa principale degli errori di accesso negato e correggere i controlli di accesso errati aggiornando le policy pertinenti. Questo contesto aggiuntivo è disponibile anche nei AWS CloudTrail log. I messaggi di errore di accesso negato avanzato per le richieste relative allo stesso account sono ora disponibili in tutte le Regioni AWS, comprese le regioni cinesi AWS GovCloud (US) Regions e cinesi. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi agli errori di accesso negato \(403 Accesso negato\) in Amazon S3](#).

[Amazon S3 supporta l'utilizzo di scritture condizionali per PutObject e CompleteMultipartUpload](#)

È possibile verificare l'esistenza di un oggetto nel bucket prima di crearlo utilizzando una scrittura condizionale sulle operazioni di caricamento. In questo modo si può impedire la sovrascrittura di dati esistenti. Le scritture condizionali verificheranno che non esiste già alcun oggetto con lo stesso nome di chiave nel bucket. Per ulteriori informazioni, consulta [Richieste condizionali](#).

20 agosto 2024

[Amazon S3 non addebita più i costi per diversi codici di errore HTTP](#)

Amazon S3 ha completato una modifica per cui le richieste non autorizzate che i clienti non hanno avviato sono gratuite. Per ulteriori informazioni, consulta [Fatturazione delle risposte di errore di Amazon S3](#).

19 agosto 2024

[Amazon S3 Select non è più disponibile per i nuovi clienti](#)

Amazon S3 Select non è più disponibile per i nuovi clienti. I clienti esistenti di Amazon S3 Select possono continuare a utilizzare la funzionalità come di consueto. [Ulteriori informazioni](#).

25 luglio 2024

[Amazon S3 Inventory supporta la chiave di condizione s3: InventoryAccessibleOptionalFields](#)

Amazon S3 Inventory supporta la chiave s3: InventoryAccessibleOptionalFields condition per controllare se gli utenti possono includere campi di metadati opzionali nei loro report. Per ulteriori informazioni, consulta [Controllare la creazione della configurazione dei report di Inventario S3](#).

20 febbraio 2024

[Supporto IPv6 per S3 su Outposts](#)

Ora puoi accedere a S3 sui bucket Outposts utilizzando IPv6 tramite S3 sugli endpoint dual-stack di Outposts. Il [supporto IPv6 per S3 su Outposts](#) consente di gestire i bucket S3 su Outposts e le risorse del piano di controllo (control-plane) su reti IPv6.

16 gennaio 2024

[Nuova classe di archiviazione Amazon S3 a zona singola ad alte prestazioni: S3 Express One Zone](#)

Amazon S3 Express One Zone è una classe di archiviazione Amazon S3 a zona singola ad alte prestazioni, creata appositamente per fornire un accesso ai dati coerente di pochi millisecondi per le applicazioni sensibili alla latenza. Per ulteriori informazioni, consulta [S3 Express One Zone](#).

28 novembre 2023

[Mountpoint per Amazon S3 aggiunge il supporto per S3 Express One Zone](#)

Ora puoi montare i bucket di directory S3 Express One Zone con [Mountpoint](#).

28 novembre 2023

[Versione dello schema di invocazione Lambda](#)

Operazioni in batch Amazon S3 introduce una nuova versione dello schema di invocazione Lambda per l'utilizzo con processi Operazioni in batch che agiscono sui bucket di directory. Per ulteriori informazioni, consulta [Utilizzo di Lambda e Operazioni in batch Amazon S3 con bucket di directory](#).

28 novembre 2023

[Azione di importazione per bucket di directory](#)

Amazon S3 introduce l'azione di importazione. L'importazione è un metodo ottimizzato di creazione di processi Operazioni in batch Amazon S3 per copiare oggetti da bucket per uso generico in bucket di directory. Per ulteriori informazioni, consulta [Importing objects into a directory bucket](#).

28 novembre 2023

[Gestione dell'accesso a S3 con S3 Access Grants](#)

Amazon S3 Access Grants consente di gestire le autorizzazioni dei dati su larga scala per i principali AWS Identity and Access Management (IAM) oltre alle identità di directory presenti nelle directory aziendali come Azure AD. Ora puoi applicare le autorizzazioni S3 con privilegio minimo e dimensionare facilmente tali autorizzazioni in base alle esigenze aziendali. Per ulteriori informazioni, consulta [Managing access with S3 Access Grants](#).

26 novembre 2023

[Mountpoint per Amazon S3 aggiunge funzionalità di memorizzazione nella cache](#)

Con [Mountpoint](#), ora puoi configurare la memorizzazione nella cache per i dati con accesso ripetuto.

22 novembre 2023

[Generazione migliorata del manifesto Operazioni in batch Amazon S3](#)

Ora puoi configurare Operazioni in batch Amazon S3 per generare automaticamente un manifesto in base ai criteri di filtro degli oggetti specificati quando si crea il processo. Questa opzione è disponibile per i processi di replica in batch creati nella console Amazon S3 o per qualsiasi tipo di processo creato utilizzando gli SDK o l'API REST di Amazon S3. AWS CLI AWS Per ulteriori informazioni, consulta [Creazione di un processo di operazioni in batch S3](#).

22 novembre 2023

[I bucket Amazon S3 esistenti possono ora aggiungere configurazioni Object Lock](#)

Ora puoi abilitare Object Lock su un bucket S3 esistente. Puoi impostare blocchi a fini legali e periodi di conservazione per bucket nuovi o esistenti. Per ulteriori informazioni, consulta [Utilizzo del blocco oggetti S3](#).

20 novembre 2023

[Parametri delle richieste di S3 Storage Lens per i prefissi](#)

S3 Storage Lens introduce parametri delle richieste per i prefissi all'interno di un bucket Amazon S3. Per ulteriori informazioni, consulta [Categorie di parametri](#).

17 novembre 2023

[Gruppi Amazon S3 Storage Lens](#)

S3 Storage Lens introduce i gruppi Storage Lens, un filtro definito su misura per gli oggetti in base ai metadati di un oggetto. Per maggiori informazioni, consulta [Utilizzo di Amazon S3 Storage Lens con i gruppi](#).

15 novembre 2023

[Nuova policy IAM](#)

S3 su Outposts presenta `AWSServiceRoleForS3onOutposts`, un ruolo collegato ai servizi per aiutarti a gestire le risorse di rete. Per ulteriori informazioni, consulta [Using service-linked roles for Amazon S3 on Outposts](#).

3 ottobre 2023

[Amazon S3 fornisce l'orario Last-Modified per i contrassegni di eliminazione](#)

Amazon S3 fornisce l'orario Last-Modified per i contrassegni di eliminazione nelle intestazioni di risposta di S3 Head e delle operazioni API Get. Per ulteriori informazioni, consulta [Utilizzo dei contrassegni di eliminazione](#).

27 settembre 2023

[Aggiornamento di Amazon S3 alla policy gestita AWS](#)

Amazon S3 ha aggiunto le autorizzazioni `s3:Describe*` a `AmazonS3ReadOnlyAccess`. Per ulteriori informazioni, consulta [Policy gestite da AWS per Amazon S3](#).

11 agosto 2023

[Tempi di avvio migliorati per le richieste di ripristino Standard effettuate tramite Operazioni in batch Amazon S3](#)

I recuperi standard per le richieste di ripristino effettuate e tramite Operazioni in batch Amazon S3 ora possono iniziare in pochi minuti. Per ulteriori informazioni consulta [Opzioni di recupero dall'archivio](#).

9 agosto 2023

[È stato aggiunto Mountpoint, un client ad alta velocità di trasmissione effettiva per il montaggio di un bucket Amazon S3 come file system locale.](#)

Con [Mountpoint](#), le applicazioni possono accedere agli oggetti archiviati in Amazon S3 tramite operazioni sui file, dando alle applicazioni l'accesso all'archiviazione elastica e alla velocità di trasmissione effettiva di Amazon S3 tramite un'interfaccia di file.

9 agosto 2023

[Dual-layer crittografia lato server con AWS Key Management Service chiavi \(DSSE-KMS\)](#)

Dual-layer la crittografia lato server con AWS Key Management Service (AWS KMS) keys (DSSE-KMS) applica due livelli di crittografia agli oggetti quando vengono caricati su Amazon S3. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server a doppio livello con chiavi. AWS KMS](#)

13 giugno 2023

[Amazon S3 abilita il blocco dell'accesso pubblico S3 e disabilita le liste di controllo degli accessi \(ACL\) di S3 per tutti i nuovi bucket.](#)

Amazon S3 ora abilita automaticamente S3 Block Public Access e disabilita gli elenchi di controllo degli accessi (ACL) S3 per tutti i nuovi bucket S3 in tutte le regioni. AWS Per ulteriori informazioni, consulta [Blocco dell'accesso pubblico allo storage Amazon S3 e Controllo della proprietà degli oggetti e disabilitazione delle ACL per il bucket.](#)

27 aprile 2023

[Metrica delle operazioni di Replica Amazon S3 non riuscite](#)

Amazon S3 aggiunge una nuova metrica per monitorare e gli errori di replica S3. Amazon CloudWatch Per ulteriori informazioni, consulta [Monitoraggio dell'avanzamento con i parametri di replica.](#)

5 aprile 2023

[DNS privato](#)

AWS PrivateLink per Amazon S3 ora supporta il DNS privato. Per ulteriori informazioni, consultare [DNS privato.](#)

14 marzo 2023

[Cross-account supporto per i punti di accesso nella console Amazon S3](#)

Amazon S3 ora supporta la creazione di punti di accesso multi-account nella propria console. Per ulteriori informazioni, consulta [Creazione dei punti di accesso.](#)

14 marzo 2023

[Amazon S3 su Outposts supporta Replica Amazon S3 su Outposts](#)

Con la replica S3 locale, puoi replicare automaticamente gli oggetti in un singolo bucket Outposts di destinazione o in più bucket di destinazione. I bucket di destinazione possono trovarsi in diversi AWS Outposts o all'interno degli stessi avamposti del bucket di origine. Per ulteriori informazioni, consulta la pagina relativa alla [replica di oggetti per S3 su Outposts](#).

14 marzo 2023

[Alias del punto di accesso Lambda per oggetti Amazon S3](#)

Quando crei un punto di accesso Lambda per oggetti, Amazon S3 genera automaticamente un alias univoco per il tuo punto di accesso Lambda per oggetti. Puoi utilizzare questo alias del punto di accesso al posto di un nome del bucket Amazon S3 o del nome della risorsa Amazon (ARN) del punto di accesso Lambda per oggetti in una richiesta per qualsiasi operazione del piano dati del punto di accesso. Per ulteriori informazioni, consulta la pagina relativa a [come utilizzare un alias in stile bucket per il punto di accesso Lambda per oggetti](#).

14 marzo 2023

[Supporto per più account per
Amazon S3 Access Points
Multi-Region](#)

Amazon S3 ora supporta la creazione di Multi-Region access point su più account con la console Amazon S3. Per ulteriori informazioni, consulta [Creazione Multi-Region di punti di accesso](#).

14 marzo 2023

[Cross-account punti di
accesso](#)

Amazon S3 supporta la creazione di punti di accesso multi-account. È possibile creare un punto di accesso multi-account utilizzando la AWS Command Line Interface (AWS CLI) o l'operazione CreateAccessPoint della REST API. Per ulteriori informazioni, consulta [Creazione dei punti di accesso](#).

30 novembre 2022

[Amazon S3 supporta i controlli di failover per i punti di accesso Amazon Multi-Region S3](#)

Amazon S3 introduce il controllo del failover per gli access point. Multi-Region Questi controlli consentono di trasferire il traffico delle richieste di accesso ai dati S3 indirizzato attraverso un punto di Multi-Region accesso Amazon S3 a un altro in Regione AWS pochi minuti per testare e creare applicazioni ad alta disponibilità. Per ulteriori informazioni, consulta i controlli di failover degli Access Point di [Amazon S3 Multi-Region](#).

28 novembre 2022

[Amazon S3 Storage Lens aumenta la visibilità a livello di organizzazione con 34 nuovi parametri](#)

S3 Storage Lens introduce altri 34 parametri per individuare migliori opportunità di ottimizzazione dei costi, identificare le best practice per la protezione dei dati e migliorare le prestazioni dei flussi di lavoro delle applicazioni. Per ulteriori informazioni, consulta la sezione [Parametri di S3 Storage Lens](#).

17 novembre 2022

[Amazon S3 supporta richieste di ripristino a velocità più elevate per le classi di archiviazione S3 Glacier Flexible Retrieval \(Recupero flessibile S3 Glacier\) e S3 Glacier Deep Archive \(Archiviazione profonda S3 Glacier\)](#)

Amazon S3 supporta richieste di ripristino a una velocità massima di 1.000 transazioni al secondo, Account AWS per le classi di storage S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

15 novembre 2022

[Amazon S3 su Outposts supporta azioni e filtri del ciclo di vita S3 aggiuntivi](#)

S3 su Outposts supporta regole aggiuntive del ciclo di vita S3 per ottimizzare la gestione della capacità. È possibile far scadere gli oggetti man mano che invecchiano o vengono sostituiti da versioni più recenti. È possibile creare una regola del ciclo di vita per un intero bucket o un sottoinsieme di oggetti in un bucket filtrando per prefissi, tag di oggetto o dimensione di oggetto. Per ulteriori informazioni, consulta [Creazione e gestione di una configurazione del ciclo di vita](#).

2 novembre 2022

[SSE-C Supporto per la replica S3 per oggetti](#)

È possibile replicare gli oggetti creati con crittografia lato server mediante chiavi fornite dal cliente. Per ulteriori informazioni sulla replica di oggetti crittografati, vedere [Replicazione di oggetti creati con crittografia lato server \(,,\).](#) [SSE-C SSE-S3 SSE-KMS](#)

24 ottobre 2022

[Amazon S3 su Outposts supporta gli alias del punto di accesso](#)

Con S3 su Outposts devi utilizzare i punti di accesso per accedere a qualsiasi oggetto in un bucket Outposts. Ogni volta che crei un punto di accesso per un bucket, S3 su Outposts genera automaticamente un alias per tale punto di accesso. Puoi utilizzare questo alias del punto di accesso al posto dell'ARN del punto di accesso per qualsiasi operazione del piano dati. Per ulteriori informazioni, consulta [Using a bucket-style alias for your S3 on Outposts bucket access point](#) (Utilizzo di un alias in stile bucket per il punto di accesso del bucket S3 su Outposts).

21 ottobre 2022

[S3 Object Lambda supporta le operazioni HeadObject , ListObjects e ListObjectsV2](#)

Puoi utilizzare il codice personalizzato per modificare e i dati restituiti dalle richieste S3 standard GET, LIST o HEAD per filtrare le righe, ridimensionare le immagini in modo dinamico, oscurare i dati riservati e molto altro. Per ulteriori informazioni, consulta [Trasformazione di oggetti con S3 Object Lambda](#).

4 ottobre 2022

[Amazon S3 su Outposts supporta il controllo delle versioni S3](#)

Se abilitato, il controllo delle versioni S3 conserva più copie distinte di un oggetto nello stesso bucket. Puoi utilizzarlo e il controllo delle versioni S3 per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nei bucket Outposts. Il controllo delle versioni S3 ti consente di eseguire il ripristino a seguito di errori dell'applicazione e operazioni non intenzionali degli utenti. Per ulteriori informazioni, consulta [Managing S3 Versioning for your S3 on Outposts bucket](#) (Gestione del controllo delle versioni S3 per un bucket S3 su Outposts).

21 settembre 2022

[AWS Backup per Amazon S3](#)

AWS Backup è un servizio completamente gestito e basato su policy che puoi utilizzare per definire una politica di backup centrale per proteggere i tuoi dati Amazon S3. Per ulteriori informazioni, consulta [Using AWS Backup for Amazon S3](#).

18 febbraio 2022

[Utilizzo di S3 Batch Replication per replicare gli oggetti esistenti](#)

S3 Batch Replication ti consente di replicare gli oggetti che esistevano già prima della configurazione della replica. La replica degli oggetti esistenti avviene tramite l'uso di un processo di operazioni in batch. S3 Batch Replication differisce dalla replica in tempo reale, che copia in modo continuo e automatico nuovi oggetti tra bucket Amazon S3. Per ulteriori informazioni, consulta la sezione [Replica di oggetti esistenti con S3 Batch Replication](#).

8 febbraio 2022

[Rinominazione di S3 Glacier Flexible Retrieval](#)

La classe di archiviazione Glacier è stata rinominata S3 Glacier Flexible Retrieval. Questa modifica non ha alcun impatto sull'API.

30 novembre 2021

[Nuova impostazione di S3 Object Ownership per disabilitare le ACL](#)

Puoi applicare l'impostazione del proprietario del bucket per Object Ownership (Proprietà dell'oggetto) per disabilitare le liste di controllo degli accessi per il tuo bucket e gli oggetti contenuti e assumere la proprietà di ogni oggetto del tuo bucket. L'impostazione applicata del proprietario del bucket semplifica la gestione degli accessi per i dati archiviati in Amazon S3. Per ulteriori informazioni, consulta [Controllo della proprietà degli oggetti e disabilitazione delle ACL per il bucket](#).

30 novembre 2021

[Nuova classe di storage S3 Intelligent-Tiering](#)

S3 Intelligent-Tiering Archive Instant Access è una classe di archiviazione aggiuntiva in S3. Intelligent-Tiering Per ulteriori informazioni, vedi [Come funziona Intelligent-Tiering S3](#).

30 novembre 2021

[Nuova classe di archiviazione S3 Glacier Instant Retrieval](#)

Ora è possibile posizionare gli oggetti nella classe di archiviazione S3 Glacier Instant Retrieval. Per maggiori informazioni su questa classe di archiviazione, consulta [Utilizzare le classi di archiviazione di Amazon S3](#).

30 novembre 2021

[AWS Backup per Amazon S3 Preview](#)

AWS Backup è un servizio completamente gestito e basato su policy che puoi utilizzare per definire una politica di backup centrale per proteggere i tuoi dati Amazon S3. Per ulteriori informazioni, consulta [Using AWS Backup for Amazon S3](#).

30 novembre 2021

[AWS Identity and Access Management Access Analyzer per Amazon S3](#)

IAM Access Analyzer esegue controlli della policy per convalidarla in rapporto alla sintassi della policy e alle best practice di IAM. Per ulteriori informazioni sulla convalida delle policy con IAM Access Analyzer, consulta [Convalida delle policy di IAM Access Analyzer](#) nella Guida per l'utente di IAM.

30 novembre 2021

[Nuovi tipi di eventi](#)

Nuovi tipi di eventi aggiunti alle notifiche di eventi di Amazon S3, consulta [Notifiche di eventi Amazon S3](#).

29 novembre 2021

[Abilita Amazon EventBridge on buckets](#)

Puoi abilitare EventBridge sui bucket Amazon S3 l'invio di eventi ad Amazon EventBridge, vedi Utilizzo. [EventBridge](#)

29 novembre 2021

[Nuovi filtri del Ciclo di vita S3](#)

È possibile creare regole del ciclo di vita in base alle dimensioni dell'oggetto o specificare il numero di versioni non correnti dell'oggetto da conservare. Per ulteriori informazioni, consulta [Esempi di configurazione del ciclo di vita S3](#).

23 novembre 2021

[Pubblica le metriche di Amazon S3 Storage Lens su Amazon CloudWatch](#)

Puoi pubblicare le metriche di utilizzo e attività di S3 Storage Lens su Amazon per CloudWatch creare una visione unificata dello stato operativo in dashboard. CloudWatch Puoi anche utilizzare CloudWatch funzionalità, come allarmi e azioni attivate, calcoli matematici e rilevamento delle anomalie, per monitorare e intervenire sulle metriche di S3 Storage Lens. Inoltre, le CloudWatch API consentono alle applicazioni, compresi i provider di terze parti, di accedere alle metriche di S3 Storage Lens. Per ulteriori informazioni, consulta le metriche di [Monitor S3 Storage Lens in. CloudWatch](#)

22 novembre 2021

[Multi-Region Access point](#)

2 settembre 2021

Puoi utilizzare gli Multi-Region Access Points per creare un endpoint globale che le applicazioni possano utilizzare e per soddisfare le richieste provenienti da bucket Amazon S3 dislocati in più bucket. Regioni AWS Puoi utilizzare questo Multi-Region Access Point per indirizzare i dati a un bucket con la latenza più bassa. Per ulteriori informazioni sugli Multi-Region Access Point e su come utilizzarli, consulta [Multi-Region Access Point in Amazon S3](#).

[Amazon S3 su Outposts aggiunge l'accesso locale diretto per le applicazioni](#)

Esegui le tue applicazioni all'esterno del cloud privato AWS Outposts virtuale (VPC) e accedi ai dati di S3 on Outposts. È inoltre possibile accedere agli oggetti S3 su Outposts direttamente dalla rete on-premise. Per ulteriori informazioni sulla configurazione di S3 on Outposts utilizzando indirizzi IP (CoIP) di [proprietà del cliente](#) e sull'accesso agli oggetti creando un gateway <https://docs.aws.amazon.com/outposts/latest/userguide/outposts-networking-components.html> locale dalla rete locale, consulta [Accedere ad Amazon S3 on Outposts utilizzando punti di accesso. VPC-only](#)

29 luglio 2021

[Alias del punto di accesso Amazon S3](#)

Quando crei un punto di accesso, Amazon S3 genera automaticamente un alias che puoi utilizzare al posto del nome del bucket per l'accesso ai dati. Puoi utilizzare questo alias del punto di accesso al posto di un Amazon Resource Name (ARN) per qualsiasi operazione del piano dati del punto di accesso. Per ulteriori informazioni, consulta [Utilizzo di un alias in stile bucket per il punto di accesso.](#)

26 luglio 2021

[Amazon S3 Inventory e Operazioni in batch Amazon S3 supportano lo stato della chiave del bucket S3](#)

Le operazioni di inventario e in batch di Amazon S3 supportano l'identificazione e la copia di oggetti esistenti con le chiavi bucket S3. Le chiavi bucket S3 accelerano la riduzione dei costi di crittografia lato server per gli oggetti esistenti. Per ulteriori informazioni, consulta [Inventario Amazon S3e Oggetto Copia per operazioni in batch.](#)

3 giugno 2021

[Snapshot dell'account con i parametri di Amazon S3 Storage Lens](#)

Lo snapshot dell'account S3 Storage Lens mostra l'archiviazione totale, il numero di oggetti e la dimensione e media degli oggetti nella pagina Home della console S3 (Bucket) riepilogando i parametri della dashboard predefinita. Per ulteriori informazioni, consultare lo [snapshot dell'account dei parametri di S3 Storage Lens.](#)

5 maggio 2021

[Aumento del supporto per endpoint Amazon S3 su Outposts](#)

S3 su Outposts supporta ora fino a 100 endpoint per Outpost. Per ulteriori informazioni, vedere [Limitazioni di rete di S3 su Outposts.](#)

29 aprile 2021

[Notifiche di CloudWatch eventi](#)
[Amazon S3 on Outposts in](#)
[Amazon Events](#)

Puoi utilizzare CloudWatch Events per creare una regola per acquisire qualsiasi evento dell'API S3 on Outposts e ricevere notifiche tramite tutti i target supportati. CloudWatch Per ulteriori informazioni, consulta [Ricezione di notifiche di eventi S3 on Outposts tramite Events. CloudWatch](#)

19 aprile 2021

[S3 Object Lambda](#)

Con S3 Object Lambda puoi aggiungere il tuo codice alle richieste GET di Amazon S3 per modificare ed elaborare i dati quando vengono restituiti a un'applicazione. Puoi utilizzare il codice personalizzato per modificare i dati restituiti dalle richieste GET S3 standard per filtrare le righe, ridimensionare le immagini in modo dinamico, oscurare i dati riservati e molto altro. Per ulteriori informazioni, consulta [Trasformazione di oggetti](#).

18 marzo 2021

[AWS PrivateLink](#)

Con AWS PrivateLink Amazon S3, puoi connetterti direttamente a S3 utilizzando un endpoint di interfaccia nel tuo cloud privato virtuale (VPC) invece di connetterti tramite Internet. Gli endpoint di interfaccia sono direttamente accessibili dalle applicazioni che si trovano on-premise o in una Regione AWS diversa. Per ulteriori dettagli, consulta [AWS PrivateLink per Amazon S3](#).

2 febbraio 2021

[Gestione della capacità di Amazon S3 on Outposts con AWS CloudTrail](#)

Gli eventi di gestione di S3 on Outposts sono disponibili tramite log. CloudTrail Per ulteriori informazioni, consulta [Gestire la capacità di S3 on Outposts con. CloudTrail](#)

21 dicembre 2020

Forte coerenza

1 dicembre 2020

Amazon S3 fornisce una coerenza di lettura dopo scrittura per le operazioni PUT e DELETE per gli oggetti nel tuo bucket Amazon S3 in tutte le Regioni AWS. Inoltre, le operazioni di lettura su Amazon S3 Select, le liste di controllo degli accessi Amazon S3, i tag di oggetti Amazon S3 e i metadati di oggetti (ad esempio l'oggetto HEAD) sono fortemente consistenti. Per maggiori informazioni, consulta il [modello di consistenza dei dati di Amazon S3](#).

[Sincronizzazione delle modifiche alla replica di Amazon S3](#)

La sincronizzazione delle modifiche alla replica di Amazon S3 mantiene sincronizzati i metadati degli oggetti come tag, ACL e le impostazioni di blocco oggetti tra gli oggetti di origine e le repliche. Quando questa funzione è abilitata, Amazon S3 replica le modifiche ai metadati apportate all'oggetto di origine o alle copie di replica. Per ulteriori informazioni, consulta [Replicating metadata changes with replica modification sync](#) (Replica delle modifiche ai metadati con sincronizzazione delle modifiche alla replica).

1 dicembre 2020

[Chiavi bucket Amazon S3](#)

Amazon S3 Bucket Keys riduce il costo della crittografia lato server di Amazon S3 con (). AWS Key Management Service SSE-KMS Questa nuova chiave a livello di bucket per la crittografia lato server può diminuire i costi delle richieste di AWS KMS fino al 99% riducendo il traffico delle richieste da Amazon S3 a AWS KMS. Per ulteriori informazioni, consulta [Ridurre i costi utilizzando S3 Bucket SSE-KMS Keys](#).

1 dicembre 2020

[Amazon S3 Storage Lens](#)

18 novembre 2020

S3 Storage Lens aggrega i tuoi parametri e mostra le informazioni nella sezione Account snapshot (Snapshot dell'account) nella pagina Buckets (Bucket) della console Amazon S3. S3 Storage Lens fornisce anche una dashboard interattiva che puoi utilizzare per visualizzare informazioni e tendenze, segnalare valori anomali e ricevere consigli per ottimizzare i costi di storage e applicare le migliori pratiche di protezione dei dati. La dashboard offre opzioni di approfondimento per generare e visualizzare informazioni dettagliate a livello di organizzazione, account, classe di archiviazione, bucket Regione AWS, prefisso o gruppo Storage Lens. Puoi anche inviare un rapporto giornaliero sulle metriche in Parquet formato CSV o a un bucket S3 generico o esportare le metriche direttamente in un bucket di tabelle S3 gestito.

AWS Per ulteriori informazioni, consulta [Valutazione dell'attività e dell'utilizzo dello storage con S3 Storage Lens](#).

[Tracciamento delle richieste S3 utilizzando AWS X-Ray](#)

Amazon S3 si integra X-Ray per propagare il contesto di [traccia](#) e fornire una catena di richieste con nodi [upstream e downstream](#). Per ulteriori informazioni, consulta [Tracciare le richieste utilizzando X-Ray](#).

16 Novembre 2020

[Parametri di replica S3](#)

I parametri di replica S3 forniscono parametri dettagliati per le regole nella configurazione di replica. Per maggiori informazioni, consulta [Replication metrics and Amazon S3 event notifications](#) (Parametri di replica e notifiche di eventi Amazon S3).

9 novembre 2020

[S3 Intelligent-Tiering Archive Access e Deep Archive Access](#)

S3 Intelligent-Tiering Archive Access e Deep Archive Access sono livelli di storage aggiuntivi in S3. Intelligent-Tiering Per ulteriori informazioni, consulta [La classe di storage che ottimizza automaticamente gli oggetti con accesso più o meno frequente](#).

9 novembre 2020

[Replica del contrassegno di eliminazione](#)

Con la replica del contrassegno di eliminazione è possibile garantire che i contrassegni di eliminazione vengano copiati nei bucket di destinazione per le regole di replica. Per ulteriori informazioni, consulta [Utilizzo della replica dei contrassegni di eliminazione](#).

9 novembre 2020

[S3 Object Ownership](#)

Object Ownership è un'impostazione del bucket S3 che è possibile utilizzare per controllare la proprietà dei nuovi oggetti che vengono caricati nei bucket. Per ulteriori informazioni, consulta [Utilizzo di S3 Object Ownership](#).

2 ottobre 2020

[Amazon S3 su Outposts](#)

Con Amazon S3 on Outposts, puoi creare bucket S3 sulle tue AWS Outposts risorse e archiviare e recuperare facilmente oggetti in locale per applicazioni che richiedono o accesso locale ai dati, elaborazione locale dei dati e residenza dei dati. Puoi utilizzare S3 su Outposts tramite, SDK o API REST. Console di gestione AWS AWS CLI AWS Per ulteriori informazioni, consulta [Utilizzo di Amazon S3 su Outposts](#).

30 settembre 2020

[Condizione proprietario del bucket](#)

Puoi utilizzare la condizione di proprietario del bucket Amazon S3 per assicurarti che i bucket utilizzati nelle tue operazioni S3 appartengano a quelli previsti. Account AWS Per ulteriori informazioni, consulta [Condizione del proprietario del bucket](#).

11 settembre 2020

[Supporto di S3 Batch Operations per Object Lock Retention](#)

È ora possibile utilizzare le operazioni in batch con il blocco oggetti S3 per applicare le impostazioni di conservazione a molti oggetti Amazon S3 contemporaneamente. Per ulteriori informazioni, consulta [Setting S3 Object Lock Retention dates with S3 Batch Operations](#) (Gestione delle date di conservazione del blocco oggetti S3 con Operazioni di batch S3).

4 maggio 2020

[Supporto delle operazioni in batch S3 per il blocco di carattere legale del blocco oggetti](#)

Puoi utilizzare Operazioni di batch con il blocco oggetti S3 per aggiungere blocchi di carattere legale a molti oggetti Amazon S3 contemporaneamente. Per ulteriori informazioni, consulta [Utilizzo di S3 Batch Operations per impostare il blocco di carattere legale del blocco oggetti S3](#).

4 maggio 2020

[Tag dei processi per Operazioni di batch S3](#)

È possibile aggiungere tag ai processi di operazioni in batch Amazon S3 per controllare ed etichettare tali processi. Per ulteriori informazioni, consulta [Tags for S3 Batch Operations jobs](#) (Tag dei processi per Operazioni di batch S3).

16 marzo 2020

[Access point Amazon S3](#)

I punti di accesso Amazon S3 semplificano la gestione dell'accesso ai dati su vasta scala per set di dati condivisi in S3. Gli access point sono endpoint di rete denominati che vengono collegati a bucket che puoi usare per eseguire operazioni su oggetti S3. Per ulteriori informazioni, consulta [Gestione dell'accesso ai dati con access point Amazon S3](#).

2 dicembre 2019

[Access Analyzer per Amazon S3](#)

Access Analyzer for Amazon S3 ti avvisa dei bucket S3 configurati per consentire l'accesso a chiunque su Internet o altro Account AWS, compresi gli account esterni alla tua organizzazione. Per ulteriori informazioni, consulta [Utilizzo di Access Analyzer per Amazon S3](#).

2 dicembre 2019

S3 Replication Time Control (S3 RTC)

S3 Replication Time Control (S3 RTC) replica la maggior parte degli oggetti caricati in Amazon S3 in pochi secondi, arrivando al 99,99% di tali oggetti in 15 minuti. Per ulteriori informazioni, consulta [Replicating objects using S3 Replication Time Control \(S3 RTC\)](#) (Replica di oggetti utilizzando il controllo del tempo di replica di S3 (S3 RTC)).

20 novembre 2019

Same-Region Replica

Puoi utilizzare Same-Region Replication (SRR) per copiare oggetti tra bucket Amazon S3 nello stesso. Regione AWS Per informazioni su Cross-Region Replication (CRR) e Replication, consulta Replication. Same-Region <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html>

18 settembre 2019

Cross-Region Supporto per la replica per S3 Object Lock

Cross-Region La replica ora supporta Object Lock. Per ulteriori informazioni, consulta [Cosa replica Amazon S3?](#)

28 maggio 2019

[Operazioni in batch S3](#)

Utilizzando Operazioni di batch S3 è possibile eseguire le operazioni in batch su vasta scala su oggetti Amazon S3. Le operazioni in batch S3 possono eseguire una singola operazione su elenchi di oggetti specificati. Un solo processo può eseguire l'operazione specificata su miliardi di oggetti contenenti exabyte di dati. Per ulteriori informazioni, consulta [Esecuzione di S3 Batch Operations](#).

30 Aprile 2019

[Regione Asia Pacifico \(Hong Kong\)](#)

Amazon S3 è ora disponibile nella regione Asia Pacifico (Hong Kong). Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a [regioni ed endpoint](#) nella Riferimenti generali di AWS.

24 aprile 2019

[Aggiunto un nuovo campo ai log di accesso al server](#)

In Amazon S3 è stato aggiunto il seguente nuovo campo ai log di accesso al server: Transport Layer Security (TLS) version (Versione di Transport Layer Security (TLS)). Per ulteriori informazioni, consulta [Formato del log di accesso al server](#).

28 marzo 2019

[Nuova classe di storage per l'archiviazione](#)

Amazon S3 offre ora una nuova classe di archiviazione per gli oggetti con accesso non frequente: Deep Archive S3 Glacier (DEEP_ARCHIVE). Per ulteriori informazioni, consulta [Classi di storage](#).

27 marzo 2019

[Aggiunti nuovi campi ai log di accesso al server](#)

In Amazon S3 sono stati aggiunti i seguenti nuovi campi ai log di accesso al server: Host Id (ID host), Signature Version (Versione firma), Cipher Suite (Pacchetto di crittografia), Authentication Type (Tipo di autenticazione) e Host Header (Intestazione host). Per ulteriori informazioni, consulta [Formato del log di accesso al server](#).

5 marzo 2019

[Supporto per i file di Parquet-formatted inventario Amazon S3](#)

Amazon S3 supporta ora il formato [Apache Parquet \(Parquet\)](#) in aggiunta ai formati di file [Apache ORC \(Optimize d Row Columnar\)](#) e CSV (Comma-Separated Values, valori separati da virgole) per i file di output di inventario. Per ulteriori informazioni, consulta [Inventario](#).

4 dicembre 2018

[Blocco di oggetti in S3](#)

Amazon S3 offre ora una funzionalità di blocco oggetti che fornisce la protezione WORM (Write Once Read Many) per gli oggetti Amazon S3. Per ulteriori informazioni, consulta [Blocco degli oggetti](#).

26 Novembre 2018

[Aggiornamento della velocità di ripristino](#)

Tramite l'aggiornamento della velocità di ripristino in Amazon S3 è possibile modificare la velocità di un'operazione di ripristino dalla classe di archiviazione S3 Glacier Flexible Retrieval (Recupero flessibile S3 Glacier) aumentandola mentre il ripristino è in corso. Per ulteriori informazioni, consulta [Ripristino di oggetti archiviati](#).

26 Novembre 2018

[Notifiche di eventi di ripristino](#)

La funzionalità di notifica eventi di Amazon S3 ora supporta eventi di avvio e completamento durante il ripristino di oggetti dalla classe di archiviazione S3 Glacier Flexible Retrieval (Recupero flessibile S3 Glacier). Per ulteriori informazioni, consulta [Notifiche di eventi](#).

26 novembre 2018

[PUT direttamente nella classe
di archiviazione recupero
flessibile S3 Glacier](#)

L'operazione PUT in Amazon S3 permette ora di specificare il recupero flessibile S3 Glacier come classe di archiviazione quando si creano oggetti. Nelle versioni precedenti era necessario eseguire la transizione degli oggetti nella classe di archiviazione S3 Glacier Flexible Retrieval da un'altra classe di archiviazione Amazon S3. Inoltre, quando si utilizza S3 Cross-Region Replication (CRR), è ora possibile specificare S3 Glacier Flexible Retrieval come classe di storage per gli oggetti replicati. Per ulteriori informazioni sulla classe di archiviazione S3 Glacier Flexible Retrieval, consulta [Classi di archiviazione](#). Per ulteriori informazioni su come specificare la classe di storage per gli oggetti replicati, consulta [Panoramica della configurazione di replica](#). Per ulteriori informazioni sulle modifiche apportate dall'operazione PUT diretta alla REST API nel recupero flessibile S3 Glacier, consulta [Document History: PUT directly to S3 Glacier Flexible Retrieval](#) (Cronologia dei documenti:

26 novembre 2018

PUT direttamente nel recupero flessibile S3 Glacier).

[Nuova classe di storage](#)

Amazon S3 offre ora una nuova classe di storage denominata S3 Intelligent-Tiering (INTELLIGENT_TIERING) progettata per dati di lunga durata con modelli di accesso mutevoli o sconosciuti. Per ulteriori informazioni, consulta [Classi di storage](#).

26 Novembre 2018

[Blocco dell'accesso pubblico di Amazon S3](#)

Amazon S3 permette ora di bloccare l'accesso pubblico a bucket e oggetti a livello di singolo bucket o di account. Per ulteriori informazioni, consulta [Utilizzo del blocco dell'accesso pubblico di Amazon S3](#).

15 Novembre 2018

[Miglioramenti del filtraggio nelle Cross-Region regole di replica \(CRR\)](#)

Nella configurazione di una regola di replica tra regioni puoi specificare un filtro di oggetti per scegliere un sottoinsieme di oggetti cui applicare la regola. Nelle versioni precedenti era possibile filtrare solo in base a un prefisso della chiave di un oggetto. In questa versione puoi filtrare in base al prefisso della chiave di un oggetto, a uno o più tag dell'oggetto o a entrambe le condizioni. Per ulteriori informazioni, consulta [Configurazione di CRR: panoramica della configurazione di replica](#).

19 settembre 2018

[Nuove caratteristiche di Amazon S3 Select](#)

Amazon S3 Select ora supporta l'input di Apache Parquet, le query su oggetti JSON annidati e due nuove metriche di monitoraggio Amazon (e). CloudWatch SelectScannedBytes SelectReturnedBytes

5 settembre 2018

[Aggiornamenti ora disponibili tramite RSS](#)

È ora possibile abbonarsi a un feed RSS per ricevere notifiche sugli aggiornamenti alla Guida per l'utente di Amazon S3.

19 giugno 2018

Aggiornamenti precedenti

La tabella seguente descrive le modifiche importanti introdotte in ogni versione della Guida per l'utente di Amazon S3 prima del 19 giugno 2018.

Modifica	Descrizione	Data
Aggiornamento degli esempi di codice	<p>Esempi di codice aggiornati:</p> <ul style="list-style-type: none"> • C# – Aggiornamento di tutti gli esempi per l'utilizzo del modello asincrono basato su attività. Per ulteriori informazioni, consulta Amazon Web Services Asynchronous APIs for .NET nella Developer Guide. AWS SDK per .NET Gli esempi di codice sono ora conformi alla versione 3 di AWS SDK per .NET. • Java – Aggiornamento di tutti gli esempi per utilizzare il modello del generatore client. Per ulteriori informazioni sul modello del generatore client, consulta Creazione di client del servizio. • PHP: tutti gli esempi sono stati aggiornati per utilizzare AWS SDK per PHP 3.0. Per ulteriori informazioni sulla versione 3.0, consulta. AWS SDK per PHP AWS SDK per PHP • Ruby: codice di esempio aggiornato in modo che gli esempi funzionino con la AWS SDK per Ruby versione 3. 	30 Aprile 2018
Amazon S3 ora riporta le classi di storage S3 Glacier Flexible Retrieval e alle metriche di storage di Amazon	<p>Oltre a fare riferimento a byte effettivi, i parametri di archiviazione includono byte in sovraccarico per oggetto per le classi di archiviazione applicabili (ONEZONE_IA , STANDARD_IA e S3 Glacier Flexible Retrieval [Recupero flessibile S3 Glacier]):</p> <ul style="list-style-type: none"> • 	30 Aprile 2018

Modifica	Descrizione	Data
Logs ONEZONE_IA CloudWatch	<p>Per gli oggetti delle classi di storage ONEZONE_IA e STANDARD_IA, Amazon S3 segnala gli oggetti con dimensioni inferiori a 128 KB come 128 KB. Per ulteriori informazioni, consulta Comprensione e gestione delle classi di storage Amazon S3.</p> <ul style="list-style-type: none"> Per gli oggetti della classe di archiviazione S3 Glacier Flexible Retrieval, i parametri di archiviazione segnalano i seguenti sovraccarichi: <ul style="list-style-type: none"> Un sovraccarico di 32 KB per oggetto, addebitato in base ai prezzi della classe di archiviazione S3 Glacier Flexible Retrieval Un sovraccarico di 8 KB per oggetto, addebitato o secondo le tariffe della classe di archiviazione STANDARD <p>Per ulteriori informazioni, consulta Trasferimento degli oggetti utilizzando il ciclo di vita Amazon S3.</p> <p>Per ulteriori informazioni sui parametri dello storage, consulta Metriche di monitoraggio con Amazon CloudWatch.</p>	
Nuova classe di storage	<p>Amazon S3 offre ora una nuova classe di archiviazione, STANDARD_IA (IA sta per "Infrequent Access", accesso infrequente) per archiviare gli oggetti. Questa classe di storage è ottimizzata per i dati esistenti da molto tempo a cui si accede meno frequentemente. Per ulteriori informazioni, consulta Comprensione e gestione delle classi di storage Amazon S3.</p>	4 Aprile 2018

Modifica	Descrizione	Data
Amazon S3 Select	a>Amazon S3 supporta ora il recupero del contenuto degli oggetti in base a un'espressione SQL. Per ulteriori informazioni, consulta Interrogazione dei dati in loco con Amazon S3 Select .	4 aprile 2018
Osaka-Local Regione Asia Pacifico ()	<p>Amazon S3 è ora disponibile nella regione Asia Pacifico (Osaka-Local). Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a regioni ed endpoint nella Riferimenti generali di AWS.</p> <div>  Important <p>Puoi utilizzare la regione Asia Pacifico (Osaka-Local) solo insieme alla regione Asia Pacifico (Tokyo). Per richiedere l'accesso alla regione Asia Pacifico (Osaka-Local), contatta il tuo rappresentante commerciale.</p> </div>	12 febbraio 2018
Timestamp di creazione di Amazon S3 Inventory	Amazon S3 Inventory include ora un timestamp che indica la data e l'ora di inizio della creazione del report di Inventari o Amazon S3. È possibile utilizzare il timestamp per determinare le modifiche nello storage Amazon S3 dall'ora di inizio della generazione del report di inventario.	16 gennaio 2018
Regione Europa (Parigi)	Amazon S3 è ora disponibile nella regione UE (Parigi). Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a regioni ed endpoint nella Riferimenti generali di AWS.	18 dicembre 2017
Regione Cina (Ningxia)	Amazon S3 è ora disponibile nella regione Cina (Ningxia) . Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a regioni ed endpoint nella Riferimenti generali di AWS.	29 novembre 2017

Modifica	Descrizione	Data
Supporto per i file di inventario di ORC-formatted Amazon S3	Amazon S3 supporta ora il formato Apache ORC (Optimize d Row Columnar) in aggiunta al formato di file CSV (Comma-Separated Values, valori separati da virgole) per i file di output di inventario. È inoltre possibile eseguire query sull'inventario Amazon S3 utilizzando SQL standard con Amazon Athena, Amazon Redshift Spectrum e altri strumenti, tra cui Presto , Apache Hive e Apache Spark . Per ulteriori informazioni, consulta Catalogazione e analisi dei dati con Inventario S3 .	17 Novembre 2017
Crittografia predefinita per i bucket S3	La crittografia predefinita di Amazon S3 offre un modo per impostare il comportamento di crittografia predefinito di un bucket S3. Puoi configurare la crittografia predefinita di un bucket in modo che gli oggetti siano crittografati quando vengono memorizzati nel bucket. Gli oggetti sono crittografati utilizzando la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3) o chiavi AWS gestite (). SSE-KMS Per ulteriori informazioni, consulta Impostazione del comportamento predefinito della crittografia lato server per i bucket Amazon S3 .	06 Novembre 2017
Stato della crittografia in Amazon S3 Inventory	Amazon S3 supporta ora l'inserimento dello stato della crittografia in Amazon S3 Inventory per verificare come sono crittografati gli oggetti quando sono inattivi, per il controllo della conformità o per altri scopi. Puoi anche configurare per crittografare Amazon S3 Inventory con crittografia lato server (SSE) o in SSE-KMS modo che tutti i file di inventario siano crittografati di conseguenza. Per ulteriori informazioni, consulta Catalogazione e analisi dei dati con Inventario S3 .	06 Novembre 2017

Modifica	Descrizione	Data
Cross-Region Miglioramenti alla replica (CRR)	<p>Cross-Region La replica ora supporta quanto segue:</p> <ul style="list-style-type: none">• In uno scenario con più account, è possibile aggiungere e una configurazione CRR (Cross-Region Replication, replica tra regioni) per trasferire la proprietà della replica all' Account AWS proprietario del bucket di destinazione. Per ulteriori informazioni, consulta Modifica del proprietario della replica.• Per impostazione predefinita, Amazon S3 non replica gli oggetti nel bucket di origine creati utilizzando la crittografia lato server utilizzando le chiavi archiviate AWS KMS nella configurazione CRR, ora puoi indirizzare Amazon S3 a replicare questi oggetti. Per ulteriori informazioni, consulta Replica di oggetti crittografati (,,,) SSE-S3 SSE-KMS DSSE-KMS SSE-C.	06 Novembre 2017
Europe (London) Region	Amazon S3 è ora disponibile nella regione UE (Londra). Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a regioni ed endpoint nella Riferimenti generali di AWS.	13 dicembre 2016
Canada (Central) Region	Amazon S3 ora è disponibile nella regione Canada (Centrale). Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a regioni ed endpoint nella Riferimenti generali di AWS.	8 dicembre 2016

Modifica	Descrizione	Data
Tagging oggetti	<p>Amazon S3 supporta ora il tagging degli oggetti. Il tagging consente di catalogare lo storage. I prefissi dei nomi delle chiavi degli oggetti consentono di categorizzare lo storage, mentre il tagging aggiunge un'altra dimensione allo storage.</p> <p>Il tagging offre ulteriori benefici. Eccone alcuni:</p> <ul style="list-style-type: none">• I tag degli oggetti consentono un controllo estremamente preciso delle autorizzazioni (ad esempio, si potrebbero concedere a un utente IAM autorizzazioni di sola lettura sugli oggetti con tag specifici).• Fine-grained controllo nella definizione della configurazione del ciclo di vita. È possibile specificare dei tag per selezionare un sottoinsieme di oggetti a cui si applica la regola del ciclo di vita.• Se hai configurato Cross-Region Replication (CRR), Amazon S3 può replicare i tag. È necessario concedere l'autorizzazione appropriata al ruolo IAM creato affinché Amazon S3 si incarichi di replicare gli oggetti automaticamente.• Puoi anche personalizzare CloudWatch metriche ed CloudTrail eventi per visualizzare le informazioni tramite filtri di tag specifici. <p>Per ulteriori informazioni, consulta Etichettare i tuoi oggetti.</p>	29 Novembre 2016

Modifica	Descrizione	Data
Il ciclo di vita di Amazon S3 supporta ora i filtri basati su tag	Amazon S3 supporta ora i filtri basati su tag nella configurazione del ciclo di vita. Ora si può specificare una regola del ciclo di vita del bucket in cui è possibile indicare un prefisso della chiave, uno o più tag dell'oggetto o una combinazione di questi elementi per selezionare un sottoinsieme di oggetti a cui si applica la regola del ciclo di vita. Per ulteriori informazioni, consulta Gestione del ciclo di vita degli oggetti .	29 Novembre 2016
CloudWatch richiedi metriche per i bucket	Amazon S3 ora supporta le CloudWatch metriche per le richieste effettuate sui bucket. Quando vengono abilitati per un bucket, questi parametri sono disponibili a intervalli di 1 minuto. È inoltre possibile definire quali oggetti in un bucket riporteranno i parametri di richiesta. Per ulteriori informazioni, consulta Metriche di monitoraggio con Amazon CloudWatch .	29 Novembre 2016
Inventario Amazon S3	Amazon S3 supporta ora l'inventario dello storage. Amazon S3 Inventory genera un file di output flat degli oggetti e dei metadati corrispondenti per un bucket S3 o un prefisso condiviso (ovvero oggetti con nomi che iniziano con una stringa comune), su base giornaliera o settimanale. Per ulteriori informazioni, consulta Catalogazione e analisi dei dati con Inventario S3 .	29 Novembre 2016

Modifica	Descrizione	Data
Analisi di Amazon S3 – Analisi della classe di storage	La nuova caratteristica di analisi di Amazon S3 (analisi della classe di archiviazione) osserva i modelli di accesso ai dati per aiutare a determinare quando è opportuno spostare i dati meno utilizzati dalla classe di archiviazione STANDARD alla classe di archiviazione STANDARD_IA (IA sta per "Infrequent Access", accesso infrequente). Dopo l'osservazione degli schemi di accesso poco frequenti a un set di dati filtrati in un certo periodo di tempo da parte dell'analisi della classe di archiviazione, i risultati dell'analisi possono essere utilizzati per migliorare le configurazioni del ciclo di vita. Questa caratteristica include anche un'analisi giornaliera dettagliata dell'utilizzo dello storage a livello di un bucket, prefisso o tag specificato che può essere esportata in un bucket S3.	29 Novembre 2016
Nuovo recupero rapido e in blocco dei dati durante il ripristino di oggetti archiviati da Amazon Glacier	Amazon S3 supporta ora il recupero rapido e in blocco dei dati oltre al recupero standard durante il ripristino di oggetti archiviati in Amazon Glacier. Per ulteriori informazioni, consulta Ripristino di un oggetto archiviato .	21 novembre 2016
CloudTrail registrazione degli oggetti	CloudTrail supporta la registrazione di operazioni API a livello di oggetto di Amazon S3 come <code>GetObject</code> , <code>PutObject</code> e <code>DeleteObject</code> . È possibile configurare alcuni selettori di evento per registrare le operazioni delle API a livello di oggetto. Per ulteriori informazioni, consulta Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail .	21 Novembre 2016
US East (Ohio) Region	Amazon S3 è ora disponibile nella regione Stati Uniti orientali (Ohio). Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a regioni ed endpoint nella Riferimenti generali di AWS.	17 Ottobre 2016

Modifica	Descrizione	Data
Supporto di IPv6 per Amazon S3 Transfer Acceleration	Amazon S3 supporta ora IPv6 (Internet Protocol versione 6) per Amazon S3 Transfer Acceleration. È possibile connettersi ad Amazon S3 tramite IPv6 utilizzando il nuovo endpoint dual-stack per Transfer Acceleration. Per ulteriori informazioni, consulta Nozioni di base su Amazon S3 Transfer Acceleration .	6 ottobre 2016
Supporto IPv6	Amazon S3 supporta ora IPv6 (Internet Protocol versione 6). È possibile accedere ad Amazon S3 tramite IPv6 mediante gli endpoint dual-stack. Per ulteriori informazioni, consulta Esecuzione di richieste ad Amazon S3 su IPv6 nella documentazione di riferimento delle API Amazon S3.	11 agosto 2016
Asia Pacific (Mumbai) Region	Amazon S3 è ora disponibile nella regione Asia Pacifico (Mumbai). Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a regioni ed endpoint nella Riferimenti generali di AWS.	27 giugno 2016
Amazon S3 Transfer Acceleration	Amazon S3 Transfer Acceleration permette il trasferimento rapido, semplice e sicuro di file su lunga distanza tra un client e un bucket S3. Transfer Acceleration sfrutta le edge location distribuite da Amazon CloudFront a livello globale. Per ulteriori informazioni, consulta Configurazione di trasferimenti veloci e sicuri di file con Amazon S3 Transfer Acceleration .	19 Aprile 2016
Supporto del ciclo di vita per rimuovere i contrassegni di eliminazione degli oggetti scaduti	L'azione <code>Expiration</code> di configurazione del ciclo di vita consente ora di configurare Amazon S3 per rimuovere i contrassegni di eliminazione degli oggetti scaduti in un bucket con versione. Per ulteriori informazioni, consulta Elementi per la descrizione delle operazioni nel ciclo di vita .	16 marzo 2016

Modifica	Descrizione	Data
La configurazione del ciclo di vita del bucket supporta l'operazione per interrompere i caricamenti in più parti incompleti	<p>La configurazione del ciclo di vita del bucket supporta ora l'operazione <code>AbortIncompleteMultipartUpload</code> , che è possibile utilizzare per fare in modo che Amazon S3 interrompa i caricamenti in più parti che non vengono completati entro un numero specificato di giorni dopo l'avvio. Quando un caricamento in più parti incompleto diventa idoneo per un'operazione di interruzione, Amazon S3 elimina le parti caricate e interrompe il caricamento in più parti.</p> <p>Per informazioni più tecniche, consulta gli argomenti seguenti nella Guida per l'utente di Amazon S3:</p> <ul style="list-style-type: none"> • Interruzione di un caricamento in più parti • Elementi per la descrizione delle operazioni nel ciclo di vita <p>Le seguenti operazioni API sono state aggiornata per supportare la nuova operazione:</p> <ul style="list-style-type: none"> • PUT Bucket lifecycle (Ciclo di vita PUT Bucket) – La configurazione XML permette ora di specificare l'operazione <code>AbortIncompleteMultipartUpload</code> in una regola di configurazione del ciclo di vita. • List Parts (Elenco parti) e Initiate Multipart Upload (Avvio del caricamento in più parti) – Entrambe queste operazioni API restituiscono ora due intestazioni di risposta aggiuntive (<code>x-amz-abort-date</code> e <code>x-amz-abort-rule-id</code>) se al bucket è associata una regola del ciclo di vita che specifica l'operazione <code>AbortIncompleteMultipartUpload</code> . Queste intestazioni di risposta indicano in quale momento il caricamento in più 	16 marzo 2016

Modifica	Descrizione	Data
	parti avviato è diventato idoneo all'operazione di interruzione e quale regola del ciclo di vita può essere applicata.	
Asia Pacific (Seoul) Region	Amazon S3 è ora disponibile nella regione Asia Pacifico (Seoul). Per ulteriori informazioni sulle regioni e gli endpoint Amazon S3, consultare la sezione relativa a regioni ed endpoint nella Riferimenti generali di AWS.	6 gennaio 2016
Nuova chiave di condizione e modifica del caricamento in più parti	<p>Le policy IAM supportano ora una chiave di condizione <code>s3:x-amz-storage-class</code> Amazon S3. Per ulteriori informazioni, consulta Esempi di policy per i bucket che utilizzano le chiavi di condizione.</p> <p>Non è più necessario essere l'account che ha iniziato un caricamento in più parti per caricare le parti e completare il caricamento. Per ulteriori informazioni, consulta Autorizzazioni e API per il caricamento in più parti.</p>	14 dicembre 2015
Regione Stati Uniti standard rinominata	È stata modificata la stringa del nome della regione da "Stati Uniti standard" a "Stati Uniti orientali (Virginia settentrionale)". Si tratta solo di un aggiornamento del nome della regione, senza modifiche della funzionalità.	11 dicembre 2015

Modifica	Descrizione	Data
Nuova classe di storage	<p>Amazon S3 offre ora una nuova classe di storage, STANDARD_IA (IA sta per "Infrequent Access", accesso infrequente) per archiviare gli oggetti. Questa classe di storage è ottimizzata per i dati esistenti da molto tempo a cui si accede meno frequentemente. Per ulteriori informazioni, consulta Comprensione e gestione delle classi di storage Amazon S3.</p> <p>La funzione di configurazione del ciclo di vita consente ora la transizione degli oggetti alla classe di storage standard_IA. Per ulteriori informazioni, consulta Gestione del ciclo di vita degli oggetti.</p> <p>In precedenza, la funzionalità di Cross-Region replica utilizzava la classe di archiviazione dell'oggetto sorgente per le repliche degli oggetti. Ora, quando configuri Cross-Region Replication, puoi specificare una classe di archiviazione per la replica dell'oggetto creata nel bucket di destinazione. Per ulteriori informazioni, consulta Replica di oggetti all'interno e tra le Regioni.</p>	16 settembre 2015
AWS CloudTrail integrazione	<p>La nuova AWS CloudTrail integrazione ti consente di registrare l'attività dell'API Amazon S3 nel tuo bucket S3. Puoi utilizzarlo CloudTrail per tenere traccia delle creazioni o delle eliminazioni dei bucket S3, delle modifiche al controllo degli accessi o delle modifiche alla configurazione del ciclo di vita. Per ulteriori informazioni, consulta Registrazione delle chiamate API Amazon S3 utilizzando AWS CloudTrail.</p>	1 settembre 2015

Modifica	Descrizione	Data
Aumento del limite del bucket	Amazon S3 supporta ora l'aumento dei limiti per i bucket. Per impostazione predefinita, i clienti possono creare fino a 100 bucket nel proprio Account AWS. I clienti che hanno bisogno di altri bucket possono aumentare tale limite richiedendo un aumento del limite di servizio. Per informazioni su come aumentare il limite per i bucket, consulta Service Quotas di Servizio AWS nella Documentazione di riferimento generale di AWS. Per ulteriori informazioni, consulta Utilizzo di AWS SDK e Quote, restrizioni e limitazioni dei bucket per uso generico .	4 agosto 2015
Aggiornamento del modello di consistenza	Amazon S3 supporta ora la consistenza di lettura dopo scrittura per i nuovi oggetti aggiunti ad Amazon S3 nella regione Stati Uniti orientali (Virginia settentrionale). Prima di questo aggiornamento tutte le regioni, eccetto la regione Stati Uniti orientali (Virginia settentrionale), supportavano la consistenza di lettura dopo scrittura per i nuovi oggetti caricati in Amazon S3. Con questo miglioramento, Amazon S3 ora supporta la coerenza lettura dopo scrittura in tutte le regioni per i nuovi oggetti aggiunti ad Amazon S3. Read-after-write la coerenza consente di recuperare gli oggetti immediatamente dopo la creazione in Amazon S3. Per ulteriori informazioni, consulta Regioni .	4 agosto 2015
Notifiche eventi	La funzionalità di notifica eventi di Amazon S3 è stata aggiornata con l'aggiunta di notifiche quando gli oggetti vengono eliminati e l'aggiunta di filtri basati sui nomi degli oggetti con prefisso e suffisso corrispondenti. Per ulteriori informazioni, consulta Notifiche di eventi Amazon S3 .	28 luglio 2015

Modifica	Descrizione	Data
Integrazione con Amazon CloudWatch	La nuova CloudWatch integrazione con Amazon ti consente di monitorare e impostare allarmi sull'utilizzo di Amazon S3 tramite CloudWatch metriche per Amazon S3. Le metriche supportate includono i byte totali per lo storage standard, i byte totali per lo storage e il numero totale Reduced-Redundancy di oggetti per un determinato bucket S3. Per ulteriori informazioni, consulta Metriche di monitoraggio con Amazon CloudWatch .	28 luglio 2015
Supporto per eliminare e svuotare i bucket non vuoti	Amazon S3 supporta ora l'eliminazione e lo svuotamento dei bucket non vuoti. Per ulteriori informazioni, consulta Eliminazione del contenuto di un bucket per uso generico .	16 luglio 2015
Policy di bucket per gli endpoint di Amazon VPC	Amazon S3 ha aggiunto il supporto per le policy del bucket per gli endpoint Virtual Private Cloud (VPC). È possibile utilizzare le policy del bucket S3 per controllare l'accesso ai bucket da VPC o da endpoint VPC specifici. Gli endpoint VPC sono facili da configurare ed estremamente affidabili e offrono una connessione sicura ad Amazon S3 senza la necessità di un gateway o di un'istanza NAT. Per ulteriori informazioni, consulta Controllo dell'accesso dagli endpoint VPC con policy di bucket .	29 Aprile 2015
Notifiche degli eventi	Le notifiche di eventi di Amazon S3 sono state aggiornate per supportare il passaggio alle autorizzazioni basate sulle risorse per le funzioni. AWS Lambda Per ulteriori informazioni, consulta Notifiche di eventi Amazon S3 .	9 Aprile 2015
Cross-Region Replica	Amazon S3 ora supporta Cross-Region la replica. Cross-Region La replica è la copia automatica e asincrona di oggetti tra bucket diversi. Regioni AWS Per ulteriori informazioni, consulta Replica di oggetti all'interno e tra le Regioni .	24 marzo 2015

Modifica	Descrizione	Data
Notifiche eventi	Amazon S3 supporta ora nuovi tipi di evento e destinazioni nella configurazione delle notifiche dei bucket. Prima di questa versione, Amazon S3 supportava solo il tipo di ReducedRedundancyLostObject evento s3: e un argomento Amazon SNS come destinazione. Per ulteriori informazioni sull'utilizzo dei nuovi tipi di eventi, consulta Notifiche di eventi Amazon S3 .	13 Novembre 2014
Server-side crittografia con chiavi di crittografia fornite dal cliente	<p>Server-side crittografia con chiavi AWS Key Management Service (AWS KMS) () SSE-KMS</p> <p>Amazon S3 ora supporta la crittografia lato server utilizzando. AWS KMS Questa funzionalità consente di gestire la chiave di inviluppo e le AWS KMS chiamate di Amazon S3 AWS KMS per accedere alla chiave di inviluppo entro le autorizzazioni impostate.</p> <p>Per ulteriori informazioni sulla crittografia lato server con, consulta Protecting Data Using Encryption with AWS KMS. Server-Side AWS Key Management Service</p>	12 Novembre 2014
Europe (Frankfurt) Region	Amazon S3 è ora disponibile nella regione UE (Francoforte).	23 ottobre 2014

Modifica	Descrizione	Data
Server-side crittografia con chiavi di crittografia fornite dal cliente	<p>Amazon S3 ora supporta la crittografia lato server utilizzando chiavi di crittografia fornite dal cliente (). SSE-C Server-side la crittografia ti consente di richiedere ad Amazon S3 di crittografare i tuoi dati inattivi. Durante l'utilizzo SSE-C, Amazon S3 crittografa i tuoi oggetti con le chiavi di crittografia personalizzate fornite. Poiché Amazon S3 esegue automaticamente la crittografia, si ottengono i vantaggi legati all'utilizzo di chiavi di crittografia personali, ma senza che sia necessario scrivere o eseguire codice di crittografia personalizzato.</p> <p>Per ulteriori informazioni SSE-C, consulta Server-Side Encryption (Using Customer-Provided Encryption Keys).</p>	12 giugno 2014
Supporto della funzione Controllo delle versioni a livello del ciclo di vita	<p>Nelle release precedenti, la configurazione del ciclo di vita era supportata solo per i bucket senza versione. Ora è possibile configurare il ciclo di vita sia sui bucket senza versione che su quelli con funzione Controllo delle versioni abilitata. Per ulteriori informazioni, consulta Gestione del ciclo di vita degli oggetti.</p>	20 maggio 2014
Argomenti del controllo degli accessi modificati	<p>È stata modificata la documentazione sul controllo degli accessi di Amazon S3. Per ulteriori informazioni, consulta Identity and Access Management per Amazon S3.</p>	15 Aprile 2014
Argomenti relativi alla registrazione degli accessi al server modificati	<p>È stata modificata la documentazione sulla registrazione degli accessi al server. Per ulteriori informazioni, consulta Registrazione delle richieste con registrazione dell'accesso al server.</p>	26 Novembre 2013
Esempi sull'SDK .NET aggiornati alla versione 2.0	<p>Gli esempi sull'SDK .NET di questa guida sono ora conformi alla versione 2.0.</p>	26 Novembre 2013

Modifica	Descrizione	Data
Supporto SOAP su HTTP obsoleto	Il supporto di SOAP su HTTP non viene più utilizzato, ma è ancora disponibile su HTTPS. Le nuove funzioni di Amazon S3 non saranno supportate per SOAP. Ti consigliamo di utilizzare l'API REST o gli AWS SDK.	20 settembre 2013
Supporto delle variabili di policy IAM	<p>Il linguaggio delle policy IAM ora supporta le variabili . Quando una policy viene valutata, eventuali variabili di policy vengono sostituite con valori forniti in base a informazioni basate sul contesto relative alla sessione dell'utente autenticato. Si possono utilizzare variabili di policy per definire policy generali senza elencare esplicitamente tutte le componenti della policy. Per ulteriori informazioni sulle variabili di policy, consulta la pagina relativa alla panoramica delle variabili di policy IAM nella Guida per l'utente di IAM.</p> <p>Per esempi di variabili di policy in Amazon S3, consulta Identity-based esempi di policy per Amazon S3.</p>	3 Aprile 2013
Supporto di Pagamento a carico del richiedente a livello console	È ora possibile configurare il bucket per Pagamento a carico del richiedente tramite la console Amazon S3. Per ulteriori informazioni, consulta Utilizzo dei bucket per uso generico con pagamento a carico del richiedente per archiviazione e trasferimenti di dati .	31 dicembre 2012

Modifica	Descrizione	Data
Supporto per l'hosting di un sito Web in un dominio root	Amazon S3 supporta ora l'hosting di siti Web statici in un dominio root. I visitatori del sito Web possono accedere al sito dal loro browser senza specificare www nell'indirizzo Web (ad esempio, digitando example.com al posto di www.example.com). Molti clienti ospitano già siti Web statici in Amazon S3 accessibili tramite un sottodominio www, ad esempio www.example.com. In precedenza, per supportare l'accesso al dominio root era necessario eseguire il proprio server Web per inoltrare tramite proxy le richieste del dominio root dai browser al sito Web in Amazon S3. L'utilizzo di un server Web per le richieste proxy comporta ulteriori costi, carichi operativi e un'altra possibilità di errore. Ora è possibile sfruttare i vantaggi della durabilità e della disponibilità elevata di Amazon S3 sia per gli indirizzi di dominio root che www. Per ulteriori informazioni, consulta Hosting di un sito Web statico tramite Amazon S3 .	27 dicembre 2012
Revisione della console	La console Amazon S3 è stata aggiornata. Gli argomenti della documentazione che si riferiscono alla console sono stati modificati di conseguenza.	14 dicembre 2012
Supporto per l'archiviazione dei dati in Amazon Glacier	Amazon S3 supporta ora un'opzione di archiviazione che permette di utilizzare il servizio di archiviazione a basso costo di Amazon Glacier per l'archiviazione dei dati. Per archiviare gli oggetti, è necessario definire le regole di archiviazione che identificano gli oggetti e l'intervallo di tempo in cui Amazon S3 deve archiviare questi oggetti in Amazon Glacier. Puoi impostare facilmente le regole su un bucket utilizzando la console Amazon S3 o a livello di codice utilizzando l'API o gli SDK di Amazon S3. AWS Per ulteriori informazioni, consulta Gestione del ciclo di vita degli oggetti .	13 Novembre 2012

Modifica	Descrizione	Data
Supporto del reindirizzamento delle pagine del sito Web	<p>Per i bucket configurati come sito Web, Amazon S3 supporta ora il reindirizzamento di una richiesta di un oggetto a un altro oggetto nello stesso bucket o a un URL esterno. Per ulteriori informazioni, consulta (Facoltativo) Configurazione del reindirizzamento di una pagina Web.</p> <p>Per informazioni sull'hosting dei siti Web, consulta Hosting di un sito Web statico tramite Amazon S3.</p>	4 Ottobre 2012
Supporto per la condivisione delle risorse (CORS) Cross-Origin	<p>Amazon S3 ora supporta la condivisione Cross-Origin delle risorse (CORS). La funzionalità CORS definisce un metodo con cui le applicazioni Web dei clienti caricate in un dominio possono interagire con le risorse situate in un dominio differente o accedere a esse. Con il supporto di CORS in Amazon S3 è possibile creare applicazioni Web lato client complete basate su Amazon S3 e concedere l'accesso selettivo tra domini alle risorse di Amazon S3. Per ulteriori informazioni, consulta Utilizzo della funzionalità Cross-Origin Resource Sharing (CORS).</p>	31 agosto 2012
Supporto dei tag dell'allocazione dei costi	<p>Amazon S3 supporta ora l'assegnazione di tag per l'allocazione dei costi, che permette di etichettare i bucket S3 in modo da poter tenere traccia più facilmente dei costi in base ai progetti o ad altri criteri. Per ulteriori informazioni sull'utilizzo del tagging per i bucket, consulta Utilizzo dei tag per l'allocazione dei costi per i bucket S3.</p>	21 agosto 2012

Modifica	Descrizione	Data
Supporto per l'accesso alle MFA-protected API nelle policy dei bucket	<p>Amazon S3 ora supporta l'accesso alle MFA-protected API, una funzionalità che può imporre AWS Multi-Factor l'autenticazione per un ulteriore livello di sicurezza quando si accede alle risorse Amazon S3. È una funzione di protezione che prevede che gli utenti dimostrino di possedere fisicamente un dispositivo MFA fornendo un codice MFA valido. Per ulteriori informazioni, vai a Autenticazione. AWS Multi-Factor È ora possibile richiedere e l'autenticazione MFA per tutte le richieste di accesso alle risorse di Amazon S3.</p> <p>Per imporre il requisito dell'autenticazione MFA, Amazon S3 supporta ora la chiave <code>aws:MultiFactorAuthAge</code> in una policy del bucket. Per un esempio di policy di bucket, consulta Richiesta dell'autenticazione a più fattori (MFA).</p>	10 luglio 2012
Supporto per la scadenza degli oggetti	Si può utilizzare la scadenza degli oggetti per pianificare la rimozione automatica dei dati dopo un periodo di tempo configurato. Per impostare la scadenza degli oggetti, devi aggiungere la configurazione del ciclo di vita in un bucket.	27 dicembre 2011
Nuova regione supportata	Amazon S3 supporta ora la regione Sud America (San Paolo). Per ulteriori informazioni, consulta Accesso a un bucket per uso generico Amazon S3 .	14 dicembre 2011
Multi-Object Elimina	Amazon S3 ora supporta l'API Multi-Object Delete che consente di eliminare più oggetti in un'unica richiesta. Grazie a questa caratteristica, è possibile rimuovere grandi quantità di oggetti da Amazon S3 più rapidamente rispetto all'utilizzo di più richieste DELETE singole. Per ulteriori informazioni, consulta Eliminazione di oggetti Amazon S3 .	7 dicembre 2011
Nuova regione supportata	Amazon S3 supporta ora la regione Stati Uniti occidentali (Oregon). Per ulteriori informazioni, consulta Bucket e regioni .	8 Novembre 2011

Modifica	Descrizione	Data
Aggiornamento della documentazione	Correzione dei bug della documentazione.	8 Novembre 2011
Aggiornamento della documentazione	<p>Oltre alla correzione dei bug della documentazione, questa release include i seguenti miglioramenti:</p> <ul style="list-style-type: none">• Nuove sezioni di crittografia lato server che utilizzano AWS SDK per PHP e AWS SDK per Ruby (vedi). Specificare la crittografia lato server con chiavi gestite da Amazon S3 () SSE-S3	17 ottobre 2011
Server-side supporto per la crittografia	Amazon S3 supporta ora la crittografia lato server. Permette di richiedere ad Amazon S3 di crittografare i dati inattivi, ovvero i dati degli oggetti quando Amazon S3 scrive i dati sui dischi nei data center. Oltre agli aggiornamenti dell'API REST, il.NET forniscono AWS SDK per Java le funzionalità necessarie per richiedere la crittografia lato server. È anche possibile richiedere la crittografia lato server durante il caricamento di oggetti tramite la Console di gestione AWS. Per ulteriori informazioni sulla crittografia dei dati, consulta Utilizzo della crittografia dei dati .	4 ottobre 2011

Modifica	Descrizione	Data
Aggiornamento della documentazione	<p>Oltre alla correzione dei bug della documentazione, questa release include i seguenti miglioramenti:</p> <ul style="list-style-type: none">• Sono stati aggiunti esempi su Ruby e PHP nella sezione Esecuzione di richieste della documentazione di riferimento delle API Amazon S3.• Aggiunta di sezioni che descrivono come generare e usare URL prefirmati. Per ulteriori informazioni, consulta Condivisione di oggetti mediante URL prefirmati e Condivisione di oggetti mediante URL prefirmati.• È stata aggiornata una sezione esistente per introdurre AWS Explorers for Eclipse e Visual Studio. Per ulteriori informazioni, consulta Sviluppo con Amazon S3 utilizzando gli AWS SDK nell'API Reference di Amazon S3.	22 settembre 2011

Modifica	Descrizione	Data
Supporto all'invio di richieste mediante credenziali di sicurezza temporanee	<p>Oltre a utilizzare le tue credenziali di sicurezza Account AWS e quelle degli utenti IAM per inviare richieste autenticate ad Amazon S3, ora puoi inviare richieste utilizzando le credenziali di sicurezza temporanee ottenute da (IAM). AWS Identity and Access Management Puoi utilizzare il Servizio di token di sicurezza AWS API o le librerie wrapper AWS SDK per richiedere queste credenziali temporanee a IAM. Si possono richiedere queste credenziali di sicurezza temporanee per uso personale oppure per fornirle agli utenti federati e alle applicazioni. Questa funzionalità consente di gestire gli utenti all'esterno AWS e fornire loro credenziali di sicurezza temporanee per accedere alle risorse. AWS</p> <p>Per ulteriori informazioni, consulta Esecuzione di richieste nella documentazione di riferimento delle API Amazon S3.</p> <p>Per ulteriori informazioni sul supporto IAM per le credenziali di sicurezza temporanee, consulta la sezione relativa alle credenziali di sicurezza temporanee nella Guida per l'utente di IAM.</p>	3 agosto 2011
L'API per il caricamento in più parti è stata ampliata per consentire la copia di oggetti fino a 5 TB	<p>Prima di questa versione, l'API Amazon S3 supportava la copia di oggetti con dimensioni massime di 5 GB. Per permettere la copia di oggetti con dimensioni superiori a 5 GB, Amazon S3 ora estende l'API per il caricamento in più parti con una nuova operazione, <code>UploadPart (Copy)</code>. È possibile utilizzare questa operazione di caricamento in più parti per copiare gli oggetti con dimensioni massime di 5 TB. Per ulteriori informazioni, consulta Copia, spostamento e denominazione di oggetti.</p> <p>Per informazioni più tecniche sull'API per il caricamento in più parti, consulta Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3.</p>	21 giugno 2011

Modifica	Descrizione	Data
Chiamate all'API SOAP su HTTP disabilitate	Per aumentare la sicurezza, le chiamate all'API SOAP su HTTP sono state disabilitate. Le richieste SOAP autenticate e anonime devono essere inviate ad Amazon S3 tramite SSL.	6 giugno 2011
IAM permette la delega multiaccount	<p>In precedenza, per accedere a una risorsa Amazon S3, un utente IAM necessitava delle autorizzazioni sia del padre che del proprietario Account AWS della risorsa Amazon S3. Con l'accesso multiaccount l'utente IAM deve ora disporre solo dell'autorizzazione concessa dall'account proprietario. Cioè, se il proprietario di una risorsa concede l'accesso a una Account AWS, ora Account AWS può concedere ai suoi utenti IAM l'accesso a tali risorse.</p> <p>Per ulteriori informazioni, consulta la pagina relativa alla creazione di un ruolo per delegare le autorizzazioni a un utente IAM nella Guida per l'utente IAM.</p> <p>Per ulteriori informazioni sulla specifica delle informazioni principali nella policy di un bucket, consulta Principali per le policy dei bucket.</p>	6 giugno 2011
Nuovo collegamento	Le informazioni relative all'endpoint del servizio si trovano ora nella Documentazione di riferimento generale di AWS . Per ulteriori informazioni, consulta la pagina relativa a regioni ed endpoint nella Documentazione di riferimento generale di AWS .	1 marzo 2011

Modifica	Descrizione	Data
Supporto per l'hosting di siti Web statici in Amazon S3	Amazon S3 introduce il supporto migliorato per l'hosting di siti Web statici. È incluso il supporto per i documenti di indice e i documenti di errore personalizzati. Quando utilizzi queste funzionalità, le richieste alla root del bucket o a una cartella (ad esempio <code>http://mywebsite.com/subfolder</code>) restituiscono il documento di indice invece dell'elenco di oggetti nel bucket. Se si verifica un errore, Amazon S3 restituisce il messaggio di errore personalizzato anziché un messaggio di errore di Amazon S3. Per ulteriori informazioni, consulta Hosting di un sito Web statico tramite Amazon S3 .	6 giugno 2011
Le informazioni relative all'endpoint del servizio si trovano ora nella Documentazione di riferimento generale di AWS . Per ulteriori informazioni, consulta la pagina relativa a regioni ed endpoint nella Documentazione di riferimento generale di AWS .	1 marzo 2011	

Modifica	Descrizione	Data
Supporto per l'hosting di siti Web statici in Amazon S3	Amazon S3 introduce il supporto migliorato per l'hosting di siti Web statici. È incluso il supporto per i documenti di indice e i documenti di errore personalizzati. Quando utilizzi queste funzionalità, le richieste alla root del bucket o a una cartella (ad esempio <code>http://mywebsite.com/subfolder</code>) restituiscono il documento di indice invece dell'elenco di oggetti nel bucket. Se si verifica un errore, Amazon S3 restituisce il messaggio di errore personalizzato anziché un messaggio di errore di Amazon S3. Per ulteriori informazioni, consulta Hosting di un sito Web statico tramite Amazon S3 .	17 febbraio 2011
Supporto API per le intestazioni di risposta	L'API GET Object REST ora consente di modificare le intestazioni di risposta di ogni richiesta REST GET Object. Si possono quindi modificare i metadata degli oggetti nella risposta senza modificare l'oggetto in sé. Per ulteriori informazioni, consulta Download di oggetti .	14 gennaio 2011
Supporto ampliato per gli oggetti	Amazon S3 ha aumentato le dimensioni massime di un oggetto che è possibile archiviare in un bucket S3 da 5 GB a 5 TB. Se si utilizza la REST API, è possibile caricare oggetti con una dimensione massima di 5 GB con una singola operazione PUT. Per oggetti di dimensioni maggiori occorre utilizzare l'API REST per il caricamento in più parti. Per ulteriori informazioni, consulta Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3 .	9 dicembre 2010
Caricamento in più parti	Il caricamento in più parti permette operazioni di caricamento più rapide e flessibili in Amazon S3. Permette di caricare un unico oggetto come un insieme di parti. Per ulteriori informazioni, consulta Caricamento e copia di oggetti utilizzando il caricamento multiparte in Amazon S3 .	10 Novembre 2010

Modifica	Descrizione	Data
Supporto ID canonico nelle policy di bucket	È ora possibile specificare ID convenzionali nelle policy di bucket. Per ulteriori informazioni, consulta Principali per le policy dei bucket	17 settembre 2010
Amazon S3 funziona con IAM	Questo servizio ora si integra con AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta Servizi AWS supportati da IAM nella Guida per l'utente di IAM.	2 settembre 2010
Notifiche	La caratteristica di notifica Amazon S3 permette di configurare un bucket in modo che Amazon S3 pubblichi un messaggio in un argomento Amazon Simple Notification Service (Amazon SNS) quando Amazon S3 rileva un evento chiave in un bucket. Per ulteriori informazioni, consulta Configurazione delle notifiche degli eventi del bucket .	14 luglio 2010
Policy di bucket	Le policy di bucket sono un sistema di gestione degli accessi utilizzato per configurare le autorizzazioni di accesso a bucket, oggetti e insiemi di oggetti. Questa funzionalità integra, e in molti casi sostituisce, le liste di controllo accessi. Per ulteriori informazioni, consulta Policy dei bucket per Amazon S3 .	6 luglio 2010
Path-style sintassi disponibile in tutte le regioni	Amazon S3 supporta ora la sintassi basata su percorsi per qualsiasi bucket nella regione Stati Uniti classica oppure se il bucket si trova nella stessa regione dell'endpoint della richiesta. Per ulteriori informazioni, consulta Hosting virtuale .	9 giugno 2010
Nuovo endpoint per la regione UE (Irlanda)	Amazon S3 fornisce ora un endpoint per la regione UE (Irlanda): <code>http://s3-eu-west-1.amazonaws.com</code> .	9 giugno 2010

Modifica	Descrizione	Data
Console	È ora possibile utilizzare Amazon S3 tramite la Console di gestione AWS. Puoi trovare le informazioni su tutte le funzionalità di Amazon S3 nella console nella Guida per l'utente di Amazon Simple Storage Service.	9 giugno 2010
Ridondanza ridotta	Amazon S3 permette ora di ridurre i costi di storage tramite l'archiviazione degli oggetti in Amazon S3 con ridondanza ridotta. Per ulteriori informazioni, consulta Reduced Redundancy Storage .	12 maggio 2010
Nuova regione supportata	Amazon S3 supporta ora la regione Asia Pacifico (Singapore). Per ulteriori informazioni, consulta Bucket e regioni .	28 Aprile 2010
Funzione Controllo delle versioni degli oggetti	In questa release è stata introdotta la funzione Controllo delle versioni degli oggetti. Tutti gli oggetti possono ora avere una chiave e una versione. Se si abilita la funzione Controllo delle versioni del bucket, Amazon S3 fornisce a tutti gli oggetti aggiunti a tale bucket un ID versione univoco. Questa caratteristica ti permette di eseguire il ripristino in seguito a operazioni accidentali di eliminazione e sovrascrittura. Per ulteriori informazioni, consulta Funzione Controllo delle versioni e Uso della funzione Controllo delle versioni .	8 febbraio 2010
Nuova regione supportata	Amazon S3 supporta ora la regione Stati Uniti occidentali (California settentrionale). Il nuovo endpoint per le richieste a questa regione è <code>s3-us-west-1.amazonaws.com</code> . Per ulteriori informazioni, consulta Bucket e regioni .	2 dicembre 2009

Modifica	Descrizione	Data
AWS SDK per .NET	AWS ora fornisce librerie, codice di esempio, tutorial e altre risorse per gli sviluppatori di software che preferiscono creare applicazioni utilizzando operazioni API specifiche del linguaggio.NET anziché REST o SOAP. Queste librerie forniscono funzioni di base (non incluse nelle API REST o SOAP), come autenticazione di richiesta, nuovi tentativi di richiesta e gestione degli errori per iniziare in modo più semplice. Per ulteriori informazioni su librerie e risorse specifiche del linguaggio, consulta Sviluppo con Amazon S3 utilizzando gli SDK nell'Amazon S3 API Reference. AWS	11 Novembre 2009

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.